(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3781640号
(P3781640)
(45)発行日　平成18年5月31日(2006.5.31)　(24)登録日　平成18年3月17日(2006.3.17)

(51)Int.Cl.　　F I
G06F 21/24 (2006.01)　　G06F 12/14 540A
H04L 9/10 (2006.01)　　H04L 9/00 621Z

請求項の数 11　(全 13 頁)

(21)出願番号　特願2001-168974(P2001-168974)
(22)出願日　平成13年6月5日(2001.6.5)
(65)公開番号　特開2002-366437(P2002-366437A)
(43)公開日　平成14年12月20日(2002.12.20)
審査請求日　平成15年1月17日(2003.1.17)

(73)特許権者　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町２２番２２号
(74)代理人　100084135
弁理士　本庄　武男
(72)発明者　鳥居　幹夫
大阪府大阪市阿倍野区長池町２２番２２号
シャープ株式会社内
(72)発明者　中井　康博
大阪府大阪市阿倍野区長池町２２番２２号
シャープ株式会社内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】暗号化処理装置，暗号化処理システム

(57)【特許請求の範囲】

【請求項１】

受信したデータを暗号化して記憶装置に記憶した後に，該データを出力する暗号化処理装置において，

上記記憶装置が揮発性を有するか否かを判別する記憶形式判別手段と，上記記憶形式判別手段による判別結果に基づいて上記データに対して暗号化が必要か否かを判断するための要否判断手段と，を具備し，上記要否判断手段によって暗号化が必要と判断された場合に上記データを暗号化することを特徴とする暗号化処理装置。

【請求項２】

前記記憶形式判別手段が，前記記憶装置が当該暗号化処理装置の電源が切断された場合にデータを揮発するものであるか否かを判断するものである請求項１記載の暗号化処理装置。

【請求項３】

前記記憶形式判別手段が，前記記憶装置が当該暗号化処理装置から取り外された場合にデータを揮発するものであるか否かを判断するものである請求項１記載の暗号化処理装置。

【請求項４】

前記要否判断手段は，前記データの形態又は具備する項目に基いて，前記データに対して暗号化が必要か否かを判断してなる請求項１から３のいずれかに記載の暗号化処理装置。

【請求項５】
前記データの形態が既に暗号化されている場合に，前記要否判断手段は前記データに対して暗号化が不必要と判断してなる請求項４記載の暗号化処理装置。
【請求項６】
前記データの具備する項目が前記データの重要度に関する指標である場合に，前記要否判断手段は前記データに対して暗号化が必要と判断してなる請求項４記載の暗号化処理装置。
【請求項７】
前記指標が，フラグ，親展指示等である請求項６記載の暗号化処理装置。
【請求項８】
前記データの具備する項目が予め定められた条件である場合に，前記要否判断手段は前記データに対して暗号化が必要と判断してなる請求項４記載の暗号化処理装置。
【請求項９】
前記記憶装置に暗号化して記憶されている前記データを復元するための復元化手段を具備し，該復元化手段によって前記データが復元された後に前記データが出力されてなる請求項１から請求項８のいずれかに記載の暗号化処理装置。
【請求項１０】
請求項１から請求項９のいずれかに記載の暗号化処理装置の用途として，前記データの受信側の機器に採用されてなる暗号化処理装置。
【請求項１１】
データの作成などのサービスを提供するホスト装置と，該ホスト装置より受信したデータを暗号化して記憶装置に記憶した後に，該データを出力する暗号化処理装置とを具備した暗号化処理システムにおいて，
上記ホスト装置は，データを上記暗号化処理装置に送信する際に，該データに対して暗号化に関する条件を付加する条件付加手段を具備し，
上記暗号化処理装置は，上記記憶装置が揮発性を有するか否かを判別する記憶形式判別手段と，上記記憶形式判別手段による判別結果及び上記条件の有無に基いて，上記データに対して暗号化が必要か否かを判断するための要否判断手段と，を具備し，
上記要否判断手段によって暗号化が必要と判断された場合に上記データを暗号化処理装置側で暗号化することを特徴とする暗号化処理システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は，受信したデータを暗号化して記憶装置に記憶した後に，該データを出力する暗号化処理装置，暗号化処理システムに関するものである。
【０００２】
【従来の技術】
近年，サーバ等のホスト装置より送出されたデータをメモリ，ハードディスクドライブ（以下，「ＨＤＤ」と称する。）等の記憶装置に一旦記憶した後に，該記憶装置より上記データを出力するようなシステムがある。
このようなシステムの代表例としては，例えば印刷システムなどがある。この印刷システムは，例えば，多数のユーザによってプリンタが共有されている場合に，プリンタ側に上記記憶装置を設けることによって，多数のユーザから上記プリンタに対してデータが同時に送出されたとしても，上記記憶装置で該データを一旦記憶するので，該記憶したデータをプリンタ本体に順次出力して印刷することを可能にするシステムである。
しかし，上記システムにおいて，記憶装置よりデータを出力した後に該記憶装置にデータが残存したままであると，再び該記憶装置より上記データを出力することが可能となるので，従来より，データの出力後は記憶したデータを記憶装置より消去することが一般に行われている。これは，例えば，上記データが機密性の高いデータである場合等においては有効な処理である。

