(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5943045号
(P5943045)
(45)発行日　平成28年6月29日(2016.6.29)　(24)登録日　平成28年6月3日(2016.6.3)

(51)Int.Cl.　　F I
G06F 21/62 (2013.01)　　G06F 21/62 318
G06F 21/31 (2013.01)　　G06F 21/31

請求項の数 14　(全 23 頁)

(21)出願番号　特願2014-172669(P2014-172669)
(22)出願日　平成26年8月27日(2014.8.27)
(65)公開番号　特開2015-64873(P2015-64873A)
(43)公開日　平成27年4月9日(2015.4.9)
審査請求日　平成26年12月12日(2014.12.12)
(31)優先権主張番号　特願2013-176072(P2013-176072)
(32)優先日　平成25年8月27日(2013.8.27)
(33)優先権主張国　日本国(JP)

(73)特許権者　390002761
キヤノンマーケティングジャパン株式会社
東京都港区港南２丁目１６番６号
(73)特許権者　592135203
キヤノンＩＴソリューションズ株式会社
東京都品川区東品川２丁目４番１１号
(74)代理人　100189751
弁理士　木村　友輔
(74)代理人　100188938
弁理士　榛葉　加奈子
(72)発明者　橋本　達也
東京都品川区東品川２丁目４番１１号　キヤノンソフトウェア株式会社内

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理方法、及びそのプログラム

(57)【特許請求の範囲】
【請求項１】
表示データからコピーするデータを選択するコピー対象データ選択手段と、
前記コピー対象データ選択手段により選択されたデータをコピーデータとして記憶するコピーデータ記憶手段と、
ユーザによる認証情報の入力を受け付ける認証情報入力受付手段と、
前記認証情報を用いずに動作を復帰する方法と、前記認証情報入力受付手段により受け付けた認証情報を用いて動作を復帰する方法とを含む復帰方法のうち１種類の復帰方法を用いて、ロックされた状態から動作を復帰する動作復帰手段と、
前記認証情報を用いずに動作を復帰した場合、前記コピーデータ記憶手段により記憶されているコピーデータを利用させないように制御するコピーデータ制御手段と
を備えることを特徴とする情報処理装置。
【請求項２】
前記コピーデータ記憶手段は、前記コピーデータと、当該コピーデータが機密であるかを識別する識別情報とを対応づけて記憶するものであり、
前記情報処理装置は、
前記識別情報に従って、前記コピーデータが機密であるか否かを判定する機密判定手段を更に備え、
前記コピーデータ制御手段は、
前記認証情報を用いずに動作を復帰した場合であっても、前記機密判定手段により機密

でないと判定されたコピーデータを利用可能にし、前記機密判定手段により機密であると判定されたコピーデータを利用させないよう制御すること
を特徴とする請求項１に記載の情報処理装置。
【請求項３】
表示データからコピーするデータを選択するコピー対象データ選択手段と、
前記コピー対象データ選択手段により選択されたデータをコピーデータとして、当該コピーデータが機密であるかを識別する識別情報と対応づけて記憶するコピーデータ記憶手段と、
ユーザによる認証情報の入力を受け付ける認証情報入力受付手段と、
前記認証情報を用いずに動作を復帰する方法と、前記認証情報入力受付手段により受け付けた認証情報を用いて動作を復帰する方法とを含む復帰方法のうち１種類の復帰方法を用いて、ロックされた状態から動作を復帰する動作復帰手段と、
前記コピーデータ記憶手段により記憶された識別情報に従って、前記コピーデータが機密であるか否かを判定する機密判定手段と
を備え、
前記認証情報を用いずに動作を復帰した場合、前記機密判定手段により機密でないと判定されたコピーデータを利用可能にし、前記機密判定手段により機密であると判定されたコピーデータを利用させないよう制御するコピーデータ制御手段と
を備えることを特徴とする情報処理装置。
【請求項４】
前記コピーデータ記憶手段は、
前記認証情報を用いて動作を復帰した場合に、前記コピーデータ記憶手段により記憶されているコピーデータを利用可能にすること
を特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項５】
ユーザの操作に応じて、前記コピーデータ記憶手段で記憶されているコピーデータを表示画面にペーストするペースト手段と、
前記ペースト手段により前記コピーデータをペースト可能な許容回数を記憶するペースト許容回数記憶手段と
を更に備え、
前記コピーデータ制御手段は、
前記ペースト手段により前記コピーデータをペーストした回数が、前記ペースト許容回数記憶手段により記憶された許容回数を超えた場合に、前記コピーデータを利用させないよう制御すること
を特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。
【請求項６】
前記認証情報入力受付手段により受け付けた認証情報を用いて動作を復帰する方法を用いて、前記動作復帰手段により動作を復帰した場合、動作を復帰するまでに要した回数があらかじめ設定された許容回数を超えたか否か判定する動作復帰許容回数判定手段
を更に備え、
前記コピーデータ制御手段は、
前記認証情報を用いて動作を復帰した場合であっても、前記動作復帰許容回数判定手段により許容回数を超えたと判定された場合、前記コピーデータ記憶手段により記憶されているコピーデータを利用させないよう制御すること
を特徴とする請求項１乃至５のいずれか１項に記載の情報処理装置。
【請求項７】
あらかじめ設定された認証情報を記憶する認証情報記憶手段と、
前記コピーデータ制御手段は、
前記認証情報入力受付手段により受け付けた認証情報が、前記認証情報記憶手段により記憶されている認証情報と一致すると判定した場合、利用させないよう制御していたコピ

ーデータを利用可能に制御すること
を特徴とする請求項１乃至６のいずれか１項に記載の情報処理装置。
【請求項８】
前記認証情報を用いて動作を復帰する設定であるか否かを判定する認証設定判定手段と、
前記認証設定判定手段により前記認証情報を用いて動作を復帰する設定でないと判定された場合に、前記コピーデータ記憶手段により記憶されているコピーデータを利用できなくなることを通知する通知手段と
を更に備えること
を特徴とする請求項１乃至７のいずれか１項に記載の情報処理装置。
【請求項９】
前記通知手段による通知の後で、前記認証情報を用いて動作を復帰する設定に変更する指示を受け付けた場合、前記認証情報を用いて動作を復帰する設定に変更すること
を特徴とする請求項８に記載の情報処理装置。
【請求項１０】
前記コピーデータ制御手段によるコピーデータを利用させないようにする制御とは、当該コピーデータを削除する、前記コピーデータ記憶手段で記憶されている当該コピーデータを画面に表示しない、前記コピーデータ記憶手段で記憶されている当該コピーデータをマスクして表示する、または前記コピーデータ記憶手段で記憶されているコピーデータを表示するがペーストできないようにすること
を特徴とする請求項１乃至９のいずれか１項に記載の情報処理装置。
【請求項１１】
表示データからコピーするデータを選択するコピー対象データ選択手段と、前記コピー対象データ選択手段により選択されたデータをコピーデータとして記憶するコピーデータ記憶手段と、ユーザによる認証情報の入力を受け付ける認証情報入力受付手段と、前記認証情報を用いずに動作を復帰する方法と、前記認証情報入力受付手段により受け付けた認証情報を用いて動作を復帰する方法とを含む復帰方法のうち１種類の復帰方法を用いて、ロックされた状態から動作を復帰する動作復帰手段とを備える情報処理装置の処理方法であって、
前記情報処理装置が、
前記認証情報を用いずに動作を復帰した場合、前記コピーデータ記憶手段により記憶されているコピーデータを利用させないように制御するコピーデータ制御ステップ
を実行することを特徴とする処理方法。
【請求項１２】
表示データからコピーするデータを選択するコピー対象データ選択手段と、前記コピー対象データ選択手段により選択されたデータをコピーデータとして、当該コピーデータが機密であるかを識別する識別情報と対応づけて記憶するコピーデータ記憶手段と、ユーザによる認証情報の入力を受け付ける認証情報入力受付手段と、前記認証情報を用いずに動作を復帰する方法と、前記認証情報入力受付手段により受け付けた認証情報を用いて動作を復帰する方法とを含む復帰方法のうち１種類の復帰方法を用いて、ロックされた状態から動作を復帰する動作復帰手段と、前記コピーデータ記憶手段により記憶された識別情報に従って、前記コピーデータが機密であるか否かを判定する機密判定手段とを備える情報処理装置の処理方法であって、
前記認証情報を用いずに動作を復帰した場合、前記機密判定手段により機密でないと判定されたコピーデータを利用可能にし、前記機密判定手段により機密であると判定されたコピーデータを利用させないよう制御するコピーデータ制御ステップ
を実行することを特徴とする処理方法。
【請求項１３】
表示データからコピーするデータを選択するコピー対象データ選択手段と、前記コピー対象データ選択手段により選択されたデータをコピーデータとして記憶するコピーデータ

