(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4337967号
(P4337967)

(45)発行日　平成21年9月30日(2009.9.30)　(24)登録日　平成21年7月10日(2009.7.10)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	560D
G06F 21/20	(2006.01)	G06F	15/00	330G
B41J 5/30	(2006.01)	B41J	5/30	Z
B41J 29/38	(2006.01)	B41J	29/38	Z
G06F 1/00	(2006.01)	G06F	1/00	370E

請求項の数 3　(全 11 頁)　最終頁に続く

(21)出願番号　特願2002-123203 (P2002-123203)
(22)出願日　平成14年3月22日 (2002.3.22)
(65)公開番号　特開2003-281100 (P2003-281100A)
(43)公開日　平成15年10月3日 (2003.10.3)
審査請求日　平成17年2月10日 (2005.2.10)

(73)特許権者　591234204
株式会社ローレルインテリジェントシステムズ
東京都港区虎ノ門１丁目１番１０号
(72)発明者　鵜養　剛
神奈川県横浜市青葉区美しが丘５丁目３５番地の２株式会社ローレルインテリジェントシステムズ内
(72)発明者　鳥飼　将迪
神奈川県横浜市青葉区美しが丘５丁目３５番地の２株式会社ローレルインテリジェントシステムズ内

最終頁に続く

(54)【発明の名称】セキュリテイネットワークシステム

(57)【特許請求の範囲】

【請求項１】

ネットワークシステムに接続される端末機器である、読取り部を有するパーソナルコンピュータ及びプリンタの前記読取り部に着脱可能なキーデバイスにおいて、

前記キーデバイスが、コンピュータ機能と、蓄電機能とを備え、

前記パーソナルコンピュータの前記読取り部に装着された前記キーデバイスが、

当該パーソナルコンピュータから前記キーデバイスに入力されたパスワードを前記コンピュータ機能で認証し、

この認証されたパスワードにより、前記コンピュータ機能でパスワードキーを生成し、

この生成されたパスワードキーにより、前記コンピュータ機能で画像及び文書情報の暗号化、復号化キーを生成し、

前記暗号化、復号化キーの生成後、前記キーデバイス内の前記パスワードを前記コンピュータ機能で消滅させる前記キーデバイスであって、かつ、

前記キーデバイスが、前記パスワードが前記キーデバイス内に入力されてから消滅されるまでの間に、前記読取り部から抜き取られると、前記蓄電機能による電気エネルギーにより前記コンピュータ機能で、前記パスワードの消滅を行い、前記キーデバイスが、前記読取り部への装着前の状態に初期化されることを特徴とするキーデバイス。

【請求項２】

ネットワークシステムに接続される端末機器である、読取り部を有するパーソナルコンピュータ及びプリンタと、

前記読取り部に脱着可能なキーデバイスと、を有し、
前記キーデバイスが前記端末機器の何れかの読取り部に装着されるネットワークシステムでのパスワードの認証消滅方法において、
前記キーデバイスが、コンピュータ機能と、蓄電機能とを備え、前記パーソナルコンピュータの前記読取り部に装着され、
当該パーソナルコンピュータから前記キーデバイスに入力されたパスワードを前記コンピュータ機能で認証する認証ステップと、
前記認証ステップで認証されたパスワードにより、前記コンピュータ機能でパスワードキーを生成するパスワードキー生成ステップと、
前記生成ステップで生成されたパスワードキーにより、前記コンピュータ機能で画像及び文書情報の暗号化、復号化キーを生成する暗号化、復号化キー生成ステップと、
前記暗号化、復号化キーの生成後、前記キーデバイス内の前記パスワードを前記コンピュータ機能で消滅させるパスワード消滅ステップと、
を有し、かつ、
前記キーデバイスが、前記パスワードが前記キーデバイス内に入力されてから消滅されるまでの間に、前記読取り部から抜き取られると、前記蓄電機能による電気エネルギーにより前記コンピュータ機能で、前記パスワードの消滅を行い、前記キーデバイスが、前記端末機器への装着前の状態に初期化されることを特徴とするパスワードの認証消滅方法。
【請求項３】
請求項２記載のパスワードの認証消滅方法において、
前記プリンタにＯＮ、ＯＦＦ可能なスイッチ機能を有するボタンを備え、前記ボタンのＯＮ，ＯＦＦによりパスワードの入力が行えるようにしたことを特徴とするパスワードの認証消滅方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はＰＣ、プリンタ、ファクシミリなどで構成されるネットワークシステムにおいて、機密保持のため、ＰＣで暗号化された画像／文書データをネットワークを介してプリンタ等の端末に送り、出力する場合のＩＤの認証、パスワードの認証、暗号化／復号化に関する技術。
【０００２】
【従来の技術】
ＰＣ、プリンタなどが接続されているネットワーク環境においては現在、機密の漏洩が問題になっている。ネットワークに接続されているＰＣで作成した情報、ファイルの情報などネットワーク上に存在する画像／文書データがこれにつながる複数のプリンタなどの出力機器から不正に出力されたり、また、ファイルなどに蓄積されている情報の抜き取り、パソコンのハードディスクやパソコンの盗難によるものなど種々の形で漏洩する。これらを回避するため機密を要する情報の取り扱い方法として、ＰＣやネットワーク上の画像／文書データを暗号化して取り扱い、必要時に復号化する方法が紹介されている。この暗号化／復号化に要するキー情報の扱いも種々の方法が提案されている。またＩＤ、パスワードなどで個人を認証し、この個人以外は情報にアクセスすることが出来ない様にすることで機密を保持する方法も公知である。
【０００３】
上記キー情報と個人認証の方法を組み合わせた手法も紹介されている。一例として特開平６－１２４１７８を引用する。図１、はこの発明のシステム構成を示したもの、図２は処理のフローを示した図である。プリントデータ生成装置１にはプリントデータを暗号化すると共に、暗号化データにユーザーＩＤ、キーコード、暗号化ＩＤを付加してプリンタ側に転送する暗号化データ生成部Ａ１２がある。プリンタには上記ＩＤ等に基づいて、上記暗号化データを解読する暗号化データ解読部Ａ２３がある。プリンタに転送された暗号化データは一旦、スプールキューＡ２２に格納し、プリントする際には、パスワードが一致