【０００３】
【発明が解決しようとする課題】
しかし，上述の技術の場合でも，ホスト装置より送出されたデータを一旦記憶装置に記憶してから該データを出力するまでの期間中は，該データは少なくとも上記記憶装置上に存在しており，該期間中に上記データが第３者によって読み出される，或いは，該期間中に上記データが記憶装置ごと盗まれる等の可能性が有り，上記データの安全性を確実に確保できているとは言い難い。
そこで，特開平４－３６６０号公報には，ファクシミリの記憶装置で受信したデータを暗号化して記憶し，該データを扱えるユーザが上記記憶装置にデータ復元用のＩＣカードを挿入することによって上記データを復元化して出力する技術について開示されている。
しかし，上述の技術では，上記記憶装置で受信した全てのデータを暗号化するものであるので，記憶装置における処理の負担が大きくなり上記暗号化に時間が掛かることや，暗号化の必要のないものまで暗号化される不都合がある。また更に，上記データの復元化の際に上記ＩＣカードを挿入する煩わしさがある。
そこで，本発明は上記事情に鑑みてなされたものであり，その目的とするところは，暗号化が必要と認められる受信データのみを暗号化することによって，効率良く記憶装置に上記データを記憶して出力することを可能にする暗号化処理装置，暗号化処理システムを提供することである。
【０００４】
【課題を解決するための手段】
本発明は，受信したデータを暗号化して記憶装置に記憶した後に，該データを出力する暗号化処理装置において，
上記記憶装置が揮発性を有するか否かを判別する記憶形式判別手段と，上記記憶形式判別手段による判別結果に基づいて上記データに対して暗号化が必要か否かを判断するための要否判断手段と，を具備し，上記要否判断手段によって暗号化が必要と判断された場合に上記データを暗号化することを特徴とする暗号化処理装置として構成されている。
本発明がこのように構成されているので，第３者によって前記記憶装置が盗難にあった場合のデータの読み出しの可能性が判別できるので，例えば，前記記憶装置のデータの保存性が低ければ盗難時にデータが消滅するので，データに対して暗号化する必要が無くなり，不要な暗号化を防止できる。
【０００５】
具体的には，前記記憶形式判別手段が，前記記憶装置が当該暗号化処理装置の電源が切断された場合にデータを揮発するものであるか否かを判断するものであることが考えられる。
また，前記記憶形式判別手段は，前記記憶装置が当該暗号化処理装置から取り外された場合にデータを揮発するものであるか否かを判断するものであってもよい。
このように構成されることで，前記記憶装置単体が盗難に遭ったとしても前記データの内容が第３者によって解読される可能性が無く，前記データが機密性の高いデータである場合に非常に有効である。
【０００６】
また，前記要否判断手段は，前記データの形態又は具備する項目に基いて，前記データに対して暗号化が必要か否かを判断するよう構成されることが望ましい。
このように前記要否判断手段が判断することによって，受信したデータの中で暗号化が必要と認められる受信データのみを選択的に暗号化することが可能となり，従来の技術に比べて効率的に前記データの暗号化を実施することが可能となる。また，暗号化が不要なデータについては暗号化されないので，処理の迅速性が維持される。
更に，前記データの形態が既に暗号化されている場合に，前記要否判断手段は前記データに対して暗号化が不必要と判断，又は，前記データの具備する項目が前記データの重要度に関する指標（フラグ，親展指示）である場合に，前記要否判断手段は前記データに対して暗号化が必要と判断，又は，前記データの具備する項目が予め定められた条件である

場合に，前記要否判断手段は前記データに対して暗号化が必要と判断するように構成しても良い。

このように構成することで，上述同様に，前記要否判断手段によって，暗号化が必要と認められる受信データのみを効率良く選択的に暗号化することが可能となる。

【０００７】

前記記憶装置に暗号化して記憶されている前記データを復元するための復元化手段を具備し，該復元化手段によって前記データが復元された後に前記データが出力されるように構成することが望ましい。

このように本発明に復元化手段が設けられることによって，暗号化が必要と認められて暗号化された前記データを自動的に復元化して出力することが可能となる。

【０００８】

また，上述の暗号化処理装置の用途として前記データの受信側の機器に採用されても良く，例えば，本発明の暗号化処理装置をホスト装置とプリンタとで構成される印刷システムに採用することで，暗号化を施すべき文書のみを効率良く印刷出力することが可能となる。