記憶手段と、ユーザによる認証情報の入力を受け付ける認証情報入力受付手段と、前記認証情報を用いずに動作を復帰する方法と、前記認証情報入力受付手段により受け付けた認証情報を用いて動作を復帰する方法とを含む復帰方法のうち１種類の復帰方法を用いて、ロックされた状態から動作を復帰する動作復帰手段とを備える情報処理装置のプログラムであって、

前記情報処理装置を、

前記認証情報を用いずに動作を復帰した場合、前記コピーデータ記憶手段により記憶されているコピーデータを利用させないように制御するコピーデータ制御手段

として機能させることを特徴とするプログラム。

【請求項１４】

表示データからコピーするデータを選択するコピー対象データ選択手段と、前記コピー対象データ選択手段により選択されたデータをコピーデータとして、当該コピーデータが機密であるかを識別する識別情報と対応づけて記憶するコピーデータ記憶手段と、ユーザによる認証情報の入力を受け付ける認証情報入力受付手段と、前記認証情報を用いずに動作を復帰する方法と、前記認証情報入力受付手段により受け付けた認証情報を用いて動作を復帰する方法とを含む復帰方法のうち１種類の復帰方法を用いて、ロックされた状態から動作を復帰する動作復帰手段と、前記コピーデータ記憶手段により記憶された識別情報に従って、前記コピーデータが機密であるか否かを判定する機密判定手段とを備える情報処理装置で実行可能なプログラムであって、

前記認証情報を用いずに動作を復帰した場合、前記機密判定手段により機密でないと判定されたコピーデータを利用可能にし、前記機密判定手段により機密であると判定されたコピーデータを利用させないよう制御するコピーデータ制御手段

として機能させることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報処理装置のデータセキュリティを高める技術に関する。

【背景技術】

【０００２】

情報処理装置においてデータをコピーすると、ペーストの有無に関わらずコピーしたデータがメモリに記憶され続けるため、情報処理装置を操作できる環境下にいる者であれば、コピーしたデータをペーストすることが可能となってしまう。特に最近は、携帯性に富んだ小型ＰＣやスマートフォンが台頭しているため、紛失や盗難により端末が他者の手に渡りやすくなっており、個人情報などの漏洩リスクが発生してしまう。

【０００３】

特許文献１には、この様なセキュリティリスクを軽減するために、コピーされたデータを特定条件時にメモリから消去する技術が開示されている。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２０１２－１３３６２０号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

特許文献１における情報処理装置は、コピーから所定の時間が経過したデータを消去することを特徴としている。

【０００６】

しかしながら、コピーデータ消去のトリガーが「時間経過」であると、ユーザの意図しないタイミングでデータが削除されてしまう恐れがある。すなわち、ペーストしたい時にデータがメモリから削除されてしまっているユーザにとって不便なケースや、第三者に端

末が渡ってしまった時に、コピーしたデータが保持され続けているセキュリティ上好ましくないケースが発生してしまう。

【０００７】

そこで、本発明の目的は、情報処理装置を使用可能状態に復帰させる方法に従ってコピーデータの利用を抑止することで、ユーザの不便さを解消し、データセキュリティを高める仕組みを提供することである。

【課題を解決するための手段】

【０００８】

表示データからコピーするデータを選択するコピー対象データ選択手段と、前記コピー対象データ選択手段により選択されたデータをコピーデータとして記憶するコピーデータ記憶手段と、ユーザによる認証情報の入力を受け付ける認証情報入力受付手段と、前記認証情報を用いずに動作を復帰する方法と、前記認証情報入力受付手段により受け付けた認証情報を用いて動作を復帰する方法とを含む復帰方法のうち１種類の復帰方法を用いて、ロックされた状態から動作を復帰する動作復帰手段と、前記認証情報を用いずに動作を復帰した場合、前記コピーデータ記憶手段により記憶されているコピーデータを利用させないように制御するコピーデータ制御手段とを備えることを特徴とする情報処理装置。

【発明の効果】

【０００９】

本発明により、情報処理装置を使用可能状態に復帰させる方法に従ってコピーデータの利用を抑止することで、ユーザの不便さを解消し、データセキュリティを高めることができる。

【図面の簡単な説明】

【００１０】

【図１】本発明の実施形態におけるシステムの構成を示す図である。
【図２】図１における情報処理装置のハードウェア構成を示す図である。
【図３】図１における情報処理装置の機能構成の一例を示す図である。
【図４】データコピー処理を行う手順の一例を説明するフローチャートである。
【図５】コピーデータ一覧表示処理を行う手順の一例を説明するフローチャートである。
【図６】モード遷移処理を行う手順の一例を説明するフローチャートである。
【図７】データペースト処理を行う手順の一例を説明するフローチャートである。
【図８】ＲＡＭ２０５ｂに保持するコピーデータの一例である。
【図９】機密コピー元設定画面の一例である。
【図１０】機密データ条件設定画面の一例である。
【図１１】ペースト可能回数を設定する十字フリック表示の一例である。
【図１２】コピーデータ一覧画面の一例である。
【図１３】コピーデータ一覧画面（機密コピーデータ削除後）の一例である。
【図１４】ペースト可能データ一覧画面の一例である。
【図１５】機密コピーデータに関する注意メッセージの一例である。
【図１６】第２の実施形態に係るモード遷移処理を行う手順の一例を説明するフローチャートである。
【図１７】第３の実施形態に係るデータペースト処理を行う手順の一例を説明するフローチャートである。

【発明を実施するための形態】

【００１１】

〔第１の実施形態〕

【００１２】

以下、図面を参照して、本発明の実施形態の一例について説明する。

【００１３】

図１は、本発明の実施形態におけるシステムの構成を示す図である。

【００１４】
情報処理装置１０１はユーザが操作する端末であって、ネットワーク１０３を介して接続されているＷｅｂサーバ１０２と通信を行い、Ｗｅｂサーバ１０２からＷｅｂページの情報を取得する。
【００１５】
ネットワーク１０３は、ＬＡＮ、インターネット等のネットワークであって、情報処理装置１０１とＷｅｂサーバ１０２は、ネットワーク１０３を介して通信可能である。
【００１６】
なお、図１のネットワーク上に接続される各種端末の構成は一例であり、用途や目的に応じて様々な構成例があることは言うまでもない。
【００１７】
図２を用いて、図１に示した情報処理装置１０１のハードウェア構成について説明する。
【００１８】
タッチセンサ入力部２０１はユーザからのタッチ入力を受け付ける入力部であり、加速度センサ入力部２０２は情報処理装置１０１の傾きを検知する入力部である。
【００１９】
タッチセンサ入力部２０１，加速度センサ入力部２０２は制御部２０４に接続されており、制御部２０４で処理が実行される。処理結果の表示は、制御部２０４に接続されたＬＥＤ部２０６が発光し、メイン表示部２０３でディスプレイに表示される。ＲＯＭ２０５ａには、ＣＰＵ２０５ｃの制御プログラムであるＢＩＯＳやオペレーティングシステム（以下、ＯＳ）、本発明を実現するための後述する各種プログラムなどが記憶されている。
【００２０】
ＲＡＭ２０５ｂは、ＣＰＵ２０５ｃの主メモリ、ワークエリア等として機能する。ＣＰＵ２０５ｃは、処理の実行に際して必要なプログラム等をＲＯＭ２０５ａからＲＡＭ２０５ｂにロードして、プログラムを実行することで各種動作を実現するものである。
【００２１】
なお、本発明を実現するための後述する各種プログラムは、ＲＯＭ２０５ａに記録されており、必要に応じてＲＡＭ２０５ｂにロードされることにより、ＣＰＵ２０５ｃによって実行されるものである。さらに、上記プログラムの実行時に用いられる各種設定情報も、ＲＯＭ２０５ａに格納されている。
【００２２】
また、通信部２０７を備えており、制御部２０４の制御に応じて、ネットワーク１０３を介して外部機器と接続・通信するものであり、ネットワークでの通信制御処理を実行する。例えば、ＴＣＰ／ＩＰを用いたインターネット通信等が可能である。
【００２３】
さらに、本発明に係わるプログラム２１３が用いる定義ファイル２１４及び各種情報テーブル２１５はＲＯＭ２０５ａに格納されており、これらについての詳細な説明は後述する。
【００２４】
図３において、情報処理装置１０１の機能について説明する。
【００２５】
コピー対象データ選択部３０１は、表示データからコピーするデータを選択する機能部である。
【００２６】
コピーデータ記憶部３０２は、コピー対象データ選択部３０１で選択されたデータをコピーデータとして記憶する機能部である。
【００２７】
認証情報入力部３０３は、認証情報を入力する機能部である。
【００２８】

