(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6703270号
(P6703270)
(45)発行日　令和2年6月3日(2020.6.3)　(24)登録日　令和2年5月12日(2020.5.12)

(51)Int.Cl.　　F I
G06F 21/62 (2013.01)　G06F 21/62 309
G06F 21/31 (2013.01)　G06F 21/31
G06F 21/60 (2013.01)　G06F 21/60 320

請求項の数 25　(全 34 頁)

(21)出願番号　特願2016-153320 (P2016-153320)
(22)出願日　平成28年8月4日 (2016.8.4)
(65)公開番号　特開2018-22351 (P2018-22351A)
(43)公開日　平成30年2月8日 (2018.2.8)
審査請求日　平成31年4月23日 (2019.4.23)

特許法第３０条第２項適用　（１）掲載年月日：平成２８年６月８日　掲載アドレス：ｈｔｔｐ：／／ｂｕｆｆａｌｏ．ｊｐ／ｐｒｏｄｕｃｔ／ｕｓｂ－ｍｅｍｏｒｙ／ｓｐｅｅｄ／ｒｕｆ３－ｈｋｓ／＃ｆｅａｔｕｒｅ－４　（２）掲載年月日：平成２８年６月８日　掲載アドレス：ｈｔｔｐ：／／ｂｕｆｆａｌｏ．ｊｐ／ｎｅｗｓ／２０１６／０６／０８＿０３／

(73)特許権者　390040187
株式会社バッファロー
愛知県名古屋市中区大須三丁目３０番２０号
(74)代理人　110000028
特許業務法人明成国際特許事務所
(72)発明者　大野　崇仁
名古屋市中区大須三丁目３０番２０号　赤門通ビル　株式会社バッファロー内
(72)発明者　石井　俊
名古屋市中区大須三丁目３０番２０号　赤門通ビル　株式会社バッファロー内

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】外部記憶装置、暗号処理方法、暗号処理プログラム、及び暗号処理プログラムを格納した記憶媒体

(57)【特許請求の範囲】
【請求項１】
電子機器に接続される外部記憶装置であって、
暗号処理プログラムを格納しており、
前記暗号処理プログラムは、前記外部記憶装置が前記電子機器に接続された状態で前記電子機器のＯＳ上で起動されると、
前記電子機器の表示部に、暗号化を行いたいファイルが送られる複数のはりつけ領域を含む処理ウインドウを表示させる処理と、
前記複数のはりつけ領域のいずれかに前記暗号化を行いたいファイルが送られたときに、はりつけ領域ごとに予め定められた認証情報入力方法による認証情報のユーザ入力を行うための入力ウインドウを前記表示部に表示させると共に、前記認証情報のユーザ入力を受け付ける処理と、
前記認証情報のユーザ入力から秘密鍵を生成する処理と、
前記秘密鍵を用いて前記複数のはりつけ領域のいずれかに送られたファイルを暗号化するとともに、前記暗号化後の暗号化ファイルに前記認証情報入力方法を識別可能な識別子を付与する処理と、
前記暗号化ファイルを前記外部記憶装置に格納する処理と、
を前記電子機器に実行させる、外部記憶装置。
【請求項２】
請求項１に記載の外部記憶装置であって、さらに、

前記外部記憶装置を識別するための機器識別子を有しており、
前記暗号処理プログラムは、
前記処理ウインドウを表示させる処理の前に前記機器識別子を取得する処理と、
前記機器識別子が予め定められたものである場合は、前記処理ウインドウを表示させ、前記機器識別子が予め定められたものでない場合は、前記処理ウインドウを表示させずに前記暗号処理プログラムを終了する処理と、
を前記外部記憶装置に実行させる、外部記憶装置。
【請求項３】
請求項１または２に記載の外部記憶装置であって、前記暗号処理プログラムは、さらに、
前記処理ウインドウ内に、前記暗号処理プログラムによって暗号化された前記暗号化ファイルが送られたとき、前記暗号化ファイルが送られた位置が、前記暗号化ファイルが作成されたときのファイルが送られたはりつけ領域に該当するか否かに関わらず、前記暗号化ファイルの識別子に基づいて前記認証情報入力方法を特定し、特定された前記認証情報入力方法に従った前記認証情報のユーザ入力を受け付ける処理と、
前記認証情報のユーザ入力から前記秘密鍵を生成する処理と、
前記秘密鍵を用いて前記暗号化ファイルを復号する処理と、
前記暗号化ファイルを復号した復号ファイルを前記外部記憶装置に格納する処理と、
を前記電子機器に実行させる、外部記憶装置。
【請求項４】
請求項３に記載の外部記憶装置であって、
前記複数のはりつけ領域の１つに複数のファイルが送られたとき、
前記暗号処理プログラムは、
（ａ－ｉ）前記複数のファイルのうちの予め定められた規則に従って定められた最初のファイルが、前記暗号処理プログラムによって暗号化されていないファイルの場合には、前記はりつけ領域ごとに予め定められた認証情報入力方法による前記認証情報のユーザ入力を受け付け、前記認証情報のユーザ入力から前記秘密鍵を生成し、前記秘密鍵を用いて前記最初のファイルの暗号化を実行する処理と、
（ａ－ｉｉ）前記複数のファイルのうちの前記最初のファイル以外の各ファイルについては、当該ファイルが前記暗号処理プログラムによって暗号化されていないファイルの場合には、前記（ａ－ｉ）の処理で用いたのと同一の前記秘密鍵を用いて当該ファイルを暗号化し、当該ファイルが前記暗号処理プログラムによって暗号化された暗号化ファイルの場合には、暗号化も復号も実行しない処理と、
（ｂ－ｉ）前記最初のファイルが、前記暗号処理プログラムによって暗号化された暗号化ファイルの場合には、前記はりつけ領域ごとに予め定められた認証情報入力方法による前記認証情報のユーザ入力を受け付け、前記認証情報のユーザ入力から前記秘密鍵を生成し、前記秘密鍵を用いて前記最初のファイルの復号を実行する処理と、
（ｂ－ｉｉ）前記複数のファイルのうちの前記最初のファイル以外の各ファイルについては、当該ファイルが前記暗号処理プログラムによって暗号化された暗号化ファイルの場合には、前記（ｂ－ｉ）の処理で用いたのと同一の前記秘密鍵を用いて当該ファイルを復号し、当該ファイルが前記暗号処理プログラムによって暗号化されたファイルでない場合には、当該ファイルを暗号化も復号も実行しない処理と、
を前記電子機器に実行させる、外部記憶装置。
【請求項５】
請求項１から４のいずれか一項に記載の外部記憶装置であって、
前記暗号処理プログラムは、
前記複数のはりつけ領域のそれぞれが肉眼より識別可能な複数の小領域を有するように前記複数のはりつけ領域を形成する処理と、
前記複数の小領域のうちのいずれかの小領域に前記暗号化を行いたいファイルが送られたときに、前記暗号化を行いたいファイルが送られた小領域に応じて、異なる暗号強度の