【０００９】

また本発明をシステムとして捉えると，データの作成などのサービスを提供するホスト装置と，該ホスト装置より受信したデータを暗号化して記憶装置に記憶した後に，該データを出力する暗号化処理装置とを具備した暗号化処理システムにおいて，

上記ホスト装置は，データを上記暗号化処理装置に送信する際に，該データに対して暗号化に関する条件を付加する条件付加手段を具備し，

上記暗号化処理装置は，上記記憶装置が揮発性を有するか否かを判別する記憶形式判別手段と，上記記憶形式判別手段による判別結果及び上記条件の有無に基いて，上記データに対して暗号化が必要か否かを判断するための要否判断手段と，を具備し，上記要否判断手段によって暗号化が必要と判断された場合に上記データを暗号化処理装置側で暗号化することを特徴とする暗号化処理システムとして構成されている。

本発明がこのように構成されているので，暗号化処理装置の要否判断手段は，上記ホスト装置側で付加された暗号化に関する条件がデータに付加されているか否かを容易に判断できるので，受信したデータの中で暗号化が必要と認められるデータのみを暗号化することが可能となる。

また，第３者によって前記記憶装置が盗難にあった場合のデータの読み出しの可能性が判別できるので，例えば，前記記憶装置のデータの保存性が低ければ盗難時にデータが消滅するので，データに対して暗号化する必要が無くなり，不要な暗号化を防止できる。

【００１０】

【発明の実施の形態】

以下添付図面を参照しながら，本発明の実施の形態及び実施例について説明し，本発明の理解に供する。尚，以下の実施の形態及び実施例は，本発明を具体化した一例であって，本発明の技術的範囲を限定する性格のものではない。

ここに，図１は本発明の実施の形態に係る暗号化処理装置を採用するプリンタＡの概略構成図，図２は本発明の実施の形態に係る暗号化処理装置を採用するプリンタＡが行う一連の処理手順を示すフローチャート，図３は図２のステップＳ２０のサブルーチンの一連の処理手順を示すフローチャート，図４は図２のステップＳ５０のサブルーチンの一連の処理手順を示すフローチャート，図５は図２のステップＳ５０のサブルーチンの別例の一連の処理手順を示すフローチャート，図６はプリンタＡが行う復元処理を示すフローチャート，図７はホスト装置Ｂが行う条件付加の処理を示すフローチャートである。

【００１１】

先ず図１を用いて，本発明の実施の形態に係る暗号化処理装置を採用する機器の一例としてプリンタＡの概略構成について説明する。

もちろん，本発明の暗号化処理装置は，上記プリンタＡのみに限定されて採用されるものではなく，本発明の暗号化処理装置を採用することで同様の効果が得られるものであれ

ば如何なるものに採用しても良い。

【００１２】

プリンタＡは，要否判断機能，記憶形式判別機能，復元化機能を具備すると共に外部機器（ホスト装置Ｂ）より送出される暗号化の必要なデータを暗号化するネットワークカード１０（以下，「ＮＩＣ１０」と称する。）と，ＮＩＣ１０で受信したデータ等に画像処理などの各種処理を施すイメージコントローラユニット２０（以下，「ＩＣＵ２０」と称する。）と，ＮＩＣ１０で受信したデータの記憶やプリンタＡの動作プログラムの展開等がなされるＨＤＤ３０（記憶不揮発性）やＲＡＭ４０（記憶揮発性）と，ＮＩＣ１０若しくはＩＣＵ２０で処理されたデータをシート材に画像形成を行うことによって出力する画像形成部７０の制御を行うプリンタコントローラユニット６０（以下，「ＰＣＵ６０」と称する。）と，ユーザがプリンタＡに対して操作，入力を行うための操作部５０とを具備して構成されている。

ここで，上記要否判断機能，上記記憶形式判別機能，上記復元化機能について説明する。

【００１３】

上記要否判断機能とは，ホスト装置Ｂより受信したデータに対して暗号化が必要か否かを判断する機能であって，プログラム或いは回路によって実現されるものである。これらのプログラム又は回路が要否判断手段の一例である。

上記記憶形式判別機能とは，ＨＤＤ３０，ＲＡＭ４０などの記憶装置が，どのようにしてデータを記憶するのか，或いは，記憶したデータに対して揮発性若しくは不揮発性の特性を有するのか等の記憶形式を判別する機能であって，プログラム或いは回路によって実現されるものである。これらのプログラム又は回路が記憶形式判別手段の一例である。

上記復元化機能とは，暗号化された暗号化データをＰＣＵ６０を介して画像形成部７０で印刷出力可能なように上記暗号化データを復元する機能であって，プログラム或いは回路によって実現されるものである。これらのプログラム又は回路が復元化手段の一例である。