抑止部３０５は、認証情報入力部３０３で入力された認証情報を用いて動作を復帰した場合に、コピーデータ記憶部３０２で記憶されているコピーデータの利用を抑止することなく、認証情報を用いずに動作を復帰した場合に、コピーデータ記憶部３０２で記憶されているコピーデータの利用を抑止する機能部である。

【００２９】

また、コピーデータ記憶部３０２は、コピーデータと、当該コピーデータが機密であるかを識別する識別情報と対応づけて記憶する機能部である。

【００３０】

機密判定部３０４は、識別情報に従って、コピーデータが機密であるか否かを判定する機能部である。

【００３１】

また、抑止部３０５は、認証情報を用いずに動作を復帰した場合に、機密判定部３０４によって機密でないと判定されたコピーデータの利用を抑止することなく、機密判定部３０４によって機密であると判定されたコピーデータの利用を抑止する機能部である。

【００３２】

また、コピーデータ記憶部３０２は、コピーデータと、当該コピーデータが機密であるかを識別する識別情報と対応づけて記憶する機能部である。

【００３３】

ペースト部３０６は、ユーザの操作に応じて、表示画面にコピーデータ記憶部３０２で記憶されているコピーデータをペーストする機能部である。

【００３４】

また、抑止部３０５は、ペースト部３０６でコピーデータをペーストした回数が所定の回数を超えた場合に、コピーデータの利用を抑止する機能部である。

【００３５】

認証情報記憶部３０７は、認証に用いられる認証情報を予め記憶する機能部である。

【００３６】

認証情報判定部３０８は、認証情報入力部３０３で入力された認証情報と認証情報記憶部３０７に記憶されている認証情報とが一致するかを判定する機能部である。

【００３７】

また、抑止部３０５は、認証情報入力部３０３で認証情報が入力され、当該入力された入力情報が認証情報判定部３０８で所定回数一致しない場合に、コピーデータ記憶部３０２で記憶されているコピーデータの利用を抑止する機能部である。

【００３８】

認証設定判定部３０９は、認証情報を用いて動作を復帰する設定であるか否かを判定する機能部である。

【００３９】

通知部３１０は、コピー対象データ選択部３０１でコピーするデータを選択し、認証設定判定部３０９で認証情報を用いて動作を復帰する設定でないと判定された場合に、コピーデータ記憶部３０２で記憶されているコピーデータの利用を抑止することを通知する機能部である。

【００４０】

また、コピーデータ記憶部３０２は、通知部３１０の通知に従って、認証設定を変更する指示を受け付けた場合に、認証情報を用いて動作を復帰する設定に変更し、コピーデータと、当該コピーデータが機密であるかを識別する識別情報と対応づけて記憶する機能部である。

【００４１】

また、抑止部３０５による抑止は、コピーデータを削除する機能部である。

【００４２】

次に、本実施形態における詳細な処理の説明を図４～図７のフローチャートを用いて説明する。

【００４３】
図４は、データコピー処理を行う手順の一例を説明するフローチャートである。図８は、ＲＡＭ２０５ｂに保持するコピーデータの一例である。図９は、機密コピー元設定画面の一例である。図１０は、機密データ条件設定画面の一例である。図１１は、ペースト可能回数を設定する十字フリック表示の一例である。図１５は、機密コピーデータに関する注意メッセージの一例である。
【００４４】
図４を参照して、本実施形態におけるデータコピー処理の流れを説明する。
【００４５】
ステップＳ４０１において、メイン表示部２０３にＷｅｂサイトや文書ファイルを表示している情報処理装置１０１のタッチセンサ入力部２０１は、ユーザからのコピー命令を検知する。具体的には、情報処理装置１０１のメイン表示部２０３に表示されている文字列や画像がユーザによってタッチされると、ＣＰＵ２０５ｃがメイン表示部２０３に表示している文字列や画像を反転させると同時にコピーボタンを表示する。ユーザによってそのコピーボタンがタップされると、タッチセンサ入力部２０１がコピー命令を検知する。すなわち、ステップＳ４０１は、表示データからコピーするデータを選択する処理の一例を示すステップである。
【００４６】
ステップＳ４０２において、ステップＳ４０１のコピーボタンのタップが機密コピーデータとして扱う指示であるダブルタップであるかどうか判定する。なお、この実施形態においては、ダブルタップされた場合、コピーデータを機密データとして扱うとしたが、ダブルタップに限定するものではなく、その他の方法であってもよい。
【００４７】
ダブルタップの場合は、ステップＳ４０６に進む。ダブルタップでない場合は、ステップＳ４０３にてコピー元のＵＲＬやアプリケーションが、ユーザによって事前に設定されＲＯＭ２０５ａに記憶している、機密コピー元（図９）と一致するかを判定する。機密コピー元は、ユーザによって事前に設定され、「ｈｔｔｐｓ：／／で始まるＵＲＬのＷｅｂサイト」（図９の９０１）や「パスワード管理ツールというアプリ」（図９の９０２）など、機密情報を扱うＷｅｂサイトやアプリケーションの設定をすることで、コピーを行ったＷｅｂサイトやアプリケーションが機密コピー元に一致する場合は、コピーデータを機密コピーデータとして扱う。なお、ＵＲＬの設定値に「＊」を使うことで、前方一致や中間一致などの条件についても設定できる。
【００４８】
この実施形態では、機密コピー元設定（図９）をユーザが行うとしたが、セキュリティベンダーやユーザが所属する企業が配布する機密コピー元設定を直接参照したり、機密コピー元設定をダウンロードしＲＯＭ２０５ａに記憶して利用することによって、ユーザ個人による設定に依存するのではなく、セキュリティベンダーが推奨するセキュリティルール、またはユーザが所属する企業のセキュリティルールに則った機密コピー元設定を適用するとしてもよい。これにより、情報漏洩のリスクをより軽減することができる。
【００４９】
また、ユーザによる機密コピー元設定や、機密コピー元設定ファイルを参照する他にも、アクセスしているＷｅｂサイトの内容や通信方法を解析して、機密コピー元として扱うとしてもよい。具体的には、金融機関のＷｅｂサイトや個人情報を表示するＷｅｂサイト、ＳＳＬによって通信を行って表示するＷｅｂサイトなどの場合、そのＷｅｂページは、機密コピー元として判定するとしてもよい。
機密コピー元に一致した場合は、ステップＳ４０６に進む。
【００５０】
機密コピー元に一致しなかった場合は、ステップＳ４０４において、反転表示したコピー対象データを取得し、ユーザによって事前に設定されＲＯＭ２０５ａに記憶している、機密データ条件（図１０）にあてはまるか判定する。ここで、機密データ条件とは、「コ

ピー対象データ内に“機密”という文字列がある」（図１０の１００１）、「コピー対象データ内に連続する数字が４文字以上ある」（図１０の１００２）など、コピー対象データを機密コピーデータとみなす条件である。

【００５１】

これらの機密データ条件を設定することで、“機密”という文字列がある文章や、連続する数字が４文字以上ある「ユーザＩＤ」「パスワード」「口座番号」「クレジットカード番号」などをコピーした場合、機密コピーデータとして扱うことができる。

【００５２】

この実施形態では、機密データ条件をユーザが設定するとしたが、セキュリティベンダーやユーザが所属する企業が配布する機密データ条件設定を直接参照したり、機密データ条件設定をダウンロードしＲＯＭ２０５ａに記憶して利用することによって、ユーザ個人による設定に依存するのではなく、セキュリティベンダーが推奨するセキュリティルール、またはユーザが所属する企業のセキュリティルールに則った機密データ条件を適用するとしてもよい。これにより、情報漏洩のリスクをさらに減らすことができる。

【００５３】

また、ユーザによる機密データ条件設定や、機密データ条件設定ファイルを参照する他にも、言語解析などによって、「ユーザＩＤ」「パスワード」「口座番号」「クレジットカード番号」などを特定し、機密コピーデータとして扱うとしてもよい。