した時のみ、暗号化データ解読部Ａ２３で暗号解読しながら出力する。スプールキューＡ２２に格納されるのは、暗号化データのみであるので、その内容を覗き見されたとしても、見えるのは意味のないデータであるので、プリントデータの内容は知られないですむ。というものである。

【０００４】

また、特開２００１－１８６３５８には目的受信者が所有するカード内のキーと、目的画像出力機器チップ内部に保持されたキー、及び暗号方式を組み合わせ、目的受信者が目的画像出力機器より確実に画像を安全送信して生成するシステムが紹介されている。これは画像生成のためのデータの暗号化をつかさどる第一の秘密キー／公開キーは、この秘密キーが目的受信者によって所有され、前記の秘密キー／公開キーの秘密キーが目的画像出力機器で保有され、この二つのキーにより、２回にわたって暗号化されている。従って復号化の場合もこの二つの秘密キーによる第一のキーの復号化が必要となる。

【０００５】

しかし、特開２００１－１８６３５８では個人の情報をカードなどのデバイスに入れた場合、紛失した時や盗難に合った時の不正使用を防止できない。これを防止するため特開平６－１２４１７８の様に個人情報とパスワードの一致により、個人を特定する方法がある。この場合にはパスワードの入力機器及びネットワーから容易にパスワードが漏れる恐れがある。照合用に機器の内部に格納してある照合手段からも解析されて漏れる可能性がある。ネットワークシステムにおいては、上記の様にセキュリテイ上の弱点があってはならない。

【０００６】

【発明が解決しようとする課題】

画像／文書データを取り扱うネットワークシステムで機密漏洩防止のため、暗号化／復号化を行う場合、暗号化／復号化のキー情報、ＩＤ、パスワード、の関連性を考慮した上で、キーデバイスの不正使用、パスワードの漏洩、ＩＤ情報の漏洩などシステムの弱点をカバーした情報漏洩の心配のない手段が求められる。

【０００７】

【課題を解決するための手段】

請求項１に記載の発明は、ネットワークシステムに接続される端末機器である、読取り部を有するパーソナルコンピュータ及びプリンタの前記読取り部に着脱可能なキーデバイスにおいて、前記キーデバイスが、コンピュータ機能と、蓄電機能とを備え、前記パーソナルコンピュータの前記読取り部に装着された前記キーデバイスが、当該パーソナルコンピュータから前記キーデバイスに入力されたパスワードを前記コンピュータ機能で認証し、この認証されたパスワードにより、前記コンピュータ機能でパスワードキーを生成し、この生成されたパスワードキーにより、前記コンピュータ機能で画像及び文書情報の暗号化、復号化キーを生成し、前記暗号化、復号化キーの生成後、前記キーデバイス内の前記パスワードを前記コンピュータ機能で消滅させる前記キーデバイスであって、かつ、前記キーデバイスが、前記パスワードが前記キーデバイス内に入力されてから消滅されるまでの間に、前記読取り部から抜き取られると、前記蓄電機能による電気エネルギーにより前記コンピュータ機能で、前記パスワードの消滅を行い、前記キーデバイスが、前記読取り部への装着前の状態に初期化されることを特徴とする。