また，上述において，上記３つの手段はＮＩＣ１０によって具備されるものとしたが，もちろんＮＩＣ１０に限定されて具備されるものでなく，独立してプリンタＡ内部に存在しても良い。

【００１４】

次に，図２を用いて，暗号化処理装置を採用するプリンタＡが行う一連の処理について説明する。以下の説明では，主にＮＩＣ１０が判断等の処理を行うものとして説明するが，同様の処理を例えばＩＣＵ２０が行うものとしても良い。

処理はステップＳ１０より開始される。

ＮＩＣ１０は，ホスト装置ＢよりプリンタＡで印刷出力されるデータを受信する（Ｓ１０）。

ステップＳ１０の処理に続いて，ＮＩＣ１０はプリンタＡの記憶装置（ＨＤＤ３０，ＲＡＭ４０）の記憶形式の判別を行う（Ｓ２０）。

このステップＳ２０で行われる処理の詳細を図３を用いて説明する。

【００１５】

先ず，ステップＳ２０の処理が行われる前提について説明する。

このステップＳ２０では記憶装置の記憶形式を判別するのであるが，この場合，上記判別の基準となる記憶装置の型番，記憶形式等の製品データ（揮発性，不揮発性等）が予めＮＩＣ１０若しくはＩＣＵ２０に記憶されており，該製品データと記憶装置のデバイスドライバの情報とに基いて，ＮＩＣ１０若しくはＩＣＵ２０が上記判別を行うものとする。（以下では上述の通りＮＩＣ１０が処理するものとする。）

先ず，上記製品データとデバイスドライバとに基いて，プリンタＡが具備する記憶装置（ＨＤＤ３０，ＲＡＭ４０）のデータ記憶領域の揮発性について判断を行う（Ｓ２１）。つまり，プリンタＡの電源が切断された場合に，記憶装置のデータ記憶領域のデータが揮発するか否かが判断される。この判断で，揮発すると判断された場合はプリンタＡが具備

する記憶装置のデータの保存性が低いと判別され（Ｓ２５），一方，揮発しないと判断された場合は処理がステップＳ２２へ移行する。

次に，上記ステップＳ２１と同様に，上記製品データとデバイスドライバとに基いて，プリンタＡが具備する記憶装置がプリンタＡから取り外された場合に，データ記憶領域のデータが揮発するか否かが判断される（Ｓ２２）。この判断で，揮発すると判断された場合はプリンタＡが具備する記憶装置のデータの保存性が低いと判別され（Ｓ２５），一方，揮発しないと判断された場合は処理がステップＳ２３へ移行する。

更に，上記ステップＳ２１，２２同様に，上記製品データとデバイスドライバとに基いて，プリンタＡが具備する記憶装置がプリンタＡから取り外された場合に，データ記憶領域のデータが第３者によって読み込み不能な形式のデータに変換するか否かが判断される（Ｓ２３）。この判断で，変換すると判断された場合はプリンタＡが具備する記憶装置のデータの保存性が低いと判別され（Ｓ２５），一方，変換しないと判断された場合はデータの保存性が高いと判断される（Ｓ２４）。

このようにして，記憶装置の記憶形式がデータの保存性の高いものであるか否かが判別される。

【００１６】

上記ステップＳ２０の該判別結果に基いて，ＮＩＣ１０は上記データに対して暗号化が必要か否かの判断を行う（Ｓ３０）。

つまり，上記ステップＳ３０で行われる処理は，上記ステップＳ２０において，記憶装置の記憶形式が保存性の低い形式であると判別された場合は，データに対して暗号化が不必要という判断がなされ，一方，上記ステップＳ２０において，記憶装置に記憶形式が保存性の高い形式であると判別された場合は，データに対して暗号化が必要があると判断するものである。

そして，データに対して暗号化が不必要と判断された場合は，処理がステップＳ８０へ移行してデータがＨＤＤ３０又はＲＡＭ４０に記憶される（Ｓ８０）。一方，データに対して暗号化が必要と判断された場合は，処理がステップＳ４０へ移行する。

【００１７】

ここで，図２で示すフローチャートのステップＳ４０以降の説明に先立って，ホスト装置Ｂで行われる前提となる処理について図７を用いて説明する。

ユーザによって，ホスト装置Ｂ側で作成されたデータの印刷指示がホスト装置Ｂに入力される（Ｓ２１０）。

つまり，このステップＳ２１０の印刷指示の入力時に，ユーザによって「データをホスト装置Ｂで暗号化するか」，「データをプリンタＡで暗号化するか」，「データに親展，重要度等のフラグを付すか」等の暗号化に関する条件の入力が行われる。この条件の入力は，ホスト装置Ｂが具備する条件付加手段によって行われる。具体的には，上記条件の選択又は指定を行うための表示が，ユーザがデータ入力を行っているホスト装置Ｂの端末機（不図示）の画面上に，ＧＵＩ（Ｇｒａｐｈｉｃａｌ　Ｕｓｅｒ　Ｉｎｔｅｒｆａｃｅ）でアイコンやウインドウ形式で容易に入力できるように表示されることで，上記条件の入力が行われる。