【００５４】

機密データ条件にあてはまった場合は、ステップＳ４０６に進む。機密データ条件にあてはまらなかった場合は、ステップＳ４０５において、反転表示したコピー対象データを取得し、機密フラグを付与せずに、コピーデータとしてＲＡＭ２０５ｂに保持する。（図８の８１４）

【００５５】

ステップＳ４０６において、ＯＳ（オペレーティングシステム）におけるユーザの設定が、画面ロック（スリープ）を解除する際に認証情報入力を必要とする設定かどうかを判定する。ユーザの設定とは、ＯＳが予め備えている、画面ロック（スリープ）時の解除設定であり、パスワード入力、ＰＩＮ入力、パターン入力などユーザが任意に設定できるものである。ここで、パスワード入力、ＰＩＮ入力、パターン入力など認証情報を入力して画面ロック（スリープ）を解除する設定になっている場合に、認証情報入力を必要とする設定と判定される。また、スワイプ操作のみによる画面ロック（スリープ）を解除する設定になっている場合には、認証情報入力を必要としない設定と判定される。すなわち、ステップＳ４０６は、認証情報を用いて動作を復帰する設定であるか否かを判定する処理の一例を示すステップである。

【００５６】

認証情報入力を必要とする設定の場合は、ステップＳ４１０に進む。認証情報入力を必要としない設定の場合は、ステップＳ４０７において、「機密データとして保持します。なお、機密データは、画面ロック（スリープ）を解除する際、認証情報を入力しない場合、削除されます。」といった内容のダイアログメッセージ１５０１（図１５）を表示する。すなわち、ステップＳ４０７は、認証情報を用いて動作を復帰する設定でないと判定された場合に、記憶されているコピーデータの利用を抑止することを通知する処理の一例を示すステップである。

【００５７】

ステップＳ４０８において、「認証情報入力を行う設定に変更する」ボタン１５０２が押されたかどうか判定する。

【００５８】

「認証情報入力を行う設定に変更する」ボタン１５０２が押された場合、ステップＳ４０９において、認証情報入力を行う設定に変更する。すなわち、ステップＳ４０９は、認証設定を変更する指示を受け付けた場合に、認証情報を用いて動作を復帰する設定に変更する処理の一例を示すステップである。

【００５９】
「認証情報入力を行う設定に変更する」ボタン１５０２が押されず、閉じるボタン１５０３が押された場合、ダイアログメッセージ１５０１を閉じる。
【００６０】
ステップＳ４１０において、反転表示したコピー対象データを取得し、機密フラグを付与し、機密コピーデータとしてＲＡＭ２０５ｂに保持する（図８の８１１）。すなわち、ステップＳ４１０は、選択されたデータをコピーデータとして記憶する処理の一例を示すステップである。
【００６１】
ステップＳ４１１において、ステップＳ４０１のコピーボタンのタップが所定の時間よりも長く押されたかどうか判定する。
【００６２】
コピーボタンが長押しされた場合は、ステップＳ４１２において、ペースト可能回数を設定するために上下左右に１～４の数字が記された十字フリック１１０１（図１１）をメイン表示部２０３に表示する。なお、十字フリック１１０１の形式でなくても、数字が選ぶことができるプルダウンなどの形式でもよく、選択させる数字も１～４に限定するものではなく、１～無制限などであってもよい。
【００６３】
ステップＳ４１３において、ユーザによって十字フリック１１０１に表示されている数字が選択されたか判定する。
【００６４】
数字が選択されなかった場合は、ステップＳ４１３において、十字フリック１１０１の表示を終了し、ペースト可能回数を設定しない（図８の８１５）。つまり、ペースト可能回数を設定しない場合、機密コピーデータがＲＡＭ２０５ｂに保持されている限り、何度でもペースト可能となる。
【００６５】
数字が選択された場合は、ステップＳ４１４において、ペースト可能回数として選択された数値をＲＡＭ２０５ｂに機密コピーデータに紐付けて設定する。具体的には、図８の８１６は、ペースト可能回数として３が選択された場合を表している。
【００６６】
ステップＳ４１１において、コピーボタンが長押しされなかった場合は、十字フリック１１０１は表示せず、ペースト可能回数も設定しない（図８の８１５）
以上で、データコピー処理を終了する。
【００６７】
図５は、コピーデータ一覧表示処理を行う手順の一例を説明するフローチャートである。図１２は、コピーデータ一覧画面の一例である。図５を参照して、本実施形態におけるコピーデータ一覧表示処理の流れを説明する。
【００６８】
ステップＳ５０１において、メイン表示部２０３にＷｅｂサイトや文書ファイルを表示している情報処理装置１０１のタッチセンサ入力部２０１は、ユーザからのコピーデータ一覧表示命令を検知する。具体的には、情報処理装置１０１のメイン表示部２０３に表示されているテキストボックス９０１などの入力可能領域をユーザによって長押しされると、ＣＰＵ２０５ｃがメイン表示部２０３にショートカットメニュー９０２を表示する。ユーザによってショートカットメニュー９０２内のコピーデータ一覧表示ショートカット９０４がタップされると、タッチセンサ入力部２０１がコピーデータ一覧表示命令として検知する。
【００６９】
ステップＳ５０２において、ＲＡＭ２０５ｂにコピーデータが存在するか判定する。
【００７０】
コピーデータが存在した場合は、ステップＳ５０３において、コピーデータ一覧画面１

２００（図１２）を表示し、後述するペースト可能回数の変更、機密フラグの変更、および、コピーデータの削除を行うことができる。

【００７１】

コピーデータが存在しなかった場合は、ステップＳ５０４において、「コピーデータが存在しない」という内容のメッセージを表示し、コピーデータ一覧表示処理を終了する。

【００７２】

ステップＳ５０５において、情報処理装置１０１のタッチセンサ入力部２０１は、ユーザによってペースト可能回数の増減ボタン（図１２の１２０２・１２０４）が押されたか判定する。

【００７３】

「－」ボタン１２０２が押された場合は、ステップＳ５０６において、ＲＡＭ２０５ｂにおける該当するコピーデータのペースト可能回数１２０３から１減算し、減算した数字を表示する。また、減算した結果、０になる場合は、１とする。

【００７４】

「＋」ボタン１２０４が押された場合は、ステップＳ５０７において、ＲＡＭ２０５ｂにおける該当するコピーデータのペースト可能回数１２０３に１加算し、加算した数字を表示する。

【００７５】

増減ボタンが押されなかった場合は、ステップＳ５０８において、情報処理装置１０１のタッチセンサ入力部２０１は、ユーザによって機密フラグセレクトボックス１２０５の値が変更されたか判定する。

【００７６】

機密フラグセレクトボックス１２０５の値が「○」から「×」に変更された場合は、「機密」から「通常」への機密フラグの変更と捉え、ステップＳ５０９において、ＲＡＭ２０５ｂにおける該当するコピーデータの機密フラグ８０３を「×」に変更する。すなわち、ステップＳ５０９は、コピーデータと、当該コピーデータが機密であるかを識別する識別情報と対応づけて記憶する処理の一例を示すステップである。更に、ステップＳ５１０において、ＲＡＭ２０５ｂにおける該当するコピーデータのペースト可能回数８０２を空白にする。

【００７７】

機密フラグセレクトボックス１２０５の値が「×」から「○」に変更された場合は、「通常」から「機密」への機密フラグの変更と捉え、ステップＳ５１１において、ＲＡＭ２０５ｂにおける該当するコピーデータの機密フラグ８０３を「○」に変更する。すなわち、ステップＳ５１１は、コピーデータと、当該コピーデータが機密であるかを識別する識別情報と対応づけて記憶する処理の一例を示すステップである。

【００７８】

ステップＳ５１２において、情報処理装置１０１のタッチセンサ入力部２０１は、ユーザによって削除ボタン１２０６が押されたか判定する。

【００７９】

削除ボタン１２０６が押された場合は、ステップＳ５１３において、ＲＡＭ２０５ｂにおける該当するコピーデータを削除する。なお、本実施形態においては、ＲＡＭ２０５ｂからコピーデータを削除することでコピーデータの利用を抑止するとしたが、コピーデータの利用を抑止はこの方法に限定するものではなく、ＲＡＭ２０５ｂにコピーデータを記憶したままでコピーデータ一覧として表示しない、ＲＡＭ２０５ｂにコピーデータを記憶したままでにアクセスできなくする、コピーデータ一覧として表示するがマスクして表示する、コピーデータ一覧として表示するがペーストできないようにするなどの方法であってもよい。すなわち、ステップＳ５１３は、コピーデータを削除する、または記憶されているコピーデータとして表示しない、または記憶されているコピーデータとしてマスクして表示する、または記憶されているコピーデータとして表示するがペーストできないようにする処理の一例を示すステップである。