暗号化方式に従って前記秘密鍵を生成する処理と、
を前記電子機器に実行させる、外部記憶装置。
【請求項６】
請求項１から５のいずれか一項に記載の外部記憶装置であって、
前記複数のはりつけ領域は、一部が重なっており、
前記暗号処理プログラムは、
互いに重なったＮ個（Ｎは２以上の整数）のはりつけ領域の重複部分に前記暗号化を行いたいファイルが送られたとき、前記Ｎ個のはりつけ領域に対応するＮ個の認証情報入力方法によるＮ個の認証情報のユーザ入力を受け付ける処理と、
前記Ｎ個の認証情報のユーザ入力から１つの前記秘密鍵を生成する処理と、
を前記電子機器に実行させる、外部記憶装置。
【請求項７】
請求項１から６のいずれか一項に記載の外部記憶装置であって、
前記暗号処理プログラムは、
前記複数のはりつけ領域のいずれかに送られたファイルのファイルサイズを取得する処理と、
前記ファイルサイズが予め定められた大きさ以上の場合には、前記認証情報入力方法による前記認証情報のユーザ入力を受けつける前に前記暗号化または復号する処理を実行できない旨の表示を行って前記暗号化または復号する処理を中止する同意を受け付ける処理と、
を前記電子機器に実行させ、
前記同意を得た場合には、前記電子機器に処理を中止させる、外部記憶装置。
【請求項８】
請求項１から７のいずれか一項に記載の外部記憶装置であって、
前記ファイルが前記はりつけ領域に送られることは、（ｉ）前記ファイルがコピーまたはカットされた後、前記ファイルが前記はりつけ領域にはりつけられること、または（２）前記ファイルがドラッグアンドドロップ操作されて、前記はりつけ領域にドロップされること、を含む、
外部記憶装置。
【請求項９】
暗号処理方法であって、
電子機器の表示部に、暗号化を行いたいファイルが送られるための複数のはりつけ領域を含む処理ウインドウを表示させ、
前記複数のはりつけ領域のいずれかに前記暗号化を行いたいファイルが送られたときに、はりつけ領域ごとに予め定められた認証情報入力方法による認証情報のユーザ入力を行うための入力ウインドウを前記表示部に表示させると共に、前記認証情報のユーザ入力を受け付け、
前記認証情報のユーザ入力から秘密鍵を生成し、
前記秘密鍵を用いて前記複数のはりつけ領域のいずれかに送られたファイルを暗号化するとともに、前記暗号化後の暗号化ファイルに前記認証情報入力方法を識別可能な識別子を付与し、
前記暗号化ファイルを外部記憶装置に格納する、
暗号処理方法。
【請求項１０】
請求項９に記載の暗号処理方法であって、
前記外部記憶装置は、前記外部記憶装置を識別するための機器識別子を有しており、
前記機器識別子を取得し、
前記機器識別子が予め定められたものである場合は、前記処理ウインドウを表示させ、前記機器識別子が予め定められたものでない場合は、前記処理ウインドウを表示させずに前記暗号処理方法を終了する、

暗号処理方法。
【請求項１１】
請求項９または１０に記載の暗号処理方法であって、さらに、
前記処理ウインドウ内に、前記暗号処理方法によって暗号化された前記暗号化ファイルが送られたとき、前記暗号化ファイルが送られた位置が、前記暗号化ファイルが作成されたときのファイルが送られたはりつけ領域に該当するか否かに関わらず、前記暗号化ファイルの識別子に基づいて前記認証情報入力方法を特定し、特定された前記認証情報入力方法に従った前記認証情報のユーザ入力を受け付け、
前記認証情報のユーザ入力から前記秘密鍵を生成し、
前記秘密鍵を用いて前記暗号化ファイルを復号し、
前記暗号化ファイルを復号した復号ファイルを前記外部記憶装置に格納する、
暗号処理方法。
【請求項１２】
請求項１１に記載の暗号処理方法であって、
前記複数のはりつけ領域の１つに複数のファイルが送られたとき、
（ａ－ｉ）前記複数のファイルのうちの予め定められた規則に従って定められた最初のファイルが、前記暗号処理方法によって暗号化されていないファイルの場合には、前記はりつけ領域ごとに予め定められた認証情報入力方法による前記認証情報のユーザ入力を受け付け、前記認証情報のユーザ入力から前記秘密鍵を生成し、前記秘密鍵を用いて前記最初のファイルの暗号化を実行し、
（ａ－ｉｉ）前記複数のファイルのうちの前記最初のファイル以外の各ファイルについては、当該ファイルが前記暗号処理方法によって暗号化されていないファイルの場合には、前記（ａ－ｉ）の処理で用いたのと同一の前記秘密鍵を用いて当該ファイルを暗号化し、当該ファイルが前記暗号処理方法によって暗号化された暗号化ファイルの場合には、暗号化も復号も実行せず、
（ｂ－ｉ）前記最初のファイルが、前記暗号処理方法によって暗号化された暗号化ファイルの場合には、前記はりつけ領域ごとに予め定められた認証情報入力方法による前記認証情報のユーザ入力を受け付け、前記認証情報のユーザ入力から前記秘密鍵を生成し、前記秘密鍵を用いて前記最初のファイルの復号を実行し、
（ｂ－ｉｉ）前記複数のファイルのうちの前記最初のファイル以外の各ファイルについては、当該ファイルが前記暗号処理方法によって暗号化された暗号化ファイルの場合には、前記（ｂ－ｉ）の処理で用いたのと同一の前記秘密鍵を用いて当該ファイルを復号し、当該ファイルが前記暗号処理方法によって暗号化されたファイルでない場合には、当該ファイルを暗号化も復号も実行しない、
暗号処理方法。
【請求項１３】
請求項９から１２のいずれか一項に記載の暗号処理方法であって、
前記複数のはりつけ領域のそれぞれが肉眼より識別可能な複数の小領域を有するように前記複数のはりつけ領域を形成し、
前記複数の小領域のうちのいずれかの小領域に前記暗号化を行いたいファイルが送られたときに、前記暗号化を行いたいファイルが送られた小領域に応じて、異なる暗号強度の暗号化方式に従って秘密鍵を生成する、
暗号処理方法。
【請求項１４】
請求項９から１３のいずれか一項に記載の暗号処理方法であって、
前記複数のはりつけ領域は、一部が重なっており、
互いに重なったＮ個（Ｎは２以上の整数）のはりつけ領域の重複部分に前記暗号化を行いたいファイルが送られたとき、前記Ｎ個のはりつけ領域に対応するＮ個の認証情報入力方法によるＮ個の認証情報のユーザ入力を受け付け、
前記Ｎ個の認証情報のユーザ入力から１つの前記秘密鍵を生成する、

暗号処理方法。
【請求項１５】
請求項９から１４のいずれか一項に記載の暗号処理方法であって、
前記複数のはりつけ領域のいずれかに送られたファイルのファイルサイズを取得し、
前記ファイルサイズが予め定められた大きさ以上の場合には、前記認証情報入力方法による前記認証情報のユーザ入力を受けつける前に前記暗号化または復号する処理を実行できない旨の表示を行って前記暗号化または復号する処理を中止する同意を受け付け、
前記同意を得た場合には、処理を中止する、
暗号処理方法。
【請求項１６】
請求項９から１５のいずれか一項に記載の暗号処理方法であって、
前記ファイルが前記はりつけ領域に送られることは、（ｉ）前記ファイルがコピーまたはカットされた後、前記ファイルが前記はりつけ領域にはりつけられること、または（２）前記ファイルがドラッグアンドドロップ操作されて、前記はりつけ領域にドロップされること、を含む、
暗号処理方法。
【請求項１７】
暗号処理プログラムであって、
電子機器の表示部に、暗号化を行いたいファイルが送られる複数のはりつけ領域を含む処理ウインドウを表示させる処理と、
前記複数のはりつけ領域のいずれかに前記暗号化を行いたいファイルが送られたときに、はりつけ領域ごとに予め定められた認証情報入力方法による認証情報のユーザ入力を行うための入力ウインドウを前記表示部に表示させると共に、前記認証情報のユーザ入力を受け付ける処理と、
前記認証情報のユーザ入力から秘密鍵を生成する処理と、
前記秘密鍵を用いて前記複数のはりつけ領域のいずれかに送られたファイルを暗号化するとともに、前記暗号化後の暗号化ファイルに前記認証情報入力方法を識別可能な識別子を付与する処理と、
前記暗号化ファイルを外部記憶装置に格納する処理と、
を前記電子機器に実行させる、暗号処理プログラム。
【請求項１８】
請求項１７に記載の暗号処理プログラムであって、さらに、
前記外部記憶装置は、前記外部記憶装置を識別するための機器識別子を有しており、
前記暗号処理プログラムは、
前記機器識別子を取得する処理と、
前記機器識別子が予め定められたものである場合は、前記処理ウインドウを表示させ、前記機器識別子が予め定められたものでない場合は、前記処理ウインドウを表示させずに前記暗号処理プログラムを終了する処理と、
を前記外部記憶装置に実行させる、暗号処理プログラム。
【請求項１９】
請求項１７または１８に記載の暗号処理プログラムであって、さらに、
前記処理ウインドウ内に、前記暗号処理プログラムによって暗号化された前記暗号化ファイルが送られたとき、前記暗号化ファイルが送られた位置が、前記暗号化ファイルが作成されたときのファイルが送られたはりつけ領域に該当するか否かに関わらず、前記暗号化ファイルの識別子に基づいて前記認証情報入力方法を特定し、特定された前記認証情報入力方法に従った前記認証情報のユーザ入力を受け付ける処理と、
前記認証情報のユーザ入力から前記秘密鍵を生成する処理と、
前記秘密鍵を用いて前記暗号化ファイルを復号する処理と、
前記暗号化ファイルを復号した復号ファイルを前記外部記憶装置に格納する処理と、
を前記電子機器に実行させる、暗号処理プログラム。