次に，ホスト装置Ｂは，上記ステップＳ２１０におけるユーザの入力に基いて，データをホスト装置Ｂで暗号化するか否かの判断をする（Ｓ２２０）。

ステップＳ２２０の判断で暗号化すると判断された場合は，上記データをホスト装置Ｂ側で暗号化し，該暗号化がされたことを示す暗号化フラグを該暗号化されたデータに付す（Ｓ２３０）。そして，ホスト装置Ｂは上記暗号化されたデータをプリンタＡに送信する（Ｓ２６０）。

一方，上記ステップＳ２２０で，データをホスト装置Ｂで暗号化しないと判断された場合は，処理がステップＳ２４０に移行する。

ホスト装置Ｂは，上記ステップＳ２１０でユーザによって入力された印刷指示の中に，上記印刷に関わる条件が入力されているか否かを判断する（Ｓ２４０）。このステップＳ２４０で，上記印刷に関わる条件が入力されていると判断された場合に，ホスト装置Ｂは

その旨を示した指標を上記データに対して付す（Ｓ２５０）。そして，ホスト装置Ｂは上記指標が付されたデータをプリンタＡに送信する（Ｓ２６０）。

一方，ステップＳ２４０で，上記暗号化に関する条件が入力されてないと判断された場合は，データに対してホスト装置Ｂ側で何も手を加えずにプリンタＡに送信する（Ｓ２６０）。

このように，ホスト装置ＢよりプリンタＡに送信されるデータには，プリンタＡにおいてデータを暗号化するか否かを判断する際の判断基準となる指標がデータに付加される。つまり，上記指標等に基いて，プリンタＡは以下でデータを暗号化するか否かの判断を行う。

【００１８】

図２のステップＳ４０において，ＮＩＣ１０は，受信したデータの形態が既に暗号化されているものか否かを判断し（Ｓ４０），暗号化されていると判断した場合は，上記データをＨＤＤ３０又はＲＡＭ４０に記憶する（Ｓ８０）。

一方，上記ステップＳ４０で，上記データが暗号化されていない形態と判断された場合は，処理がステップＳ５０へ移行する。

また，上記ステップＳ４０におけるデータが暗号化されているか否かの判断は，例えば，データが上述の暗号化フラグを具備しているか否かを判断することで可能となる。

【００１９】

ステップＳ５０では，ＮＩＣ１０によって上記データが具備する項目，即ち重要度に関する指標に基いて，該データの重要度が判別される（Ｓ５０）。

このステップＳ５０で行われる処理の詳細は図４に示すようになる。

先ず，上記データに対してデータの保存を指示するような指標の一例であるフラグが付されているか否かを判断する（Ｓ５１）。

上記ステップＳ５１で，上記データに上記フラグが付されてないと判断された場合は，上記データは保存する必要が無い，即ち上記データは揮発しても構わないという程度の重要度しか無いもの（重要度低）と判断される（Ｓ５５）。

一方，上記ステップＳ５１で，上記フラグが付されていると判断された場合は，処理がステップＳ５２に移行して，親展フラグが付されているか否かが判断される（Ｓ５２）。

上記ステップＳ５２で，上記データに上記親展フラグが付されていないと判断された場合は，重要度が低いと判断され（Ｓ５５），一方上記親展フラグが上記データに付されている場合は，上記データは重要度が高いと判断される（Ｓ５４）。

このように判断がなされることで，データの保存指示と親展フラグとが共にデータに付されている場合に，該データは重要度が高いと判別される。

ここで，再び図２を用いて説明する。

【００２０】

上記ステップＳ５０におけるデータの重要度（重要度高い（Ｓ５４），重要度低い（Ｓ５５））判別結果に基いて，ＮＩＣ１０は上記データに対して暗号化が必要か否かの判断を行う（Ｓ６０）。

つまり，上記ステップＳ６０で行われる処理は，上記ステップＳ５０で重要度が低いと判別されたデータに対しては暗号化の必要が無いと判断し，一方上記ステップＳ５０で重要度が高いと判別されたデータに対しては暗号化の必要があると判断するものである。

そして，上記データに対して暗号化が不必要と判断された場合は，処理がステップＳ８０へ移行してデータがＨＤＤ３０又はＲＡＭ４０に記憶される（Ｓ８０）。一方，上記データに対して暗号化が必要と判断された場合は，処理がステップＳ７０へ移行して暗号化が施される（Ｓ７０）。