【００８０】
削除ボタン１２０６が押されなかった場合は、ステップＳ５１４に進む。
【００８１】
ステップＳ５１４において、情報処理装置１０１のタッチセンサ入力部２０１は、ユーザによって閉じるボタン１２０７が押されたか判定する。
【００８２】
閉じるボタン１２０７が押されなかった場合は、ステップＳ５０５に戻る。閉じるボタン１２０７が押された場合は、コピーデータ一覧表示処理を終了する。
【００８３】
図６は、モード遷移処理を行う手順の一例を説明するフローチャートである。図１３は、コピーデータ一覧画面（機密コピーデータ削除後）の一例である。
【００８４】
図６を参照して、本実施形態におけるモード遷移時の処理の流れを説明する。
【００８５】
ステップＳ６０１において、画面ロック（スリープ）状態の情報処理装置１０１は、ユーザによってタッチセンサ入力部２０１などの入力部に触れられると、画面ロック（スリープ）を解除し、情報処理装置１０１の各種操作が使用可能状態に復帰させる。
【００８６】
ステップＳ６０２において、画面ロック（スリープ）の解除時に認証情報の入力を行ったかを判定する。なお、認証情報とは、パスワード、ユーザＩＤとパスワード、パターン、生体情報などの情報であって、入力・選択した情報があらかじめＲＯＭ２０５ａなどに格納されている認証情報と一致する場合に画面ロック（スリープ）の解除を行う。すなわち、ステップＳ６０２は、認証情報を入力する処理の一例を示すステップである。また、認証情報が格納されているＲＯＭ２０５ａは、認証に用いられる認証情報を予め記憶する認証情報記憶部の一例である。また、ステップＳ６０２は、入力された認証情報と認証情報記憶部に記憶されている認証情報とが一致するかを判定する処理の一例を示すステップである。
【００８７】
認証情報の入力がされずに画面ロック（スリープ）を解除した場合（例えば、スワイプ操作のみによる解除）、ステップＳ６０３において、ＲＡＭ２０５ｂに保持するコピーデータのうち、機密コピーデータを削除する。すなわち、ステップＳ６０３は、コピーデータが機密であるかを識別する識別情報に従って、コピーデータが機密であるか否かを判定する処理の一例を示すステップである。また、ステップＳ６０３は、認証情報を用いずに動作を復帰した場合に、コピーデータ記憶手段で記憶されているコピーデータの利用を抑止する処理の一例を示すステップである。具体的には、ＲＡＭ２０５ｂに保持するコピーデータのうち、機密フラグ８０３が「○」のコピーデータ（図８の８１１・８１２・８１３・８１５・８１６）を削除する。
【００８８】
なお、本実施形態においては、ＲＡＭ２０５ｂからコピーデータを削除することでコピーデータの利用を抑止するとしたが、コピーデータの利用を抑止はこの方法に限定するものではなく、ＲＡＭ２０５ｂにコピーデータを記憶したままでコピーデータ一覧として表示しない、ＲＡＭ２０５ｂにコピーデータを記憶したままでにアクセスできなくする、コピーデータ一覧として表示するがマスクして表示する、コピーデータ一覧として表示するがペーストできないようにするなどの方法であってもよい。なお、コピーデータを抑止した場合、事前に設定された認証情報が入力されることに従って、機密コピーデータの利用を可能にする。この認証情報は、画面ロック（スリープ）を解除するための認証情報と同じ認証情報としても、別の認証情報としてもよい。すなわち、ステップＳ６０３は、コピーデータを削除する、または記憶されているコピーデータとして表示しない、または記憶されているコピーデータとしてマスクして表示する、または記憶されているコピーデータとして表示するがペーストできないようにする処理の一例を示すステップである。

【００８９】
ステップＳ６０２にて認証情報の入力に従って画面ロック（スリープ）を解除した場合、ステップＳ６０４において、入力された認証情報とあらかじめＲＯＭ２０５ａなどに格納されている認証情報とが一致するまで、認証情報の入力を４回以上行ったかを判定する。
【００９０】
ステップＳ６０４にて認証情報の入力を４回以上行ったと判定された場合は、ステップＳ６０３において、機密コピーデータをＲＡＭ２０５ｂから削除する。具体的には、ＲＡＭ２０５ｂから機密コピーデータをすべて削除する（図１３の１２００）。すなわち、ステップＳ６０４は、入力された入力情報が認証情報記憶部に記憶されている認証情報と所定回数一致しない場合に、ＲＡＭ２０５ｂに記憶されているコピーデータの利用を抑止する処理の一例を示すステップである。
【００９１】
認証情報の入力を４回以上行わなかった場合、つまり、３回以内で画面ロック（スリープ）を解除できた場合は、モード遷移処理を終了する、よって、当該コピーデータはＲＡＭ２０５ｂに保持したままである。すなわち、ステップＳ６０４は、認証情報を用いて動作を復帰した場合に、コピーデータ記憶手段で記憶されているコピーデータの利用を抑止しない処理の一例を示すステップである。
【００９２】
なお、認証情報の入力回数は４回ではなくてもよく、ユーザが所定の回数を設定できるとする。
【００９３】
以上により、情報処理装置を使用可能状態に復帰させる方法に従ってコピーデータの利用を抑止することで、ユーザの不便さを解消し、データセキュリティを高めることができる。
【００９４】
図７は、データペースト処理を行う手順の一例を説明するフローチャートである。図１４は、ペースト可能データ一覧画面の一例である。図７を参照して、本実施形態におけるデータペースト処理の流れを説明する。
【００９５】
ステップＳ７０１において、情報処理装置１０１のタッチセンサ入力部２０１は、ユーザからのデータペースト命令を検知する。具体的には、情報処理装置１０１のメイン表示部２０３に表示されているテキストボックスなどの入力可能領域をユーザによって長押しされると、ＣＰＵ２０５ｃがメイン表示部２０３にショートカットメニュー９０２を表示する。ユーザによってショートカットメニュー９０２内のペーストショートカット９０３がタップされると、タッチセンサ入力部２０１がデータペースト命令を検知する。
【００９６】
ステップＳ７０２において、ＲＡＭ２０５ｂに存在するコピーデータとペースト可能回数の表を表示する。（図１４の１４０１）
【００９７】
ステップＳ７０３において、ユーザによってペーストするコピーデータが選択されたことを検知する。
【００９８】
ステップＳ７０４において、メイン表示部２０３に表示されているテキストボックスなどの入力可能領域に、選択されたコピーデータをペーストする。すなわち、ステップＳ７０４は、ユーザの操作に応じて、ＲＡＭ２０５ｂに記憶されているコピーデータを表示画面にペーストする処理の一例を示すステップである。
【００９９】
ステップＳ７０５において、ＲＡＭ２０５ｂにおける該当するコピーデータにペースト可能回数８０２が設定されているか判定する。