【請求項２０】
請求項１９に記載の暗号処理プログラムであって、
前記複数のはりつけ領域の１つに複数のファイルがドロップされたとき、
（ａ－ｉ）前記複数のファイルのうちの予め定められた規則に従って定められた最初のファイルが、前記暗号処理プログラムによって暗号化されていないファイルの場合には、前記はりつけ領域ごとに予め定められた認証情報入力方法による前記認証情報のユーザ入力を受け付け、前記認証情報のユーザ入力から前記秘密鍵を生成し、前記秘密鍵を用いて前記最初のファイルの暗号化を実行する処理と、
（ａ－ｉｉ）前記複数のファイルのうちの前記最初のファイル以外の各ファイルについては、当該ファイルが前記暗号処理プログラムによって暗号化されていないファイルの場合には、前記（ａ－ｉ）の処理で用いたのと同一の前記秘密鍵を用いて当該ファイルを暗号化し、当該ファイルが前記暗号処理プログラムによって暗号化された暗号化ファイルの場合には、暗号化も復号も実行しない処理と、
（ｂ－ｉ）前記最初のファイルが、前記暗号処理プログラムによって暗号化された暗号化ファイルの場合には、前記はりつけ領域ごとに予め定められた認証情報入力方法による前記認証情報のユーザ入力を受け付け、前記認証情報のユーザ入力から前記秘密鍵を生成し、前記秘密鍵を用いて前記最初のファイルの復号を実行する処理と、
（ｂ－ｉｉ）前記複数のファイルのうちの前記最初のファイル以外の各ファイルについては、当該ファイルが前記暗号処理プログラムによって暗号化された暗号化ファイルの場合には、前記（ｂ－ｉ）の処理で用いたのと同一の前記秘密鍵を用いて当該ファイルを復号し、当該ファイルが前記暗号処理プログラムによって暗号化されたファイルでない場合には、当該ファイルを暗号化も復号も実行しない処理と、
を前記電子機器に実行させる、暗号処理プログラム。
【請求項２１】
請求項１７から２０のいずれか一項に記載の暗号処理プログラムであって、
前記複数のはりつけ領域のそれぞれが肉眼より識別可能な複数の小領域を有するように前記複数のはりつけ領域を形成する処理と、
前記複数の小領域のうちのいずれかの小領域に前記暗号化を行いたいファイルが送られたときに、前記暗号化を行いたいファイルが送られた小領域に応じて、異なる暗号強度の暗号化方式に従って前記秘密鍵を生成する処理と、
を前記電子機器に実行させる、暗号処理プログラム。
【請求項２２】
請求項１７から２１のいずれか一項に記載の暗号処理プログラムであって、
前記複数のはりつけ領域は、一部が重なっており、
互いに重なったＮ個（Ｎは２以上の整数）のはりつけ領域の重複部分に前記暗号化を行いたいファイルが送られたとき、前記Ｎ個のはりつけ領域に対応するＮ個の認証情報入力方法によるＮ個の認証情報のユーザ入力を受け付ける処理と、
前記Ｎ個の認証情報のユーザ入力から１つの前記秘密鍵を生成する処理と、
を前記電子機器に実行させる、暗号処理プログラム。
【請求項２３】
請求項１７から２２のいずれか一項に記載の暗号処理プログラムであって、
前記複数のはりつけ領域のいずれかに送られたファイルのファイルサイズを取得する処理と、
前記ファイルサイズが予め定められた大きさ以上の場合には、前記認証情報入力方法による前記認証情報のユーザ入力を受けつける前に前記暗号化または復号する処理を実行できない旨の表示を行って前記暗号化または復号する処理を中止する同意を受け付ける処理と、
を前記電子機器に実行させ、
前記同意を得た場合には、前記電子機器に処理を中止させる、暗号処理プログラム。
【請求項２４】

請求項１７から２３のいずれか一項に記載の暗号処理プログラムであって、
前記ファイルが前記はりつけ領域に送られることは、（ｉ）前記ファイルがコピーまたはカットされた後、前記ファイルが前記はりつけ領域にはりつけられること、または（２）前記ファイルがドラッグアンドドロップ操作されて、前記はりつけ領域にドロップされること、を含む、
暗号処理プログラム。
【請求項２５】
請求項１７から２４のいずれか一項に記載の暗号処理プログラムを格納した記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、外部記憶装置、暗号処理方法、暗号処理プログラム、及び暗号処理プログラムを格納した記憶媒体。
【背景技術】
【０００２】
引用文献１には、金庫を模倣しアイコンを対象として、ドラッグアンドドロップという直感的な操作により、ファイル暗号化の操作を実現し、さらに、ユーザ認証用のパスワードから自動的にファイルの暗号化・復号に使う暗号鍵を生成して暗号化を行うことが開示されている。特許文献１の技術では、暗号化されたファイルを格納する暗号フォルダを作成するときにユーザより入力された任意数字と、ユーザが暗号フォルダにアクセスするときに認証に用いるパスワードとを用いて暗号鍵を作成する。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開平０９－２０４３３０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
ユーザの認証には、パスワード入力やパターン入力、ＮＦＣ、生体認証など、さまざまな認証方法があるが、特許文献１の技術では、複数の認証方法に対応できないという問題があり、ファイルの暗号化や復号において、利便性が悪かった。
【課題を解決するための手段】
【０００５】
上記した課題を達成するために、本発明は、以下の形態として実施することができる。
【０００６】
（１）本発明の一形態によれば、電子機器に接続される外部記憶装置が提供される。この外部記憶装置は、暗号処理プログラムを格納しており、前記暗号処理プログラムは、前記外部記憶装置が前記電子機器に接続された状態で前記電子機器のＯＳ上で起動されると、前記電子機器の表示部に、暗号化を行いたいファイルが送られるための複数のはりつけ領域を含む処理ウインドウを表示させる処理と、前記複数のはりつけ領域のいずれかに前記暗号化を行いたいファイルが送られたときに、はりつけ領域ごとに予め定められた認証情報入力方法による認証情報のユーザ入力を行うための入力ウインドウを前記表示部に表示させると共に、前記認証情報のユーザ入力を受け付ける処理と、前記認証情報のユーザ入力から秘密鍵を生成する処理と、前記秘密鍵を用いて前記複数のはりつけ領域のいずれかに送られたファイルを暗号化するとともに、前記暗号化後の暗号化ファイルに前記認証情報入力方法を識別可能な識別子を付与する処理と、前記暗号化ファイルを前記外部記憶装置に格納する処理と、を前記電子機器に実行させる。
この形態によれば、ユーザがどちらのはりつけ領域にファイルを送るかにより認証情報入力方法を選択できるので、ファイルの暗号化における利便性を向上させることができる。