請求項２に記載の発明は、ネットワークシステムに接続される端末機器である、読取り部を有するパーソナルコンピュータ及びプリンタと、前記読取り部に脱着可能なキーデバイスと、を有し、前記キーデバイスが前記端末機器の何れかの読取り部に装着されるネットワークシステムでのパスワードの認証消滅方法において、前記キーデバイスが、コンピュータ機能と、蓄電機能とを備え、前記パーソナルコンピュータの前記読取り部に装着され、当該パーソナルコンピュータから前記キーデバイスに入力されたパスワードを前記コンピュータ機能で認証する認証ステップと、前記認証ステップで認証されたパスワードにより、前記コンピュータ機能でパスワードキーを生成するパスワードキー生成ステップと、前記生成ステップで生成されたパスワードキーにより、前記コンピュータ機能で画像及

び文書情報の暗号化、復号化キーを生成する暗号化、復号化キー生成ステップと、前記暗号化、復号化キーの生成後、前記キーデバイス内の前記パスワードを前記コンピュータ機能で消滅させるパスワード消滅ステップと、を有し、かつ、前記キーデバイスが、前記パスワードが前記キーデバイス内に入力されてから消滅されるまでの間に、前記読取り部から抜き取られると、前記蓄電機能による電気エネルギーにより前記コンピュータ機能で、前記パスワードの消滅を行い、前記キーデバイスが、前記端末機器への装着前の状態に初期化されることを特徴とする。

請求項３に記載の発明は、請求項２記載の発明において、前記プリンタにＯＮ，ＯＦＦ可能なスイッチ機能を有するボタンを備え、前記ボタンのＯＮ，ＯＦＦによりパスワードの入力が行えるようにしたことを特徴とする。

本発明ではネットワークに接続された管理サーバー、ネットワーク管理装置、クライアントＰＣ（以下、パーソナルコンピュータをいう。）プリンタ、ファックス等により構成されるネットワーク環境において、ＩＤ、パスワードの運算／認証手段により認証後、画像／文書データの暗号化／複号化キーが生成される。これらはＣＰＵとメモリーを持ち、コンピュータ機能を有するキーデバイス内に暗号化した形で入れ、人が操作する端末機器にはすべてこのキーデバイスの読取り装置を設ける。このネットワークで作業するにはまず、端末機器の読取り装置にキーデバイスを挿入する。クライアントＰＣからキーデバイスのパスワードをキーパットから入力する。次にキーデバイス内でパスワードを認証する。パスワードの入力は連続して予め定められた回数間違うとキーデバイスは自動ロックする。キーデバイス内の認証情報は暗号化したまま管理サーバーに送られる。認証情報は予めネットワーク管理装置の持つ基本キーにより、暗号化されている。ネットワークサーバーではネットワーク管理装置の持つ基本キーと予め登録されている認証情報により、サーバー内で認証される。認証されればネットワークへのログインが可能となる。

【０００８】

パスワードは、一例として８桁の数値を用い、入力が６回間違うと無効となり、キーデバイスの機能が不能になる。端末にパスワードが入力されると端末に装着されているキーデバイスにパスワードが送られその内部で認証が行はれる。キーデバイス内部でこのパスワードはある関数の形式になっていて、照合には運算を必要とする。例えば、入力されるパスワードをｘ、正規のパスワードx_1を８桁の正の整数、フィルターとの照合を何回目で行うかを示す数をｎとし、パスワード関数をｙ＝ｆ（ｘ，$_n$）：式１とする。パスワードｘ、回数ｎを決めれば各回のパスワード関数の値は決定する。フィルターＦは照合をａ回目、ｂ回目で行うこととし、Ｆａ＝ｆ（ｘ，ｎ）－１：式１、Ｆｂ＝ｆ（ｘ，ｎ）＋１：式２で構成すると、フィルターの値も決定する。例えば２回目でＦａ＜ｙが成立すること、及び、５回目でｙ＜Ｆｂが成立するようにフィルターＦを構成すれば、この二つの式を満足するのはｙ即ち、ｆ（ｘ，ｎ）だけとなり、ｘがx_1と認定される。x_1は予め決めるので、何回目で照合するかを決めことにより、各回のフィルターの数値が決定される。例えばフィルターＦａ，Ｆｂを２回目、５回目に設定しする。これ以外はダミーのフィルターＦｄを設定すれば良い。ダミーフィルターＦｄは０＜Ｆｄ＜ｆ（ｘ、ｎ）－ｐ：式３およびｆ（ｘ，ｎ）＋ｐ＜Ｆｄ＜１０００００００：式４で構成する。ｐは１以上の正の整数である。上記の方法でパスワードの照合を行うが、簡単に照合の例を示すと次のようになる。ｙ＝２ｎｘでx_1＝１２３４５６７８とし、フィルターＦａを２回目、及びＦｂを５回目の所に設定する。パスワード関数ｙは２回目で２×２×１２３４５６７８＝４９３８２７１２となり２回目のフィルターＦａは２×２×１２３４５６７８－１で４９３８２７１１となり、５回目のパスワード関数ｙは、２×５×１２３４５６７８＝１２３４５６７８０となる。５回目のフィルターＦｂは１２３４５６７８１となる。２回目でＦａ＝４９３８２７１１＜ｙで５回目でｙ＜Ｆｂ＝１２３４５６７８１を満足する正の整数はx_1以外になく、２回目及び、５回目のフィルターＦａ，Ｆｂにより、パスワードx_1が認定される。ＣＰＵの能力の範囲でｆ（ｘ，ｎ）は複雑な関数にすることも出来、２回の照合時の回数もダミーの関数に混ぜて任意に設定出来る。x_1は認定されると、次のステップである画像／文書データの暗号化／復号化キーを生成したのち、x_1を消去する。不