【０１００】
ペースト可能回数８０２が設定されていない場合は、データペースト処理を終了する、つまり、当該コピーデータはＲＡＭ２０５ｂに保持したままである
【０１０１】
ペースト可能回数８０２が設定されている場合は、ステップＳ７０６において、ＲＡＭ２０５ｂにおける該当するコピーデータのペースト可能回数８０２から１減算する。
【０１０２】
ステップＳ７０７において、ペースト可能回数が０かどうか判定する。
【０１０３】
ペースト可能回数が０である場合は、ステップＳ７０８において、当該コピーデータをＲＡＭ２０５ｂから削除し、データペースト処理を終了する。すなわち、ステップＳ７０８は、コピーデータをペーストした回数が所定の回数を超えた場合に、コピーデータの利用を抑止する処理の一例を示すステップである。
【０１０４】
ペースト可能回数が０でない場合は、データペースト処理を終了する、つまり、当該コピーデータはＲＡＭ２０５ｂに保持したままである
以上で、データペースト処理を終了する。
【０１０５】
ここまでで、情報処理装置を使用可能状態に復帰させる方法に従ってコピーデータを削除する流れについて、説明を完了する。
【０１０６】
以上、本実施形態によれば、情報処理装置を使用可能状態に復帰させる方法に従ってコピーデータの利用を抑止（例えば、コピーデータを削除）することで、ユーザの利便性を向上させ、データセキュリティを高めることができる。
【０１０７】
また、画面ロック（スリープ）を解除する際に認証情報入力を必要としない設定の場合に、認証情報入力を必要とする設定への変更を促すことによって、データセキュリティをより高めることができる。
【０１０８】
さらに、本実施形態によって、機密コピー元や機密データ条件などの設定を、ユーザが所属する企業のセキュリティルールに則った設定を利用し、所属企業の所望するセキュリティルールを多くの従業員に対して適用し、データセキュリティをより高めることができる。
【０１０９】
〔第２の実施形態〕
図１６は、第２の実施形態に係るモード遷移処理を行う手順の一例を説明するフローチャートである。図１６は、第１の実施形態に係るモード遷移処理を行う手順の一例を説明するフローチャート（図６）の一部を変更したフローチャートである。その他の図面に関しては、第１の実施形態と第２の実施形態とにおいて同等のものとし、繰り返しになるため再度の説明は省略する。以下、図１６について説明する。
【０１１０】
認証情報の入力がされずに画面ロック（スリープ）を解除した場合（例えば、スワイプ操作のみによる解除）、ステップＳ１６０１において、ＲＡＭ２０５ｂから機密コピーデータだけでなく、コピーデータのすべてを削除する。具体的には、ＲＡＭ２０５ｂに保持するコピーデータのすべて（図８の８１１～８１６）を削除する。なお、ＲＡＭ２０５ｂからコピーデータを削除する他にも、コピーデータにアクセスできなくしたり、コピーデータをペーストできなくしたりするなど、コピーデータの利用を抑止するとしてもよい。コピーデータを抑止した場合、画面ロック（スリープ）を解除するための認証情報とは別の、事前に設定された認証情報が入力されることに従って、コピーデータの利用を可能にする。

【０１１１】
ステップＳ６０４にて認証情報の入力を４回以上行ったと判定された場合は、ステップＳ１６０１において、コピーデータをＲＡＭ２０５ｂから削除する。具体的には、ＲＡＭ２０５ｂからコピーデータをすべて削除する。（図１３の１２００）
【０１１２】
なお、認証情報の入力回数は４回ではなくてもよく、ユーザが所定の回数を設定できるとする。
【０１１３】
以上で、図１６の第２の実施形態に係るモード遷移処理を終了する。
【０１１４】
以上により、第２の実施形態において、情報処理装置を使用可能状態に復帰させる方法に従ってコピーデータの利用を抑止することで、ユーザの不便さを解消し、データセキュリティを高めることができる。
【０１１５】
〔第３の実施形態〕
図１７は、第３の実施形態に係るデータペースト処理を行う手順の一例を説明するフローチャートである。図１７は、第１の実施形態に係るデータペースト処理を行う手順の一例を説明するフローチャート（図７）の一部を変更したフローチャートである。その他の図面に関しては、第１の実施形態と第３の実施形態とにおいて同等のものとし、繰り返しになるため再度の説明は省略する。以下、図１７について説明する。
【０１１６】
ステップＳ１７０１において、ステップＳ７０３にて選択されたコピーデータのペースト可能回数をＲＡＭ２０５ｂから取得し、その数字が０の場合はステップＳ１７０２に進み、０より大きい場合はステップＳ７０４に進む。
【０１１７】
ステップＳ１７０２において、ペースト回数が０であるコピーデータをペーストするため、認証情報の入力または選択画面を表示し、ユーザに認証情報を入力・選択させる。なお、認証情報とは、パスワード、ユーザＩＤとパスワード、パターン、生体情報などの情報である。なお、この認証情報は、画面ロック（スリープ）を解除するための認証情報と同一の認証情報であってもよいし、画面ロック（スリープ）を解除するための認証情報とは異なり、ペースト回数が０であるコピーデータをペーストするための認証情報であってもよい。
【０１１８】
ステップＳ１７０３において、ステップＳ１７０２にて入力または選択した情報があらかじめＲＯＭ２０５ａなどに格納されている認証情報と一致するか否かを判定し、一致する場合にＳ７０４に進み、（ペースト回数が０である）選択されたコピーデータのペースト処理を行い、一致する場合に図１７のデータペースト処理を終了する。これにより、利用を抑止していたコピーデータの再利用が可能になり、データセキュリティを保ったままで、ユーザの利便性を高めることができる。すなわち、ステップＳ１７０３は、入力された入力情報が認証情報記憶部に記憶されている認証情報とが一致すると判定した場合に、抑止していたコピーデータの利用を可能にする処理の一例を示すステップである。
【０１１９】
ステップＳ１７０４において、ステップＳ７０３にて選択されたコピーデータのペースト可能回数をＲＡＭ２０５ｂから取得し、その数字が０未満の場合はステップＳ１７０５に進み、０以上の場合は図１７のデータペースト処理を終了する。
【０１２０】
ステップＳ１７０５において、ステップＳ１７０４にて取得したペースト可能回数から１減算し、ＲＡＭ２０５ｂに記憶する。
【０１２１】
以上で、図１７の第３の実施形態に係るデータペースト処理を終了する。

【０１２２】
以上により、第３の実施形態において、情報処理装置を使用可能状態に復帰させる方法に従ってコピーデータの利用を抑止することで、ユーザの不便さを解消し、データセキュリティを高めることができる。
【０１２３】
〔第４の実施形態〕
第４の実施形態では、モード遷移処理を行う手順として図１６のフローチャートを、データペースト処理を行う手順として図１７のフローチャートを用いる。その他の図面に関しては、第１の実施形態と第４の実施形態とにおいて同等のものとする。
【０１２４】
以上により、第４の実施形態において、情報処理装置を使用可能状態に復帰させる方法に従ってコピーデータの利用を抑止することで、ユーザの不便さを解消し、データセキュリティを高めることができる。
【０１２５】
ここまでで、情報処理装置を使用可能状態に復帰させる方法に従ってコピーデータを削除する流れについて、説明を完了する。
【０１２６】
以上、第１～４の本実施形態によれば、情報処理装置を使用可能状態に復帰させる方法に従ってコピーデータの利用を抑止（例えば、コピーデータを削除）することで、ユーザの利便性を向上させ、データセキュリティをより高めることができる。
【０１２７】
また、画面ロック（スリープ）を解除する際に認証情報入力を必要としない設定の場合に、認証情報入力を必要とする設定への変更を促すことによって、データセキュリティをより高めることができる。
【０１２８】
さらに、本実施形態によって、機密コピー元や機密データ条件などの設定を、ユーザが所属する企業のセキュリティルールに則った設定を利用し、所属企業の所望するセキュリティルールを多くの従業員に対して適用し、データセキュリティをより高めることができる。
【０１２９】
以上のように、前述した実施形態の機能を実現するプログラムを記録した記録媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記録媒体に格納されたプログラムを読出し実行することによっても、本発明の目的が達成されることは言うまでもない。
【０１３０】
この場合、記録媒体から読み出されたプログラム自体が本発明の新規な機能を実現することになり、そのプログラムを記憶した記録媒体は本発明を構成することになる。
【０１３１】
プログラムを供給するための記録媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＥＥＰＲＯＭ、シリコンディスク、ソリッドステートドライブ等を用いることができる。
【０１３２】
また、コンピュータが読み出したプログラムを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。
【０１３３】
さらに、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張

ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１３４】

また、本発明は、複数の機器から構成されるシステムに適用しても、１つの機器からなる装置に適用してもよい。また、本発明は、システムあるいは装置にプログラムを供給することによって達成される場合にも適応できることは言うまでもない。この場合、本発明を達成するためのプログラムを格納した記録媒体を該システムあるいは装置に読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０１３５】

上記プログラムの形態は、オブジェクトコード、インタプリタにより実行されるプログラムコード、ＯＳ（オペレーティングシステム）に供給されるスクリプトデータ等の形態から成ってもよい。

【０１３６】

さらに、本発明を達成するためのプログラムをネットワーク上のサーバ、データベース等から通信プログラムによりダウンロードして読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【０１３７】