【０００７】
（２）上記形態の暗号化処理装置であって、前記外部記憶装置を識別するための機器識別子を有しており、前記暗号処理プログラムは、前記処理ウインドウを表示させる処理の前に前記機器識別子を取得する処理と、前記機器識別子が予め定められたものである場合は、前記処理ウインドウを表示させ、前記機器識別子が予め定められたものでない場合は、前記処理ウインドウを表示させずに前記暗号処理プログラムを終了する処理と、を前記外部記憶装置に実行させてもよい。
この形態によれば、暗号処理プログラムが不正にコピーされても、正規な外部記憶装置が接続されたときでなければ暗号処理プログラムが終了するので、暗号化処理を実行できない。その結果、不正なコピーの拡散を抑制できる。
【０００８】
（３）上記形態の暗号化処理装置であって、前記暗号処理プログラムは、さらに、前記処理ウインドウ内に、前記暗号処理プログラムによって暗号化された前記暗号化ファイルが送られたとき、前記暗号化ファイルが送られた位置が、前記暗号化ファイルが作成されたときのファイルが送られたはりつけ領域に該当するか否かに関わらず、前記暗号化ファイルの識別子に基づいて前記認証情報入力方法を特定し、特定された前記認証情報入力方法に従った前記認証情報のユーザ入力を受け付ける処理と、前記認証情報のユーザ入力から前記秘密鍵を生成する処理と、前記秘密鍵を用いて前記暗号化ファイルを復号する処理と、前記暗号化ファイルを復号した復号ファイルを前記外部記憶装置に格納する処理と、を前記電子機器に実行させてもよい。
この形態によれば、ユーザは、復号時にどちらのはりつけ領域にファイルを送るかを考慮しなくてもよいので、暗号化されたファイルの復号における利便性を向上させることができる。
【０００９】
（４）上記形態の暗号化処理装置であって、前記複数のはりつけ領域の１つに複数のファイルが送られたとき、前記暗号処理プログラムは、（ａ－ｉ）前記複数のファイルのうちの予め定められた規則に従って定められた最初のファイルが、前記暗号処理プログラムによって暗号化されていないファイルの場合には、前記はりつけ領域ごとに予め定められた認証情報入力方法による前記認証情報のユーザ入力を受け付け、前記認証情報のユーザ入力から前記秘密鍵を生成し、前記秘密鍵を用いて前記最初のファイルの暗号化を実行する処理と、（ａ－ｉｉ）前記複数のファイルのうちの前記最初のファイル以外の各ファイルについては、当該ファイルが前記暗号処理プログラムによって暗号化されていないファイルの場合には、前記（ａ－ｉ）の処理で用いたのと同一の前記秘密鍵を用いて当該ファイルを暗号化し、当該ファイルが前記暗号処理プログラムによって暗号化された暗号化ファイルの場合には、暗号化も復号も実行しない処理と、（ｂ－ｉ）前記最初のファイルが、前記暗号処理プログラムによって暗号化された暗号化ファイルの場合には、前記はりつけ領域ごとに予め定められた認証情報入力方法による前記認証情報のユーザ入力を受け付け、前記認証情報のユーザ入力から前記秘密鍵を生成し、前記秘密鍵を用いて前記最初のファイルの復号を実行する処理と、（ｂ－ｉｉ）前記複数のファイルのうちの前記最初のファイル以外の各ファイルについては、当該ファイルが前記暗号処理プログラムによって暗号化された暗号化ファイルの場合には、前記（ｂ－ｉ）の処理で用いたのと同一の前記秘密鍵を用いて当該ファイルを復号し、当該ファイルが前記暗号処理プログラムによって暗号化されたファイルでない場合には、当該ファイルを暗号化も復号も実行しない処理と、を前記電子機器に実行させてもよい。
この形態によれば、最初のファイルの処理が暗号化処理の場合には、同時に送られた暗号化されていないファイルを暗号化でき、最初のファイルの処理が復号処理の場合には、同時に送られた暗号化ファイルを復号できるので、複数のファイルの暗号化、復号における利便性を向上させることができる。
【００１０】
（５）上記形態の暗号化処理装置であって、前記暗号処理プログラムは、前記複数のは

りつけ領域のそれぞれが肉眼より識別可能な複数の小領域を有するように前記複数のはりつけ領域を形成する処理と、前記複数の小領域のうちのいずれかの小領域に前記暗号化を行いたいファイルが送られたときに、前記暗号化を行いたいファイルが送られた小領域に応じて、異なる暗号強度の暗号化方式に従って前記秘密鍵を生成する処理と、を前記電子機器に実行してもよい。

一般に暗号強度を強くすれば、暗号化や復号の処理時間がかかる。この形態によれば、処理時間はかかるが暗号強度を強くするか、暗号強度は弱いが処理時間を短くするか、ユーザが選択または決定することができ、ファイルの暗号化における利便性及びセキュリティを向上させることができる。

【００１１】

（６）上記形態の暗号化処理装置であって、前記複数のはりつけ領域は、一部が重なっており、前記暗号処理プログラムは、互いに重なったＮ個（Ｎは２以上の整数）のはりつけ領域の重複部分に前記暗号化を行いたいファイルが送られたとき、前記Ｎ個のはりつけ領域に対応するＮ個の認証情報入力方法によるＮ個の認証情報のユーザ入力を受け付ける処理と、前記Ｎ個の認証情報のユーザ入力から１つの前記秘密鍵を生成する処理と、を前記電子機器に実行させてもよい。

この形態によれば、複数の認証情報入力方式でユーザ入力を行うので、ファイルの暗号化におけるセキュリティを向上させることができる。

【００１２】

（７）上記形態の暗号化処理装置であって、前記暗号処理プログラムは、前記複数のはりつけ領域のいずれかに送られたファイルのファイルサイズを取得する処理と、前記ファイルサイズが予め定められた大きさ以上の場合には、前記認証情報入力方法による前記認証情報のユーザ入力を受けつける前に前記暗号化または復号する処理を実行できない旨の表示を行って前記暗号化または復号する処理を中止する同意を受け付ける処理と、を前記電子機器に実行させ、前記同意を得た場合には、前記電子機器に処理を中止させてもよい。

この形態によれば、ファイルサイズが大きく、暗号化、復号に時間がかかるときには、暗号化または復号する処理を実行できない旨の表示を行い、ユーザの同意を得て暗号化または復号する処理を中止するので、暗号化または復号する処理を開始してから中止するよりも暗号化、復号における利便性を向上させることができる。

【００１３】

（８）上記形態の暗号化処理装置であって、前記ファイルが前記はりつけ領域に送られることは、（ｉ）前記ファイルがコピーまたはカットされた後、前記ファイルが前記はりつけ領域にはりつけられること、または（２）前記ファイルがドラッグアンドドロップ操作されて、前記はりつけ領域にドロップされること、を含んでもよい。

この形態によれば、ユーザが、ファイルをコピーして貼付（コピー＆ペースト）してもよく、ファイルをドラッグアンドドロップしてもよいので、ユーザの利便性を向上させることができる。

【００１４】

なお、本発明は、種々の形態で実現することが可能であり、例えば、外部記憶装置の他、暗号化処理装置、暗号処理方法、暗号処理プログラム、暗号処理プログラムを格納した記憶媒体、暗号化処理のためのユーザインターフェース等の形態で実現することができる。

【図面の簡単な説明】

【００１５】

【図１】第１の実施形態の外部記憶装置と、電子機器を示す説明図。

【図２】第１の実施形態における動作フローチャート。

【図３】ユーザが暗号処理プログラムを起動したときの電子機器の表示部に表示される画面の一例。

【図４】暗号化されていないファイルの第１ドロップ領域へのドラッグ＆ドロップの一例

を示す説明図。
【図５】ステップＳ１６０で表示される第１認証情報入力方式の入力画面の一例。
【図６】ステップＳ１８０で表示される第２認証情報入力方式の入力画面の一例。
【図７】暗号化処理後の表示部に表示される画面の一例。
【図８】暗号化ファイルのドラッグ＆ドロップの一例を示す説明図。
【図９】復号処理後の表示部に表示される画面の一例。
【図１０】第２の実施形態の外部記憶装置と、電子機器を示す説明図。
【図１１】第２の実施形態における動作フローチャート。
【図１２】第３の実施形態における動作フローチャート。
【図１３】第３の実施形態における複数のファイルの第１ドロップ領域へのドラッグ＆ドロップの一例を示す説明図。
【図１４】第３の実施形態の暗号化または復号の処理後における表示部に表示される画面の一例。
【図１５】第３の実施形態における複数のファイルの第１ドロップ領域へのドラッグ＆ドロップの一例を示す説明図。
【図１６】第３の実施形態の暗号化または復号の処理後における表示部に表示される画面の一例。
【図１７】第３の実施形態におけるフォルダの第１ドロップ領域へのドラッグ＆ドロップの一例を示す説明図。
【図１８】フォルダをドロップしたときの暗号化または復号の処理後における表示部に表示される画面の一例。
【図１９】第４の実施形態における暗号処理プログラムを起動したときの表示部に表示される画面の一例。
【図２０】第５の実施形態における暗号処理プログラムを起動したときの表示部に表示される画面の一例。
【図２１】第５の実施形態における動作フローチャート。
【図２２】第６の実施形態の外部記憶装置と、電子機器を示す説明図。
【図２３】第６の実施形態における動作フローチャート。
【発明を実施するための形態】
【００１６】
・第１の実施形態：
図１は、第１の実施形態の外部記憶装置１００と、電子機器２００を示す説明図である。電子機器２００は、外部記憶装置１００を接続可能な機器であり、例えば、コンピュータ、タブレット端末、スマートホンを含む。電子機器２００は、ＣＰＵ２１０と、記憶部２２０と、入力部２３０と、表示部２４０と、インターフェース２６０（「Ｉ／Ｆ２６０」とも呼ぶ。）と、コネクタ２７０と、を備える。記憶部２２０は、オペレーティングシステム２２５（「ＯＳ２２５」と呼ぶ。）を格納している。ＯＳ２２５は、電子機器２００を利用するための基本ソフトウェアである。入力部２３０は、ユーザからの入力を受け付けるための装置である。入力部２３０としては、例えば、キーボードやマウス、トラックボール、タブレット等が利用可能である。表示部２４０は、ユーザへの情報を表示するための表示装置である。なお、表示部２４０をタッチパネル等で構成することにより、表示部２４０を入力部を兼ねる入力部兼表示部として構成してもよい。但し、この場合であっても、入力部２３０を別途備えていてもよい。コネクタ２７０は、外部記憶装置１００を接続するためのコネクタである。コネクタ２７０としては、例えば、ＵＳＢコネクタ（「ＵＳＢ」は登録商標）や、ＩＥＥＥ１３９４コネクタ、メモリーカード用コネクタが利用可能である。なお、コネクタ２７０は、ホットプラグ対応のコネクタが好ましい。ホットプラグとは、電子機器２００の電源を切ることなく、コネクタ２７０に接続しているコネクタ（外部記憶装置１００のコネクタ１７０）を抜き差しすることができる機能を言う。また、第１の実施形態では、電子機器２００と外部記憶装置１００との間を、コネクタ２７０、１７０を用いた有線により接続しているが、無線による接続であってもよい。こ