正使用により、ランダムに入力されるｘは途中で一致しない場合、その後の運算を中止するので、電気信号によるアナライズが行はれても６回のアタックでパスワードx_1を割り出すのは困難である。また、キーデバイスのメモリーに残るダミーを含むフィルターの数字からパスワードを割り出すのも困難である。６回のアタックでx_1が認定されない場合、カードの無効化処理がなされる。パスワード照合の上記の方法は一例であり、上記の方法以外にも種々の方法が考えられる。解析が難解でパスワードの割り出しが困難であれば、他の方法でも良い。

【０００９】

パスワードが認証されればx_1を有効にし、これを元にしたパスワードキーが発行される。次のステップである画像／文書データの暗号化／復号化キーを生成した後x_1を消滅させる。画像、文書データの暗号化／復号化キーはこのパスワードキーにより、生成されてＰＣに渡され、画像／文書データを暗号化する。クライアントＰＣやプリンタなどの端末による復号化の場合も同様の手順で画像／文書データを復号化する。従ってキーデバイスを有する者でパスワードを正しく入力で出来ないと、暗号化／復号化することが出来ない。プリンタなどの出力装置はＵＳＢ、ＲＳ２３２Ｃなどの標準ポートを設け、キーデバイスをここに挿入し、パスワードを入力ことにすることでクライアントＰＣの時と同様の手順で復号化キーを生成することにより画像／文書データを復号化し、プリントアウトが出来る。ネットワーク上のすべての通信データはネットワーク管理装置から出される乱数により、ランダム化されている。本考案はこのように機密が漏洩しないシステムなので、ネットワークが公衆回線や衛星通信を含む大規模のものであっても機密が保持される。

【００１０】

暗号化には、例えばエクスクルーシブＯＲ，バイト置換、換字の組合せからなり、処理単位が可変長バイトであることを特徴とするＳＸＡＬ／ＭＢＡＬとして紹介されているアルゴリズムを使用する。これにより、高速で解読困難な暗号化画像の作成が可能となる。他のアルゴリズムであっても高速で解読困難なものであれば使用可能である。

【００１１】

上記した手順により、プリンタで出力する場合につき更に説明を加える。画像、文書データはクライアントＰＣでジョブ情報が加えられ、暗号化されて印刷データとなる。これに暗号化されているＩＤが付加されてプリンタに送られる。プリンタに送られた情報は記憶装置にストアされる。プリンタにもクライアントＰＣと同様のキーデバイスの読取り装置があり、上記したと同様の手順でキーパットから入力されるパスワードが認証されればパスワードキーがキーデバイス内で発生し、これにより復号化キーを生成し、パスワードは消滅する。復号化キーにより印刷データの復号化を行うと共にジョブ情報を抽出し、プリントアウトすることが可能となる。プリントアウトと同時に暗号化した画像／文書データに出力者のＩＤと、出力日時、枚数がプリンタのロギング装置に記憶されるようにすることができる。プリントアウトを行う場合はクライアントＰＣでプリントアウトの指示をし、一度キーデバイスを抜き取り、ネットワークプリンタのキーデバイスの読取り装置にキーデバイスを挿入しておこなうことになる。