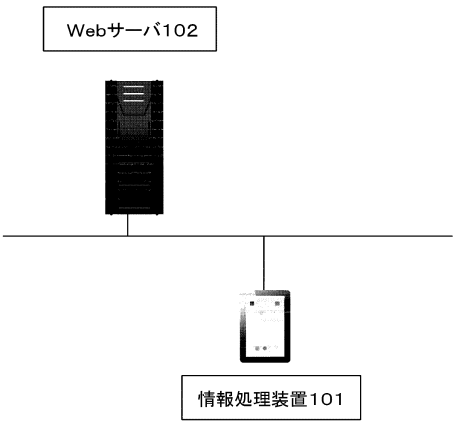
なお、上述した各実施形態およびその変形例を組み合わせた構成も全て本発明に含まれるものである。

【符号の説明】

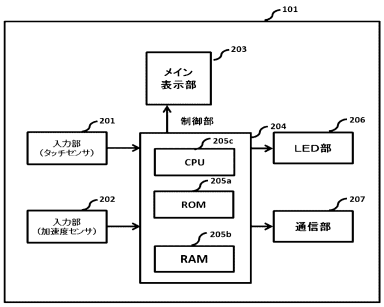
【０１３８】

１０１　クライアント端末
１０２　Ｗｅｂサーバ
１０３　ネットワーク
２０１　入力部（タッチセンサ）
２０２　入力部（加速度センサ）
２０３　メイン表示部
２０４　制御部
２０５ａ　ＲＯＭ
２０５ｂ　ＲＡＭ
２０５ｃ　ＣＰＵ
２０５　入力コントローラ
２０６　ＬＥＤ部
２０７　メモリコントローラ

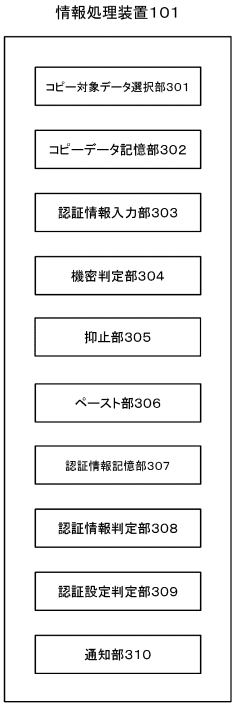
【図１】


Webサーバ102
情報処理装置101

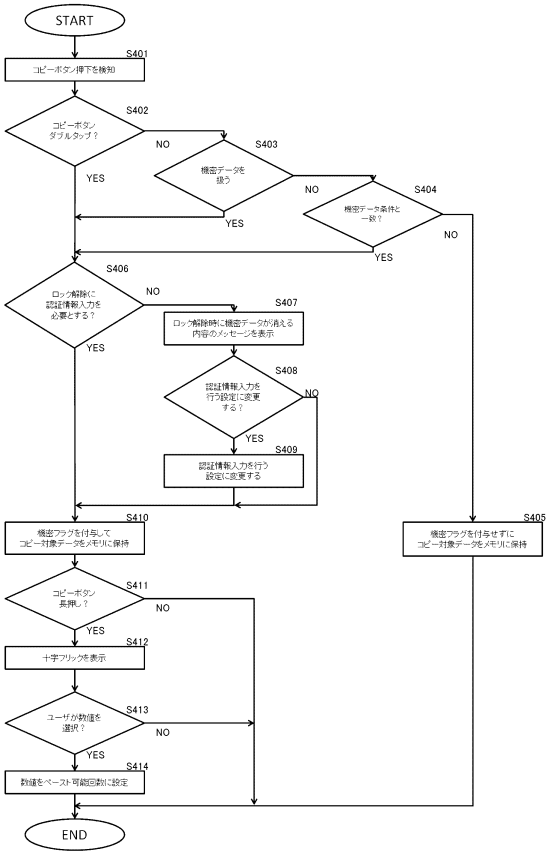
【図２】


101
203
メイン
表示部
制御部
201
入力部
（タッチセンサ）
205c
CPU
204
LED部
206
205a
ROM
202
入力部
（加速度センサ）
207
通信部
205b
RAM

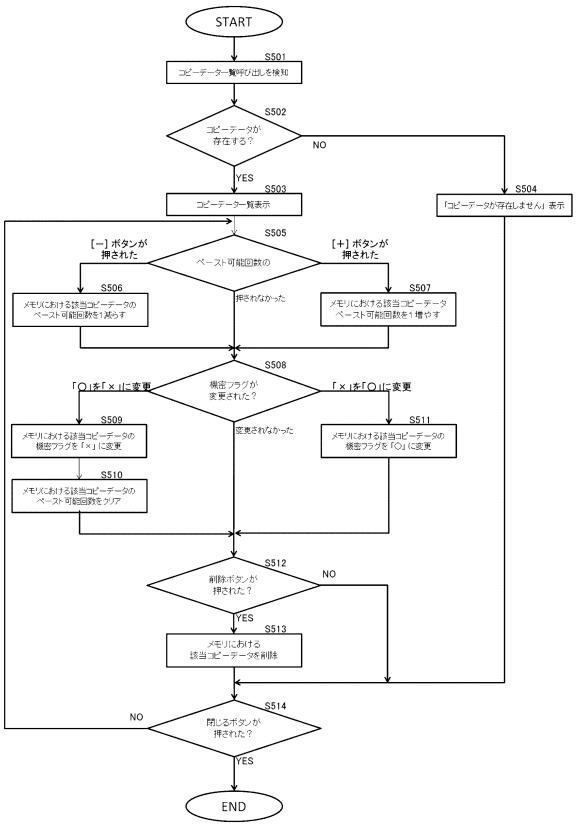
【図３】


情報処理装置101
コピー対象データ選択部301
コピーデータ記憶部302
認証情報入力部303
機密判定部304
抑止部305
ペースト部306
認証情報記憶部307
認証情報判定部308
認証設定判定部309
通知部310

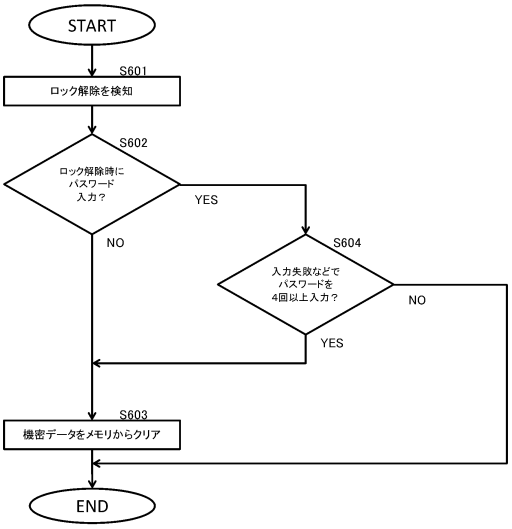
【図４】


START
S401
コピーボタン押下を検知
S402
コピーボタン
ダブルタップ？
NO
S403
機密データを
扱う
NO
S404
機密データ条件と
一致？
NO
YES
YES
YES
S406
ロック解除に
認証情報入力を
必要とする？
NO
S407
ロック解除時に機密データが消える
内容のメッセージを表示
S408
認証情報入力を
行う設定に変更
する？
NO
YES
S409
認証情報入力を行う
設定に変更する
YES
S410
機密フラグを付与して
コピー対象データをメモリに保持
S405
機密フラグを付与せずに
コピー対象データをメモリに保持
S411
コピーボタン
長押し？
NO
YES
S412
十字プリッタを表示
S413
ユーザが数値を
選択？
NO
YES
S414
数値をペースト可能回数に設定
END