の場合、コネクタ２７０に代えてあるいは、コネクタ２７０とともに、無線接続装置を備えていてもよい。コネクタ２７０は、インターフェース２６０を介してＣＰＵ２１０に接続されている。

【００１７】

外部記憶装置１００は、ＵＳＢコネクタやＩＥＥＥ１３９４コネクタ、メモリーカード用コネクタにより電子機器２００に接続される装置であり、例えば、ＵＳＢやＩＥＥＥ１３９４で接続されるハードディスク、ＵＳＢやＩＥＥＥ１３９４で接続されるＳＳＤ、ＵＳＢメモリの他、ＳＤカード、コンパクトフラッシュ（登録商標）、メモリースティック（登録商標）などのメモリーカードが含まれる。外部記憶装置１００は、制御部１１０と、記憶部１２０と、インターフェース１６０と、コネクタ１７０と、を備える。記憶部１２０は、暗号処理プログラム１３０と、格納フォルダ１５０と、を有している。

【００１８】

暗号処理プログラム１３０は、電子機器２００のＣＰＵ２１０によって実行されるプログラムであり、処理ウインドウ形成部１３２と、認証情報入力部１３４と、ファイル判定部１３６と、秘密鍵生成部１３８と、暗号化処理部１４０と、復号処理部１４２とを備える。処理ウインドウ形成部１３２は、電子機器２００の表示部２４０に、暗号化を行いたいファイルがドラッグアンドドロップされる複数のドロップ領域を含む処理ウインドウを表示する。ドロップ領域は、ファイルが送られるはりつけ領域である。

【００１９】

認証情報入力部１３４は、ファイルが複数のドロップ領域のいずれかにドロップされたときには、そのドロップ領域に応じて予め決められている認証情報入力方式による認証情報入力ウインドウを電子機器２００の表示部２４０に表示する。その後、認証情報入力ウインドウに入力された認証情報のユーザ入力を受け付ける。なお、ユーザは、電子機器２００の入力部２３０により認証情報入力ウインドウへの認証情報のユーザ入力を行なう。

【００２０】

ファイル判定部１３６は、ドロップ領域にドロップされたファイルが暗号処理プログラム１３０により暗号化された暗号化ファイルか否かを判定する。第１の実施形態では、ドロップ領域にドロップされたファイルが暗号処理プログラム１３０により暗号化された暗号化ファイルの場合には、暗号処理プログラム１３０は、暗号化する処理ではなく、復号する処理を行うからである。ファイル判定部１３６は、例えばファイルの拡張子に基づいてこの判定を行う。したがって、暗号化後に拡張子が変更されるようなファイル名の変更があった場合には、２重に暗号化される。また、暗号処理プログラム１３０以外の暗号処理プログラムにより暗号化されている場合にも、拡張子が異なれば、同様に２重に暗号化される。なお、暗号化されていないファイルの拡張子が変更され、暗号処理プログラム１３０により暗号化された暗号化ファイルと同じ拡張子となっていた場合には、暗号処理プログラム１３０は、復号する処理を実行しようとする。しかし、この場合、認証情報入力方式や秘密鍵が不一致となるため、そのファイルは復号されない。

【００２１】

秘密鍵生成部１３８は、認証情報入力ウインドウに入力された認証情報のユーザ入力に基づいて、秘密鍵を生成する。したがって、認証情報入力ウインドウに入力された認証情報のユーザ入力が同じ場合には、同じ秘密鍵が生成される。なお、秘密鍵は、外部に取り出せないことが好ましい。暗号化処理部１４０は、秘密鍵を用いてファイルを暗号化する処理を行う。復号処理部１４２は、秘密鍵を用いて暗号化ファイルを復号する処理を行う。

【００２２】

格納フォルダ１５０は、暗号化された暗号化ファイルを格納するフォルダである。第１の実施形態では、格納フォルダ１５０は、外部記憶装置１００の記憶部１２０のフォルダ階層上の一番上位（「ルートフォルダ」とも呼ぶ。）に作成されている。但し、格納フォルダ１５０は、外部記憶装置１００の記憶部１２０の中であれば、ルートフォルダに作成されていなくてもよい。なお、外部記憶装置１００は、初期設定において、格納フォルダ

１５０の場所を外部記憶装置１００の記憶部１２０のルートフォルダとする構成とし、その後、ユーザが格納フォルダ１５０の場所を任意の場所に変えられる構成としてもよい。この場合であっても、格納フォルダ１５０は、外部記憶装置１００の記憶部１２０の中に作成されることが好ましい。なお、復号されたファイルも、格納フォルダ１５０に格納される。

【００２３】

コネクタ１７０は、電子機器２００のコネクタ２７０と対応するコネクタである。コネクタ１７０の代わりに無線接続装置を備えていてもよい。この場合、外部記憶装置１００は、電子機器２００と無線接続される。コネクタ１７０は、インターフェース１６０を介して制御部１１０に接続されている。

【００２４】

図２は、第１の実施形態における動作フローチャートである。ステップＳ１００では、ユーザが、外部記憶装置１００を電子機器２００に接続する。ステップＳ１１０では、ユーザが、外部記憶装置１００の記憶部１２０に格納されている暗号処理プログラム１３０（図１参照）を起動する。ステップＳ１２０では、処理ウインドウ形成部１３２が、電子機器２００の表示部２４０に処理ウインドウを形成する。

【００２５】

図３は、ユーザが暗号処理プログラム１３０を起動したときの電子機器２００の表示部２４０に表示される画面の一例である。図３では、表示部２４０に、処理ウインドウ３００と、ドキュメントフォルダを示すウインドウ４００と、外部記憶装置１００の記憶部１２０に格納されているフォルダやファイルの構成を示すウインドウ５００が表示されている。

【００２６】

ウインドウ４００、５００は、ユーザが、ＯＳ２２５に所定の操作を行うことで、表示部２４０に表示させる。ウインドウ４００には、ドキュメントフォルダに含まれる子フォルダやファイルが表示されている。ドキュメントフォルダは、第１の実施形態のユーザがファイルの格納に用いているフォルダである。但し、ユーザによりファイルの格納に用いるフォルダやドライブは異なるため、ユーザがファイルの格納に用いているフォルダは、ドキュメントフォルダとは限らない。ウインドウ５００には、外部記憶装置１００の、格納フォルダ１５０を示すアイコン５１５０と、暗号処理プログラム１３０を示すアイコン５１３０が表示されている。本実施形態では、暗号処理プログラム１３０は、ｃｒｙｐｔ．ｅｘｅというファイル名であり、格納フォルダ１５０は、ＳｅｃｕｒｅＬｏｃｋＭｏｂｉｌｅ２というフォルダ名である。なお、暗号処理プログラム１３０や格納フォルダ１５０の名前は一例であり、これ以外の名前であってもよい。ユーザが、ウインドウ５００の暗号処理プログラム１３０（ｃｒｙｐｔ．ｅｘｅ）を選択して起動することで、処理ウインドウ３００が表示される。