そして，ステップＳ７０で暗号化された暗号化データをＨＤＤ３０又はＲＡＭ４０に記憶する（Ｓ８０）。

プリンタＡにおいて，受信したデータを暗号化するか否かの判断の処理が，上述のように行われることで，暗号化が必要と認められるデータのみを暗号化することが可能となり，効率良く上記データを記憶装置に一旦記憶して出力することが可能となる。

【００２１】
また，上述の処理で暗号化された後に記憶装置（ＨＤＤ３０，ＲＡＭ４０）に記憶されたデータをプリンタＡより出力する処理について，図６を用いて以下に説明する。
ＮＩＣ１０は，ユーザによって操作部５０に出力指示が入力されたか否かを判断する（Ｓ９０）。
そして，上記入力がなされた場合に，ステップＳ７０で暗号化されたデータが復元されて印刷出力される（Ｓ１００）。
また，上記ステップＳ９０において，上記出力指示の入力の際にデータのパスワードやＩＤを入力することによって，該データを印刷出力するようにしても良く，このようにすることで更に該データの安全性が高められる。
【００２２】
【実施例】
上記実施の形態におけるステップＳ５０の「データの重要度判別」の処理の替わりに，データが予め定められた条件を具備するか否かを判別する処理（Ｓ５０ａ）を行っても良い。
もちろんこの場合も，ホスト装置Ｂにおいて，予め定められた条件が図７のステップＳ２１０でユーザによって入力されているとする。
この判別を行う一連の処理を図５を用いて説明する。
ＮＩＣ１０は，データが，予め定められた条件の１つである「ジョブ名称」を具備するか否かの判断を行う（Ｓ５１ａ）。
ステップＳ５１ａで，データが「ジョブ名称」を具備すると判断された場合は，上記データが上記条件を具備するものであると判別する（Ｓ５４ａ）。
一方，ステップＳ５１ａで，データが「ジョブ名称」を具備しないと判断された場合は，処理がステップＳ５２ａへ移行する。
ここで，上記「ジョブ名称」とは，例えば，会社組織における職制上の役職名のことである。つまり，一般的に，役職をもった人ほど仕事上の責任が増加すると共に扱う文書やそのデータの機密性も高まるといえるので，データが上記「ジョブ名称」を具備するものか否かを判別した結果が，図２のステップＳ６０において，データに対して暗号化が必要か否かの判断を行う際の判断基準となる。
【００２３】
続いて，ステップＳ５２ａでは，データが，予め定められた条件の１つである「暗号化の指示」を具備するか否かの判断がなされる（Ｓ５２ａ）。
この「暗号化の指示」とは，例えば，データの内容が機密事項を含むものであることを示すフラグのようなものであり，該フラグが上記データに具備されているか否かを上記ステップＳ５２ａで判別した結果が，上述同様に図２のステップＳ６０において，データに対して暗号化が必要か否かの判断を行う際の判断基準となる。
上記ステップＳ５２ａで，上記データが上記「暗号化の指示」を具備しないと判断された場合は，上記データが上記条件を具備しないものと判別される（Ｓ５５ａ）。一方，上記データが上記「暗号化の指示」を具備すると判断された場合は，上記条件を具備しないものと判別される（Ｓ５４ａ）
続いて，図２のステップＳ６０の処理が行われ，上記データが上記条件を具備しない場合は，上記データに対して暗号化が不必要と判断され，一方上記データが上記条件を具備する場合は，上記データに対して暗号化が必要を判断される（Ｓ６０）。
以降の処理は上記実施の形態と同様の処理が実行される。
このように，ステップＳ５０「データの重要度判別」に替えて，ステップＳ５０ａとしてデータが予め定められた条件を具備するか否かを判別する処理を実行することで，ステップＳ６０で行う判断の判断基準を定めることが可能となる。
【００２４】
【発明の効果】
本発明は，受信したデータを暗号化して記憶装置に記憶した後に，該データを出力する