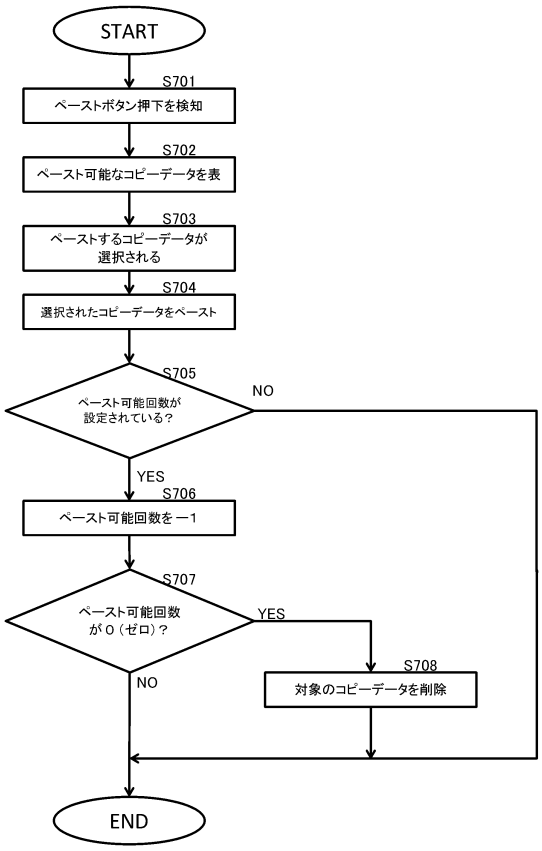
【図５】



【図６】



【図７】

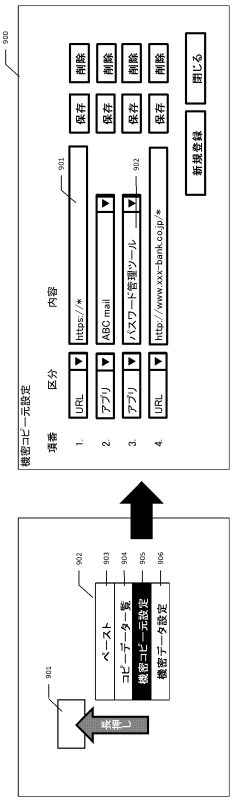


【図８】

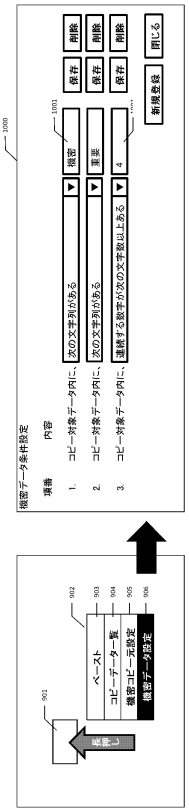
801 802 803

データ	ペースト可能回数	機密フラグ	
aaaaa		○	811
bb機密bb		○	812
ccccc		○	813
ddddd		×	814
eeeee		○	815
fffff	3	○	816

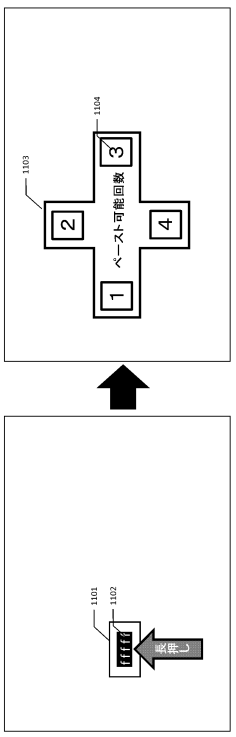
【図９】



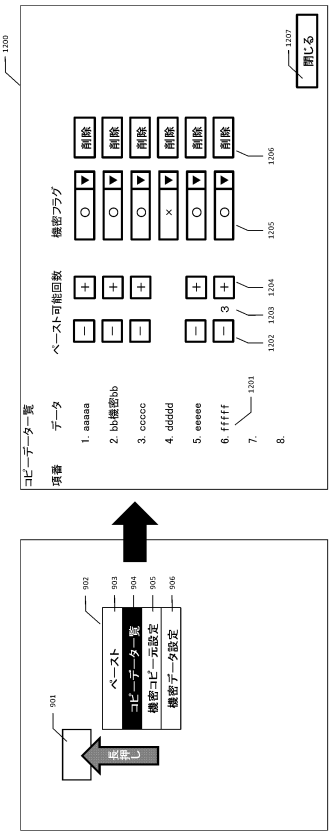
【図１０】



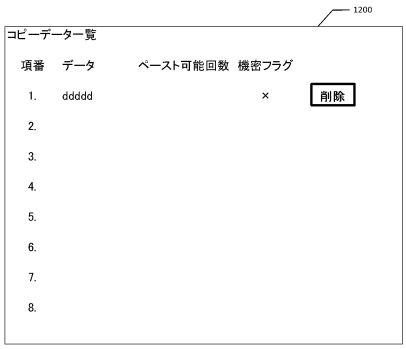
【図１１】



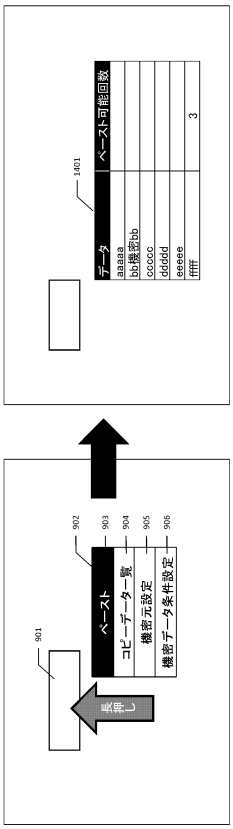
【図１２】



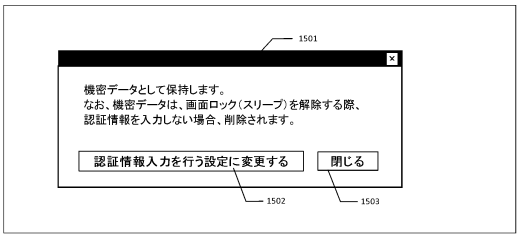
【図１３】



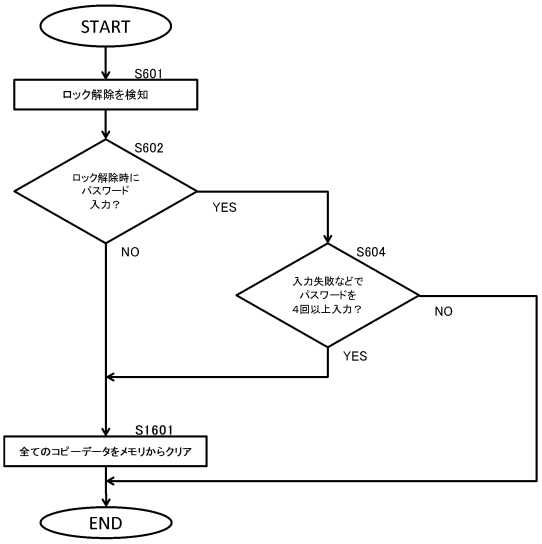
【図１４】



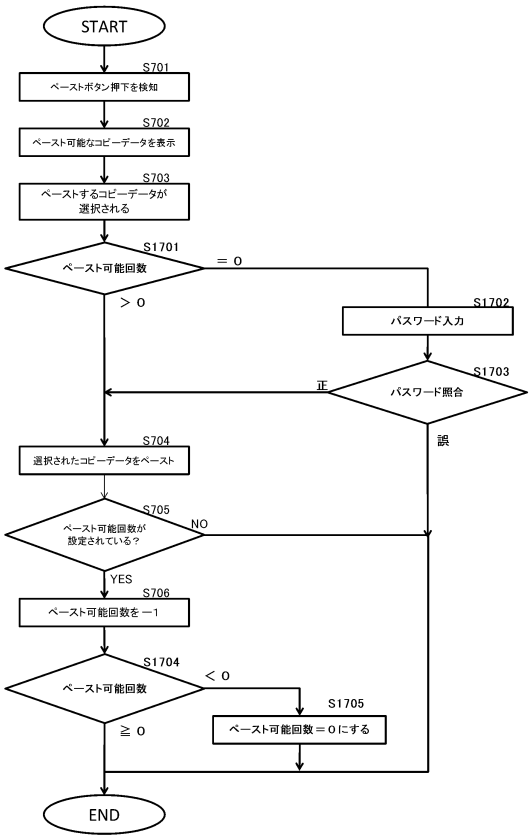
【図１５】



【図１６】



【図１７】


START
S701
ペーストボタン押下を検知
S702
ペースト可能なコピーデータを表示
S703
ペーストするコピーデータが選択される
S1701
ペースト可能回数
＝０
＞０
S1702
パスワード入力
S1703
パスワード照合
正
誤
S704
選択されたコピーデータをペースト
S705
ペースト可能回数が設定されている？
NO
YES
S706
ペースト可能回数を－1
S1704
ペースト可能回数
＜０
≧０
S1705
ペースト可能回数＝０にする
END

フロントページの続き

(72)発明者　池上　新吾
東京都品川区東品川２丁目４番１１号　キヤノンソフトウェア株式会社内

審査官　宮司　卓佳

(56)参考文献　国際公開第２０１３／０９６９４３（WO，Ａ１）
特開２００３－１２２４４３（ＪＰ，Ａ）
特開２０１３－０２０３０４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／００－２１／８８