【００２７】

処理ウインドウ３００は、第１ドロップ領域３１０と、第２ドロップ領域３２０と、ステータスバー３３０とを含んでいる。第１ドロップ領域３１０と、第２ドロップ領域３２０は、暗号化あるいは復号したいファイルやフォルダ、具体的にはファイルやフォルダに対応するアイコン、をドラッグした後ドロップする（「ドラッグアンドドロップする」（「ドラッグ＆ドロップ」と略す。）あるいは単に「ドロップする」とも呼ぶ。）領域である。第１ドロップ領域３１０と、第２ドロップ領域３２０は、領域を区別するため、異なる色または異なるタイルパターンで表示されることが好ましい。第１ドロップ領域３１０に暗号処理プログラム１３０により暗号化された暗号化ファイルでないファイルがドロップされたとき第１認証情報入力方式（パスワード方式）による認証情報のユーザ入力が行われ、第２ドロップ領域３２０に暗号処理プログラム１３０により暗号化された暗号化ファイルでないファイルがドロップされたとき第２認証情報入力方式（パターン方式）による認証情報のユーザ入力が行われる。図３に示す例では、第１ドロップ領域３１０には、パスワード方式であることを示すアスタリスクからなるイメージパターン３１１が表示さ

れ、第２ドロップ領域３２０には、パターン方式であることを示す３×３の９個の点からなるイメージパターン３２１が表示されている。イメージパターン３１１、３２１の表示があると、ユーザが認証情報入力方式を直感的に判断できる点で好ましい。なお、イメージパターン３１１、３２１は一例であり、ユーザが認証情報入力方式を直感的に判断できるイメージパターンであるならば、図３に示すイメージパターン以外のイメージパターンであってもよい。また、処理ウインドウ形成部１３２は、ドロップ領域３１０、３２０に、イメージパターン３１１、３２１を表示しなくてもよい。ステータスバー３３０には、格納フォルダ１５０へのパス３４０が表示される。なお、格納フォルダ１５０の場所が記憶部１２０のいずれかに固定の場合には、パス３４０の表示が無くてもよく、さらには、ステータスバー３３０は無くてもよい。

【００２８】

図２のステップＳ１３０では、ユーザは、暗号化あるいは復号したいファイルやフォルダ、具体的にはファイルやフォルダに対応するアイコンを、第１ドロップ領域３１０または第２ドロップ領域３２０にドラック＆ドロップする。ステップＳ１４０では、ファイル判定部１３６は、ドロップされたファイルが暗号処理プログラムにより暗号化された暗号化ファイルか否かを判定する。上述したように、ファイル判定部１３６は、ファイルの拡張子によってこの判定を行う。ドロップされたファイルが暗号処理プログラムにより暗号化された暗号化ファイルでない場合、例えば平文のファイルの場合には、ステップＳ１５０に移行し、暗号処理プログラム１３０により暗号化された暗号化ファイルの場合には、ステップＳ２２０に移行する。

【００２９】

ステップＳ１５０は、ステップＳ１５５からＳ２１０までのステップが含まれ、ファイルを暗号化する処理が行われる。ステップＳ１５５では、認証情報入力部１３４は、ファイルがドロップされた領域が第１ドロップ領域３１０（図３）か否かを判定する。認証情報入力部１３４は、ファイルがドロップされた領域が第１ドロップ領域３１０であると判定した場合には、ステップＳ１６０に移行し、ファイルがドロップされた領域が第１ドロップ領域３１０でないと判定した場合には、ステップＳ１７０に移行する。

【００３０】

図４は、暗号化されていないファイルの第１ドロップ領域３１０へのドラッグ＆ドロップの一例を示す説明図である。ここでは、一例として、ユーザがドキュメントフォルダのｉｍａｇｅｓフォルダのｐｉｃ０２．ｊｐｇのアイコンを第１ドロップ領域３１０にドロップする例を示している。ステップＳ１６０では、認証情報入力部１３４（図１）は、第１ドロップ領域３１０に対応する認証情報入力ウインドウ（第１認証情報入力ウインドウ）を電子機器２００の表示部２４０に表示し、ユーザから認証情報のユーザ入力を受け付ける。

【００３１】

図５は、ステップＳ１６０で表示される第１認証情報入力方式の入力画面の一例である。図５では、図３で示すウインドウ３００、４００、５００に加えて、第１認証情報入力ウインドウ６００が表示されている。第１認証情報入力ウインドウ６００には、識別情報入力部６１０と、完了ボタン６２０と、クリアボタン６３０とが表示される。ユーザは、例えば電子機器２００の入力部２３０（図１）から識別情報入力部６１０に識別情報を入力する。ユーザは、識別情報の入力後、完了ボタン６２０を押す（例えばマウスでクリックする）ことで、識別情報のユーザ入力（単に「ユーザ入力」とも呼ぶ。）を確定し、完了する。クリアボタン６３０は、完了ボタン６２０を押して識別情報のユーザ入力を確定する前に、識別情報入力部６１０に入力された入力内容をクリアするためのボタンである。この場合、ユーザは、識別情報入力部６１０へのユーザ入力をやり直す。なお、入力部２３０としてキーボードを有する場合には、キーボードのＤｅｌキーやＢＳキーにより文字単位で識別情報のユーザ入力を修正することも可能である。

【００３２】

図２のステップＳ１７０では、認証情報入力部１３４は、ファイルがドロップされた領

域が第２ドロップ領域３２０（図３）か否かを判定する。ファイルがドロップされた領域が第２ドロップ領域３２０であると判定した場合には、ステップＳ１８０に移行し、ファイルがドロップされた領域が第２ドロップ領域３２０でないと判定した場合には、処理を終了する。ファイルが第１ドロップ領域３１０、第２ドロップ領域３２０のいずれにもドロップされていない例としては、例えば、ステータスバー３３０にファイルがドラッグ＆ドロップされる場合がある。ステップＳ１８０では、認証情報入力部１３４（図１）は、第２ドロップ領域３２０に対応する認証情報入力ウインドウ（第２認証情報入力ウインドウ）を電子機器２００の表示部２４０に表示し、ユーザから認証情報のユーザ入力を受け付ける。

【００３３】

図６は、ステップＳ１８０で表示される第２認証情報入力方式の入力画面の一例である。図６は、図４で、ファイルが第１ドロップ領域３１０ではなく、第２ドロップ領域３２０にドロップされたときに表示部２４０（図１）に表示される画面である。図６では、図３で示すウインドウ３００、４００、５００に加えて、第２認証情報入力ウインドウ７００が表示されている。第２認証情報入力ウインドウ７００には、識別情報入力部７１０と、完了ボタン７２０と、クリアボタン７３０とが表示される。本実施形態では、識別情報入力部７１０は、縦横３×３の９個の点を有しており、この９個の点がどのように選択されたか、により識別情報のユーザ入力が行われる。図６に示す例では、（右上）→（右中）→（右下）→（中下）→（左中）の順で連続的に点が選択されている。

【００３４】

図２のステップＳ１９０では、秘密鍵生成部１３８は、認証情報のユーザ入力から秘密鍵を生成する。ステップＳ２００では、暗号化処理部１４０は、ドロップされたファイルに対して秘密鍵を用いて暗号化処理を行うとともに、どの認証情報入力方式を用いたかを示す識別子を暗号化後の暗号化ファイルに付与する。なお、暗号化処理部１４０は、秘密鍵のハッシュ値を暗号化ファイルに付与することが好ましい。秘密鍵のハッシュ値は、秘密鍵から予め定められた計算式によって算出される値であり、秘密鍵のビット数よりも小さいビット数を有する。同じ秘密鍵からは同じハッシュ値が得られるが、秘密鍵が少しでも異なれば、ハッシュ値は異なる。ハッシュ値の計算は情報量の欠損を含む不可逆的計算なので、ハッシュ値から元の秘密鍵を算出することは不可能である。

【００３５】

ステップＳ２１０では、暗号化ファイルを外部記憶装置１００の格納フォルダ１５０に格納する。暗号化ファイルの格納フォルダ１５０への格納は、暗号化処理部１４０が実行する。なお、暗号化処理部１４０は、格納フォルダ１５０にすでに同一のファイル名を有するファイルが存在する場合には、別名で保存する。