【００１２】

キーデバイスは読取り装置から、異常なタイミングで抜き取られる場合があり、この場合、抜き取られた瞬間に不要情報を消去し、キーデバイスを正常化する必要が生じる。この時の動作について説明する。この作業は例えば抜き取られてから１０ｍｓｅｃ以内に完了し、この電源はキーデバイス内のコンデンサなどの蓄電器から供給される。これにより、キーデバイは読取り装置に挿入前の状態に初期化される。次にプリンタのキーデバイス読取り装置に挿入された場合にも、前記した挿入時の手順でキーデバイスは作動する。キーデバイスは小型の携帯に便利で脱着可能なものであり、ＩＣカードで構成することも出来る。

【００１３】

このように、ネットワーク端末に設けられた読取り装置にこのキーデバイスを挿入し、パスワードを入力するだけで、パスワードの認証、画像／文書データの暗号化／復号化、

ＩＤなどの認証を行う事が出来る。パスワードの入力が正しくなければネットワーク上の情報を暗号化、復号化することが出来ない。また、キーデバイス内の認証情報がサーバーで認証されなければネットワークに入ることが出来ない。これにより、機密の漏洩を防止することが出来る。しかし、このキーデバイスを紛失したり、盗難などにより、当事者以外の人による不正使用の恐れがある。ＰＣはキーボードによりパスワードの入力が可能であるため、前記カードとパスワードの入力を組合わせることにより、不正使用を防止することが出来るが、プリンタなどの端末機器にはパスワードの入力装置がないものが多い。しかし、プリンタにはロギング機能を持たせるようにして、出力者のＩＤが付記されて再度ストアされるようにすることができる。これにより、誰がどのような情報をいつ出力したかというログ情報はプリンタ内部にストアされるようになる。この情報を復号化し出力出来るＩＤ、復号化キーを設定し、このキーデバイスを有する上位管理者などを定めることもできる。このシステムにより、機密保持のレベルを上げることが出来る。プリンタにストアされる情報はこの管理者が消滅させるか。ある一定時間後に自動消滅するか、一定のメモリー内に新しい情報が入った分だけ、古い情報が消滅する方法でも良い。

【００１４】

プリンタにもパスワードの入力装置を持たせる場合について説明する。この為にはテンキーの入力キーを設ければよいが、スペースを必要とするので、テンキーではなく一つのＯＮ、ＯＦＦの機能を有するボタンまたはタッチセンサーを設け数桁の数値を一桁ごとに間隔を置いて押すことにより、パスワードを入力する。例えば３の入力であれば０．２秒以内に３回押し、０．５秒以上間隔をおいて次の数値を入力する。この入力によれば、簡単な装置でパスワードの入力が可能である。パスワードは８桁の数値で構成し、６回正しく入力されなければキーデバイスの機能が無効となるようにする。

【００１５】

一方、プリンタから出力される画像／文書データは復号化されている為、人目に触れることになる。このため、出力中は機密防止上プリンタの所から離れることが出来ない。これは時間のかかる出力の場合非効率である。これを解決する手段としてプリンタのペーパー出力部にカバーを設け、カバーには物理的な鍵があり、プリンタのカードリーダにカードを挿入しなければカバーを開けることが出来ないようにして、ペーパーの情報を見ることも出来ないようにすることができる。この方法により、プリンタにキーデバイスを挿入し、プリントアウトを開始すればキーデバイスを抜いてプリンタのところを離れ、終了後キーデバイスを再び挿入するようにすれば、カバーを開けてプリントを取り出すことが出来るようになる。

【００１６】

ロギング機能のメモリーに記録される情報は圧縮後暗号化されて記録され、この場合、データの容量を削減するため、必要に応じて非可逆、可逆の画像圧縮の方式が用いられるようにしてもよい。例えば絵などのカラー画像と文字が混在する場合、カラー画像は一般に情報量が多く、非可逆でも充分内容が把握出来るため、非可逆の方式を使用、文字情報は詳細な情報も復元する必要があるため可逆の圧縮方式を用いるようにすることができる。また、ストアするデータだけでなくネットワーク上のすべてのデータに特定の色（例えば黒）又は文字のみを暗号化の対照とし、他の色や絵や写真などの画像は通常画像として扱うようにすることによりデータ削減、高速処理を行うことができるようになる。

【００１７】

【発明実施の形態】

本考案を図を用いて詳細に説明する。

図３はキーデバイスを使用したセキュリテイネットワークの概要を示したものである。図３において１はクライアントＰＣで、２はプリンタ、３はプリンタに属するロギング装置、４はネットワークを管理するサーバー、５はネットワークである。これらのネットワークに接続される機器には図に示した様にキーデバイス８の脱着が可能なキーデバイスの読取り手段を持つ。６はネットワークを管理するサーバー４に属するロギング手段、７はネットワーク管理装置、８はキーデバイスでＩＣカードなどのＣＰＵとメモリー等で構成さ