暗号化処理装置において，
上記記憶装置が揮発性を有するか否かを判別する記憶形式判別手段と，上記記憶形式判別手段による判別結果に基づいて上記データに対して暗号化が必要か否かを判断するための要否判断手段と，を具備し，上記要否判断手段によって暗号化が必要と判断された場合に上記データを暗号化することを特徴とする暗号化処理装置として構成されている。
本発明がこのように構成されているので，第３者によって前記記憶装置が盗難にあった場合のデータの読み出しの可能性が判別できるので，例えば，前記記憶装置のデータの保存性が低ければ盗難時にデータが消滅するので，データに対して暗号化する必要が無くなり，不要な暗号化を防止できる。
【００２５】
具体的には，前記記憶形式判別手段が，前記記憶装置が当該暗号化処理装置の電源が切断された場合にデータを揮発するものであるか否かを判断するものであることが考えられる。
また，前記記憶形式判別手段は，前記記憶装置が当該暗号化処理装置から取り外された場合にデータを揮発するものであるか否かを判断するものであってもよい。
このように構成されることで，前記記憶装置単体が盗難に遭ったとしても前記データの内容が第３者によって解読される可能性が無く，前記データが機密性の高いデータである場合に非常に有効である。
【００２６】
また，前記要否判断手段は，前記データの形態又は具備する項目に基いて，前記データに対して暗号化が必要か否かを判断するよう構成されることが望ましい。
このように前記要否判断手段が判断することによって，受信したデータの中で暗号化が必要と認められる受信データのみを選択的に暗号化することが可能となり，従来の技術に比べて効率的に前記データの暗号化を実施することが可能となる。また，暗号化が不要なデータについては暗号化されないので，処理の迅速性が維持される。
更に，前記データの形態が既に暗号化されている場合に，前記要否判断手段は前記データに対して暗号化が不必要と判断，又は，前記データの具備する項目が前記データの重要度に関する指標（フラグ，親展指示）である場合に，前記要否判断手段は前記データに対して暗号化が必要と判断，又は，前記データの具備する項目が予め定められた条件である場合に，前記要否判断手段は前記データに対して暗号化が必要と判断するように構成しても良い。
このように構成することで，上述同様に，前記要否判断手段によって，暗号化が必要と認められる受信データのみを効率良く選択的に暗号化することが可能となる。
【００２７】
前記記憶装置に暗号化して記憶されている前記データを復元するための復元化手段を具備し，該復元化手段によって前記データが復元された後に前記データが出力されるように構成することが望ましい。
このように本発明に復元化手段が設けられることによって，暗号化が必要と認められて暗号化された前記データを自動的に復元化して出力することが可能となる。
【００２８】
また，上述の暗号化処理装置の用途として前記データの受信側の機器に採用されても良く，例えば，本発明の暗号化処理装置をホスト装置とプリンタとで構成される印刷システムに採用することで，暗号化を施すべき文書のみを効率良く印刷出力することが可能となる。
【００２９】
また本発明をシステムとして捉えると，データの作成などのサービスを提供するホスト装置と，該ホスト装置より受信したデータを暗号化して記憶装置に記憶した後に，該データを出力する暗号化処理装置とを具備した暗号化処理システムにおいて，
上記ホスト装置は，データを上記暗号化処理装置に送信する際に，該データに対して暗号化に関する条件を付加する条件付加手段を具備し，

上記暗号化処理装置は，上記記憶装置が揮発性を有するか否かを判別する記憶形式判別手段と，上記記憶形式判別手段による判別結果及び上記条件の有無に基いて，上記データに対して暗号化が必要か否かを判断するための要否判断手段と，を具備し，上記要否判断手段によって暗号化が必要と判断された場合に上記データを暗号化処理装置側で暗号化することを特徴とする暗号化処理システムとして構成されている。

本発明がこのように構成されているので，暗号化処理装置の要否判断手段は，上記ホスト装置側で付加された暗号化に関する条件がデータに付加されているか否かを容易に判断できるので，受信したデータの中で暗号化が必要と認められるデータのみを暗号化することが可能となる。

また，第３者によって前記記憶装置が盗難にあった場合のデータの読み出しの可能性が判別できるので，例えば，前記記憶装置のデータの保存性が低ければ盗難時にデータが消滅するので，データに対して暗号化する必要が無くなり，不要な暗号化を防止できる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る暗号化処理装置を採用するプリンタＡの概略構成図。