【００３６】

図７は、暗号化処理後の表示部に表示される画面の一例である。図３と図７を比較すると、図７では、格納フォルダ１５０であるＳｅｃｕｒｅＬｏｃｋＭｏｂｉｌｅ２というフォルダにｐｉｃ０２．ｊｐｇ．ｂｕｆｅｎｃという暗号化ファイルが形成されていることがわかる。暗号化ファイルは、暗号化される前の元のファイル名「ｐｉｃ０２．ｊｐｇ」の語尾に、「．ｂｕｆｅｎｃ」という文字列が拡張子として新たに付与されている。ファイル判定部１３６は、この拡張子「．ｂｕｆｅｎｃ」の有無により、そのファイルが、暗号処理プログラム１３０により暗号化された暗号化ファイルか否かを判定できる。また、ファイル名の前段に元のファイル名を含んでいるので、ユーザは、ファイル名から元のファイルがどのようなファイルであったかを、認識し易い。なお、「．ｂｕｆｅｎｃ」という拡張子の文字列は一例であり、他の文字列であってもよい。暗号化処理部１４０は、格納フォルダ１５０にすでに同一のファイル名を有するファイルが存在する場合には、別名で保存する。

【００３７】

図８は、暗号化ファイルのドラッグ＆ドロップの一例を示す説明図である。ここでは、格納フォルダ１５０（図１）であるＳｅｃｕｒｅＬｏｃｋＭｏｂｉｌｅ２に格納されてい

るｓｔｕｖ．ｄｏｃ．ｂｕｆｅｎｃという名前の暗号化ファイルのアイコンが、第１ドロップ領域３１０にドラッグ＆ドロップされる場合を例にとって説明する。

【００３８】

図２のステップＳ１４０では、ファイル判定部１３６は、第１ドロップ領域３１０にドロップされたファイルが暗号処理プログラム１３０により暗号化されたファイルか否かを、ドロップされたファイルの拡張子により判定する。図８に示す例では、ドロップされたファイルに「．ｂｕｆｅｎｃ」という拡張子があるため、ファイル判定部１３６は、暗号処理プログラム１３０により暗号化された暗号化ファイルと判定し、処理をステップＳ２２０に移行する。

【００３９】

ステップＳ２２０は、ステップＳ２２５からＳ２８０までのステップが含まれ、ファイルを復号する処理が行われる。ステップＳ２２５では、認証情報入力部１３４は、暗号化ファイルについて、どの認証情報入力方式で暗号化のための認証情報が入力されたかを特定する。ステップＳ２００で説明したように、暗号化ファイルには、どの認証情報入力方式を用いたかを示す識別子が付与されている。したがって、認証情報入力部１３４は、この識別子を用いてどの認証情報入力方式で暗号化のための認証情報が入力されたかを特定できる。なお、認証情報入力部１３４は、認証情報入力方式を用いたかを示す識別子で、認証情報入力方式を特定できるため、認証情報入力部１３４は、ファイルが第１ドロップ領域３１０、第２ドロップ領域３２０のいずれにドロップされたかを判定しなくてもよい。また、ファイルがステータスバー３３０にドロップされた場合でも、認証情報入力部１３４は、この識別子を用いてどの認証情報入力方式で暗号化のための認証情報が入力されたかを特定できる。

【００４０】

ステップＳ２３０では、認証情報入力部１３４は、特定された認証情報入力方式による認証情報入力ウインドウ（図５の第１認証情報入力ウインドウ６００または図６の第２認証情報入力ウインドウ７００）を表示部２４０（図１）に表示し、ユーザに認証情報のユーザ入力を行わせる。ステップＳ２４０では、秘密鍵生成部１３８は、ユーザ入力に基づいて秘密鍵を生成する。ステップＳ２５０では、復号処理部１４２は、生成された秘密鍵が正しいか否かを判定する。秘密鍵が正しいとは、暗号化ファイルがその秘密鍵で復号できることを意味する。生成された秘密鍵が正しいか否かは、暗号化ファイルに格納されている秘密鍵のハッシュ値と、ステップＳ２４０で生成された秘密鍵のハッシュ値とが一致するか否かにより判定できる。復号処理部１４２は、ハッシュ値が一致すれば、その暗号化ファイルを復号できる正しい秘密鍵であると判断する。生成された秘密鍵が正しい場合にはステップＳ２６０に移行し、復号処理部１４２は、暗号化ファイルに対して復号処理を行う。ステップＳ２７０では、復号されたファイルは、外部記憶装置１００の格納フォルダ１５０に格納される。復号されたファイルの格納は、復号処理部１４２が実行する。復号処理部１４２は、復号されたファイルを格納するフォルダにすでに同一のファイル名を有するファイルが存在する場合には、別名で保存する。ステップＳ２５０で秘密鍵が正しくなかった場合には、復号処理部１４２は、ステップＳ２８０に移行し、電子機器２００の表示部２４０に、例えば、ユーザ入力が正しくなく、復号できない旨のエラー表示を行う。

【００４１】

図９は、復号処理後の表示部に表示される画面の一例である。図８と図９とを比較すると、図９では、格納フォルダ１５０に、平文ファイルであるｓｔｕｖ．ｄｏｃが生成される。この平文ファイルのファイル名「ｓｔｕｖ．ｄｏｃ」は、暗号化ファイルである「ｓｔｕｖ．ｄｏｃ．ｂｕｆｅｎｃ」から、暗号処理プログラム１３０により暗号化ファイルであることを示す「．ｂｕｆｅｎｃ」という拡張子が削除されたファイル名である。

【００４２】

以上、第１の実施形態によれば、暗号処理プログラム１３０は、電子機器２００の表示部２４０に、暗号化を行いたいファイルをドロップするための複数のドロップ領域（第１

ドロップ領域３１０と第２ドロップ領域３２０）を含む処理ウインドウ３００を表示させる。その後、複数のドロップ領域３１０、３２０のいずれかに暗号化を行いたいファイルがドロップされたときに、ドロップ領域ごとに予め定められた認証情報入力方法による認証情報のユーザ入力を行うための入力ウインドウを表示部２４０に表示させ、認証情報のユーザ入力を受け付ける。そのため、ユーザがどちらのドロップ領域にファイルをドロップするかにより認証情報入力方法を選択できるので、ファイルの暗号化における利便性を向上させることができる。また、ユーザは、ユーザ入力したワードやパターンを憶えればよく、秘密鍵の生成や秘密鍵の管理を意識しなくてもよく、この点でもファイルを暗号化する処理における利便性を向上させることができる。

【００４３】

本実施形態では、暗号化された暗号化ファイルを外部記憶装置１００に格納している。これは、暗号化ファイルが格納された外部記憶装置１００を移動先に持ち出し、移動先で復号することを想定している。すなわち、暗号化されたファイルは、必ず復号する時が来る。その時、暗号処理プログラム１３０と暗号化ファイルとが同じ外部記憶装置１００に格納されていると、外部記憶装置１００を移動先の電子機器に接続して復号することができる。

【００４４】

第１の実施形態によれば、暗号処理プログラム１３０は、さらに、処理ウインドウ３００内に、暗号処理プログラム１３０によって暗号化された暗号化ファイルがドロップされたとき、暗号化ファイルがドロップされた位置が、暗号化ファイルが作成されたときの暗号化前のファイルがドロップされたドロップ領域（第１ドロップ領域３１０または第２ドロップ領域３２０）に該当するか否かに関わらず、暗号化ファイルに格納されている識別子に基づいて認証情報入力方法を特定し、特定された認証情報入力方法に従った認証情報のユーザ入力を受け付ける処理と、ユーザ入力から秘密鍵を生成する処理と、秘密鍵を用いて前記暗号化ファイルを復号する処理と、を前記電子機器に実行させるので、暗号化されたファイルを復号する処理における利便性を向上させることができる。

【００４５】

第１の実施形態では、暗号処理プログラム１３０は暗号化処理部１４０と、復号処理部１４２とを備えているため、暗号化処理と復号処理の両方を実行できる。ここで、暗号処理プログラム１３０は、暗号化処理部１４０のみ、あるいは、復号処理部１４２のみを有する構成であってもよい。この場合、暗号処理プログラム１３０は、暗号化処理のみ、あるいは、復号処理のみ、を実行できる。