れコンピュータ機能を持つが、ステイック状のキーなどで構成することも出来る。９はサーバー用ディスプレイである。キーデバイス８にはサーバーの持つ基本キーにより暗号化されたＩＤなどの個人認証情報、及びパスワードの運算、認証機能、パスワード認証後に画像、文書データを暗号化／復号化する為のキー生成手段が収められている。キーデバイスの役割としてはクライアントＰＣ、ネットワークへのログイン、本人の認証、ファイルやメールの暗号化／復号化、接続先の管理、ＡＰＬごとのＩＤ／パスワードの管理、プリンタ２内に暗号化ログ保存、プリント出力管理、プリントアウトの取りだし、ＦＤなどの使用可否の管理などである。このキーデバイスがなければネットワークに入る事が出来ない。ＰＣ、または端末機器に接続されているか、内蔵されている読取り装置にキーデバイスを挿入し、端末機器よりパスワードを入力することで、暗号化されたネットワーク環境での作業が可能となる。

【０００１８】

また、ネットワーク上での情報はすべてネットワーク管理装置７から出される乱数によりランダム化した状態で相互の送受信が行はれる。ネットワーク管理装置７には乱数発生手段、個人情報暗号化の基本キーなどが格納されている。この管理装置は物理的にも保護されていて、無理に開けると内容が消滅する。

【００１９】

図４はＰＣで画像／文書データを暗号化してプリンタに送るまでの手順、図５はプリンタ側でＰＣより受け取る暗号化された画像／文書データを復号化してプリントアウトしロギング機能に格納するまでの手順を示したものである。キーデバイスはパスワードの運算、認証機能を有し、認証後に画像／文書データの暗号化キーを生成する。暗号化きーを生成後、パスワードを消去する。一方、キーデバイス内の認証情報は暗号化したままサーバーに送られ、ここで認証され、ネットワークへのログインが可能となる。クライアントＰＣではこの認証後に画像／文書データの暗号化キーをキーデバイスから受け取り、画像／文書データを暗号化し、このデータにジョブ情報を付加し暗号化してあるＩＤと共にランダム化してプリンタに送る。プリンタはＰＣ機能を合わせ持つので、前記したＰＣの場合と手順は同じであるが、画像／文書データ及び、送信者ＩＤを暗号化のまま蓄積し、ＩＣカードが挿入された時点をＰＣ機能で読取り。クライアントＰＣの時と同じ手順でパスワードが入力されキーデバイス内で照合される。また、キーデバイス内の認証情報はサーバーに送られ、認証を受ける。復号化に必要なキーはキーデバイスから得られ、このキーで画像／文書データを複号化してプリントアウトする。プリンタにはロギング機能があり、ペーパーに出力された場合は暗号化されたまま残っている文書／画像データに出力者のこれも暗号化されたＩＤが付記され、出力日時、枚数と共にストアされる。プリンタにストアされている文書、画像データを選択して、復号化し、プリントアウトすることも可能である。このストアされているデータは特別の権限を有する管理者などが特別権限のキーを持つキーデバイスで出力することが出来る。図６は前項の課題を解決するための手段のところで説明したが、一つのボタンスイッチ１０によるパスワードの入力手段、１１は鍵のついたプリントアウト部を被うカバーでキーデバイスの挿入により、鍵が開きプリントアウトペーパーを取り出すことが出来る。キーデバイスを抜くと閉じて鍵によりロックされる。また、図ではキーデバイスの読取りが内蔵されている場合のスリットの挿入口１２を示したが、読取り装置をプリンタのＵＳＢ、ＲＳ２３２Ｃ端子などに接続して使用することも可能である。

【００２０】

【発明の効果】

個人を認定するのに便利で有効なキーデバイスに、これを正規の所有者以外が使用することを防止する手段としてのパスワードの認証手段を同じキーデバイスに持たせることにより、キーデバイスの挿入及び、パスワードの入力がなければ、暗号データを復号化出来ない。パスワード及びパスワードの認証機能もキーデバイスを抜き取った後、システム側に残らないので従来の様にシステム側からパスワードが漏れることはない。キーデバイス内でも使用後パスワードは消滅し、パスワード認証機能も数値の範囲を限定する複数のフ

ィルターと回数により変化するパスワード関数の組み合わせで判定する方法で、途中間違うとそれ以上算出出来ず、６回のアタックでキーデバイスが機能不能となるため、認証手段からのパスワードの割り出しは困難である。また、プリンタには数値入力をするテンキーがついていないものもあり、一つのボタン、ワンタッチセンサーを使用し、ＯＮ，ＯＦＦの回数で入力するので場所をとらず、有効である。