【図２】本発明の実施の形態に係る暗号化処理装置を採用するプリンタＡが行う一連の処理手順を示すフローチャート。

【図３】図２のステップＳ２０のサブルーチンの一連の処理を示すフローチャート。

【図４】図２のステップＳ５０のサブルーチンの一連の処理を示すフローチャート。

【図５】図２のステップＳ５０のサブルーチンの別例の一連の処理を示すフローチャート。

【図６】プリンタＡが行う復元処理を示すフローチャート。

【図７】ホスト装置Ｂが行う条件付加の処理を示すフローチャート。

【符号の説明】

Ａ……プリンタ（暗号化処理装置採用）

Ｂ……ホスト装置

１０……ＮＩＣ

２０……ＩＣＵ

３０……ＨＤＤ（不揮発性）

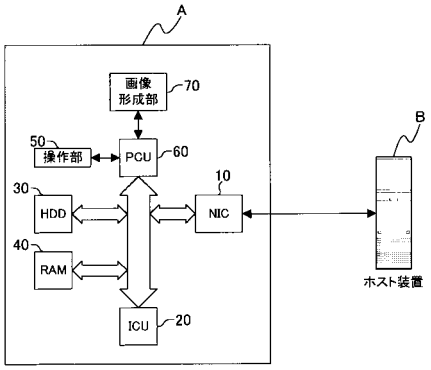
４０……ＲＡＭ（揮発性）

５０……操作部

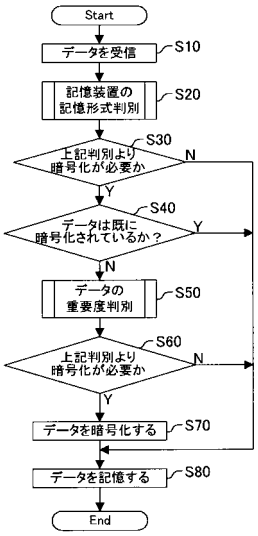
６０……ＰＣＵ

７０……画像形成部

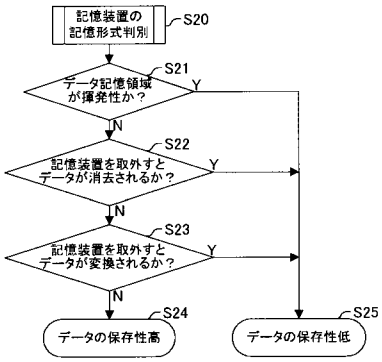
【図１】


A
画像形成部
70
50
操作部
PCU
60
10
30
HDD
NIC
40
RAM
ICU
20
B
ホスト装置

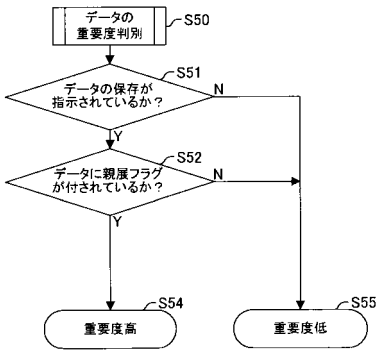
【図２】


Start
データを受信
S10
記憶装置の記憶形式判別
S20
上記判別より暗号化が必要か
S30
N
Y
データは既に暗号化されているか？
S40
Y
N
データの重要度判別
S50
上記判別より暗号化が必要か
S60
N
Y
データを暗号化する
S70
データを記憶する
S80
End

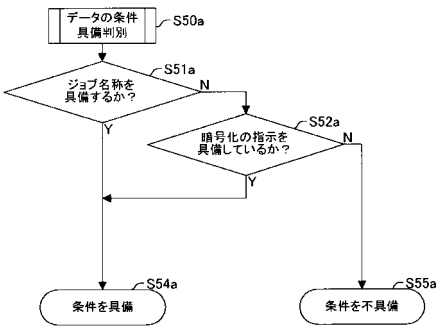
【図３】


記憶装置の記憶形式判別
S20
データ記憶領域が揮発性か？
S21
Y
N
記憶装置を取外すとデータが消去されるか？
S22
Y
N
記憶装置を取外すとデータが変換されるか？
S23
Y
N
データの保存性高
S24
データの保存性低
S25

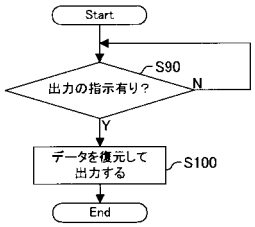
【図４】


データの重要度判別
S50
データの保存が指示されているか？
S51
N
Y
データに親展フラグが付されているか？
S52
N
Y
重要度高
S54
重要度低
S55

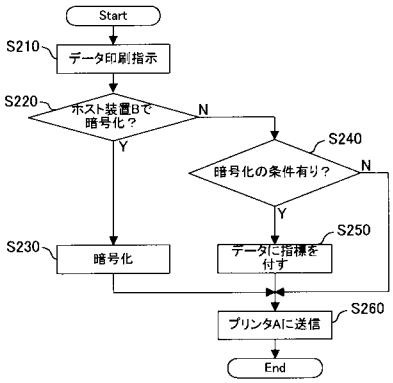
【図５】


データの条件具備判別
S50a
ジョブ名称を具備するか？
S51a
N
Y
暗号化の指示を具備しているか？
S52a
N
Y
条件を具備
S54a
条件を不具備
S55a

【図６】


Start
S90
出力の指示有り？
N
Y
データを復元して
出力する
S100
End

【図７】


Start
S210
データ印刷指示
S220
ホスト装置Bで
暗号化？
N
Y
S240
暗号化の条件有り？
N
Y
S230
暗号化
S250
データに指標を
付す
S260
プリンタAに送信
End

フロントページの続き

(56)参考文献 特開平０５－２７３９１８（ＪＰ，Ａ）
特開平０９－１０１８６９（ＪＰ，Ａ）
特開平１１－２２７２９８（ＪＰ，Ａ）
特開平１０－０４２１４７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/24
H04L 9/10