【図面の簡単な説明】

【図１】特開平６－１２４１７８のシステム構成を示した図

【図２】特開平６－１２４１７８の作動手順を示すフローチャート

【図３】セキュリテイネットワークの概要を示した図

【図４】クライアントＰＣで画像／文書データを暗号化する手順を示した図

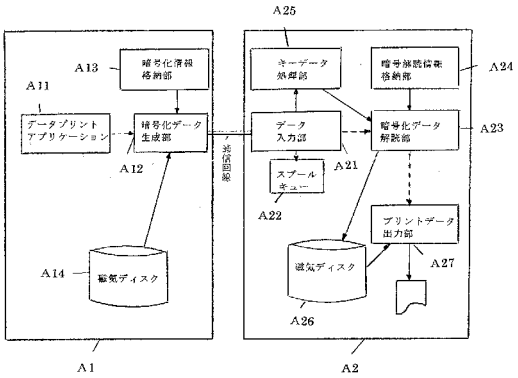
【図５】クライアントＰＣから送られた画像をプリンタで出力する場合の手順を示した図

【図６】キーデバイスの挿入公口、ワンボタンによるパスワード入力部及び出力部にカバーを有するプリンタ

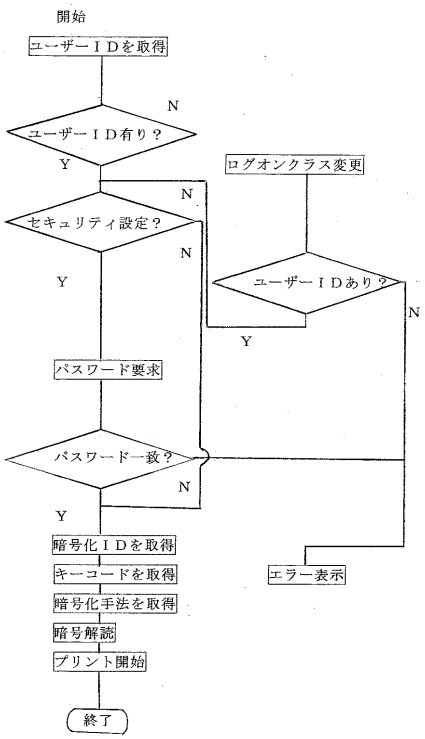
【符号の説明】

Ａ１　プリントデータ生成装置
Ａ２　プリンタ
Ａ１１　データプリントアプリケーション
Ａ１２　暗号データ生成部
Ａ１３　暗号化情報格納部
Ａ１４　磁気ディスク
Ａ２２　スプールキュー
Ａ２３　暗号データ解読部
Ａ２４　暗号解読情報格納部
Ａ２５　キーデータ処理部
Ａ２６　磁気ディスク
Ａ２７　プリントデータ出力部
１　クライアントＰＣ
２　プリンタ
３　プリンタに属するロギング装置
４　ネットワーク管理サーバー
５　ネットワーク
６　ネットワーク管理サーバーに属するロギング装置
７　ネットワーク管理装置
８　ＩＣカード
９　サーバー用ディスプレイ
１０　入力ボタン
１１　鍵付きカバー
１２　キーデバイス用スリット

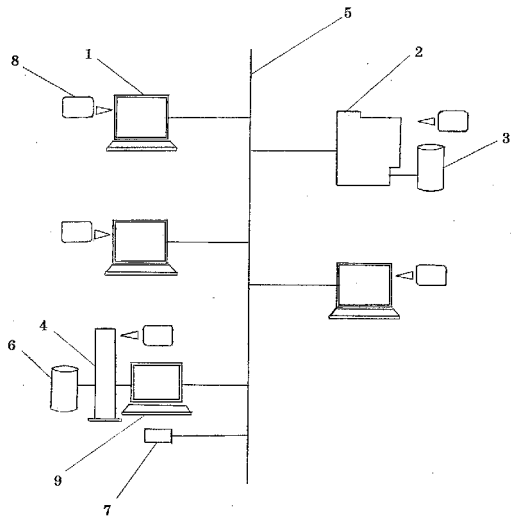
【図１】


A25
A13
暗号化情報格納部
A24
A11
キーデータ処理部
暗号解読情報格納部
データプリントアプリケーション
暗号化データ生成部
データ入力部
暗号化データ解読部
A23
A12
送信回線
スプールキュー
A21
A22
プリントデータ出力部
A14
磁気ディスク
磁気ディスク
A27
A26
A1
A2

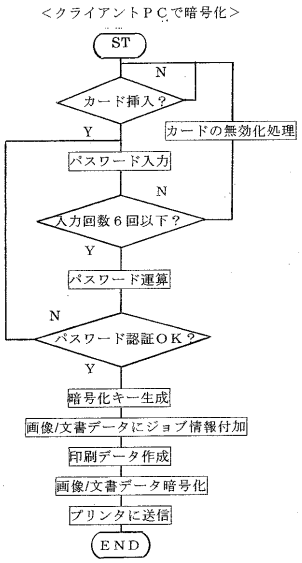
【図２】


開始
ユーザーＩＤを取得
ユーザーＩＤ有り？
N
Y
ログオンクラス変更
セキュリティ設定？
N
N
Y
ユーザーＩＤあり？
N
Y
パスワード要求
パスワード一致？
N
Y
暗号化ＩＤを取得
キーコードを取得
暗号化手法を取得
暗号解読
プリント開始
終了
エラー表示

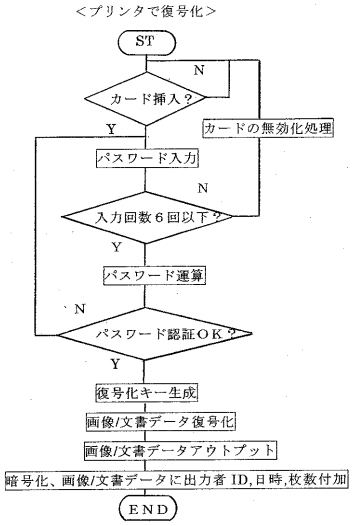
【図３】


1
2
3
4
5
6
7
8
9

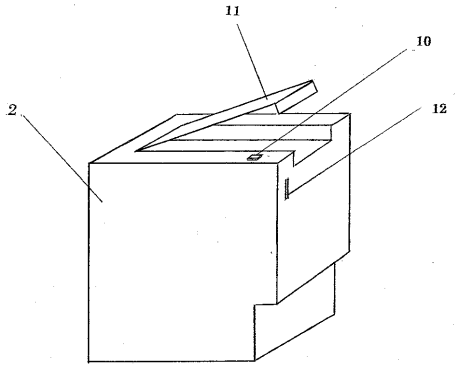
【図４】


<クライアントＰＣで暗号化>
ST
N
カード挿入？
Y
カードの無効化処理
パスワード入力
N
入力回数６回以下？
Y
パスワード運算
N
パスワード認証ＯＫ？
Y
暗号化キー生成
画像/文書データにジョブ情報付加
印刷データ作成
画像/文書データ暗号化
プリンタに送信
END

【図５】


<プリンタで復号化>
ST
カード挿入？
N
Y
カードの無効化処理
パスワード入力
入力回数６回以下？
N
Y
パスワード運算
パスワード認証ＯＫ？
N
Y
復号化キー生成
画像/文書データ復号化
画像/文書データアウトプット
暗号化、画像/文書データに出力者 ID,日時,枚数付加
END

【図６】


11
10
12
2

フロントページの続き

(51)Int.Cl.		FI		
G06K 17/00	*(2006.01)*	G06K	17/00	T
G06K 19/10	*(2006.01)*	G06K	19/00	R
G06K 19/07	*(2006.01)*	G06K	19/00	N
B41J 29/00	*(2006.01)*	B41J	29/00	Z

(72)発明者 小野 武英
神奈川県横浜市青葉区美しが丘５丁目３５番地の２株式会社ローレルインテリジェントシステムズ内

審査官 児玉 崇晶

(56)参考文献 特開２００１－１８６３５８（ＪＰ，Ａ）
特開平０９－２８２２３５（ＪＰ，Ａ）
特開平１１－１７５４０６（ＪＰ，Ａ）
特開２０００－０９００５１（ＪＰ，Ａ）
特開平１０－２８５１５３（ＪＰ，Ａ）
特開昭６０－２３６１８３（ＪＰ，Ａ）
特開平０９－２６５４５５（ＪＰ，Ａ）
特開２００１－３４６０３４（ＪＰ，Ａ）
特開２００１－３５０９３６（ＪＰ，Ａ）
特開平０４－３６６２８６（ＪＰ，Ａ）
特開昭５９－０１７６５０（ＪＰ，Ａ）
特開平０４－２２３７６７（ＪＰ，Ａ）
特開２０００－３５０００５（ＪＰ，Ａ）
特開平０６－１２４１７８（ＪＰ，Ａ）
特開平０９－２１９７００（ＪＰ，Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
G06F 21/24
B41J 5/30
B41J 29/00
B41J 29/38
G06F 1/00
G06F 21/20
G06K 17/00
G06K 19/07
G06K 19/10