【００４６】

・第２の実施形態：

図１０は、第２の実施形態の外部記憶装置１０２と、電子機器２００を示す説明図である。第２の実施形態の外部記憶装置１０２は、第１の実施形態の外部記憶装置１００と比較すると、機器識別子１８０が設けられており、暗号処理プログラム１３０は、さらに機器識別部１４４を備えている点が異なる。機器識別子１８０は、外部記憶装置１０２を識別するための識別標識である。機器識別子としては、例えば、ＶＩＤ（ベンダーＩＤ）、ベンダー名のいずれかを含むことが好ましい。ベンダーＩＤとは、外部記憶装置１０２を製造した企業または会社毎に、特定の組織から付与されるコードである。外部記憶装置１０２がＵＳＢ機器の場合には、ＶＩＤは、ＵＳＢインプリメンターズ・フォーラムから発行される。ベンダー名は、外部記憶装置１０２を製造した企業または会社の名前である。なお、例示したＶＩＤ（ベンダーＩＤ）、ベンダー名は、機器識別子の一例であり、機器識別子は、機器を識別できるコードであれば、ＶＩＤ（ベンダーＩＤ）、ベンダー名に限定されない。機器識別部１４４は、外部記憶装置１０２から機器識別子１８０を取得し、機器識別子１８０が正規なものか否かを判定する。

【００４７】

図１１は、第２の実施形態における動作フローチャートである。図２に示す第１の実施形態における動作フローチャートと比較すると、さらに、ステップＳ１１２、Ｓ１１４、

Ｓ１１８を備える点が異なっているが、他のステップは同じである。図１１では、図２のステップＳ１２０からＳ１４０と、ステップＳ１５０（暗号化）と、ステップＳ２２０（復号）については、ステップＳ１１６として図示して記載を簡略化している。以下、図２に示す動作フローチャートと異なる点について説明する。

【００４８】

ステップＳ１１２では、機器識別部１４４は、外部記憶装置１０２の機器識別子１８０を取得する。ステップＳ１１４では、機器識別部１４４は、機器識別子１８０が予め定められた機器識別子のリストと合致するか否かを判定する。合致する場合には、機器識別子１８０及び外部記憶装置１０２は正規なものであり、暗号処理プログラム１３０は、ステップＳ１１６に移行して、図２のステップＳ１２０～Ｓ１４０のステップを実行し、ステップＳ１４０の判定結果により、暗号化（ステップＳ１５０）または復号（ステップＳ２２０）を実行する。すなわち、このステップＳ１２０以降の動作は、第１の実施形態の動作と同じである。一方、ステップＳ１１４において機器識別子が合致しない場合には、機器識別子１８０及び外部記憶装置１０２は正規なものでないので、暗号処理プログラム１３０は、ステップＳ１１８に移行し、処理ウインドウ３００（図３）を表示せずにプログラムを終了する。

【００４９】

第２の実施形態によれば、暗号処理プログラム１３０が不正にコピーされても、正規な外部記憶装置１０２が接続されたときでなければ機器識別子１８０が合致しないため、暗号処理プログラムが終了し、暗号化処理や復号処理が実行できない。すなわち、不正なコピーを作成する意味が無くなり、不正なコピーの拡散を抑制することが可能となる。

【００５０】

また、本実施形態では、暗号処理プログラム１３０が起動できなければ、ユーザ入力からの秘密鍵を生成できない。ここで、暗号化ファイルを例えば電子メール等で送られた場合、暗号化ファイルを受け取ったユーザが復号する時に正規な外部記憶装置１０２が電子機器２００に接続されていないと、暗号処理プログラム１３０が起動できず、ユーザ入力からの秘密鍵を生成することができない。この場合、暗号化ファイルを平文ファイルに復号するためには、秘密鍵を解読する必要がある。しかし、一般に、秘密鍵を解読するには膨大な時間がかかる。本実施形態では、機器識別子１８０の合致を判断することで、ファイルを復号する処理における処理環境を制限している。そのため、機器識別子１８０が合致する場合には、ユーザは、ユーザ入力を行うことで暗号化ファイルを容易に復号できるが、機器識別子１８０が合致しない場合には、暗号処理プログラム１３０が起動しないため、ユーザは、ユーザ入力を行うことができず、暗号化ファイルを容易に復号できない。その結果、セキュリティを高めることができる。すなわち、ユーザの利便性の向上とセキュリティの向上とを両立できる。

【００５１】

・第３の実施形態：

図１２は、第３の実施形態における動作フローチャートである。第１、第２の実施形態では、１個のファイルをドロップ領域にドラッグ＆ドロップする例について説明した第３の実施形態では、２以上のファイルが選択され、ドロップ領域にドラッグ＆ドロップする例について説明する。なお、第３の実施形態における外部記憶装置の構成は、第１の実施形態における外部記憶装置１００の構成と同じである。但し、第３の実施形態における外部記憶装置の構成を、第２の実施形態における外部記憶装置１０２の構成と同じとしてもよい。

【００５２】

第３の実施形態では、まず、図２で説明したステップＳ１００からＳ１３０の処理が実行される。ここで、外部記憶装置の構成が第２の実施形態における外部記憶装置１０２の構成と同じ場合には、図１１で説明したように、ステップＳ１１２、Ｓ１１４、Ｓ１１８が実行される。

【００５３】

ステップＳ３００では、ドロップ領域にドラッグ＆ドロップされたファイルの数が２以上であるか否かを判断する。ドロップされたファイルの数が２以上の場合には、暗号処理プログラム１３０は、ステップＳ３１０に移行する。ドロップされたファイルの数が２以上でない場合、すなわち１つの場合には、暗号処理プログラム１３０は、ステップＳ３０５に移行して、図２に示すステップＳ１４０及び、その結果に応じて暗号化（ステップＳ１５０）または復号（ステップＳ２２０）を実行する。この場合の処理は、第１の実施形態と同じである。ステップＳ３１０では、暗号処理プログラム１３０は、ファイルの処理順をＯＳ２２５より取得する。ファイルの処理順は、ＯＳが異なれば異なる可能性があるが、一例として、最初のファイルは、ドラッグ開始時にカーソルが指し示しているファイルであり、２番目以降は、ファイルのアルファベット順である。

【００５４】

ステップＳ３２０では、暗号処理プログラム１３０は、最初のファイルについて、図２に示すステップＳ１４０及び、その結果に応じて暗号化（ステップＳ１５０）または復号（ステップＳ２２０）を実行する。ステップＳ３３０以降は、２番目以降のファイルが順に処理対象に選択されて処理される。ステップＳ３３０では、ファイル判定部１３６は、処理対象のファイルの拡張子から、処理対象のファイルが暗号化ファイルか否かを判定する。処理対象のファイルが暗号化ファイルでない場合には、ステップＳ３４０に移行し、処理対象のファイルが暗号化ファイルの場合には、ステップＳ３６０に移行する。

【００５５】

ステップＳ３４０では、ステップＳ３２０における最初のファイルに対する処理がファイルを暗号化する処理であったか否かを判定する。この判定は、最初のファイルに対する処理がファイルを暗号化する処理の場合にはフラグを立て、暗号化する処理でない場合、すなわちファイルを復号する処理の場合にはフラグを下げることで、フラグが立っているか、あるいは、下がっているかにより、容易に判定できる。この判定は、２番目以降のファイルの暗号化を行う暗号化処理部１４０または、復号を行う復号処理部１４２のいずれか一方が行ってもよい。ステップＳ３４０で最初の処理がファイルを暗号化する処理であった場合には、ステップＳ３５０に移行する。

【００５６】

ステップＳ３５０では、暗号化処理部１４０は、最初のファイルを暗号化する処理で用いた秘密鍵で処理対象のファイルを暗号化し、格納フォルダ１５０（図１）に格納する。一方、ステップＳ３４０で、最初の処理がファイルを暗号化する処理でない場合（ファイルを復号する処理）の場合、ステップＳ３９５に移行する。この場合、対象のファイルに対しては、ファイルを暗号化する処理も、復号する処理もされない。ステップＳ３９５では、全てのファイルの処理が完了したか否かを判定する。この判定は、例えば、暗号化処理部１４０または、復号を行う復号処理部１４２のいずれか一方が行ってもよい。全てのファイルの処理が完了していない場合には、ステップＳ３３０に戻る。全てのファイルの処理が完了している場合には、処理を終了する。

【００５７】

ステップＳ３３０で、処理対象のファイルが暗号化ファイルの場合、ステップＳ３６０に移行する。ステップＳ３６０では、ステップＳ３２０における最初のファイルに対する処理がファイルを復号する処理であったか否かを判定する。ステップＳ３４０とは逆に、フラグが下がっている場合には、最初のファイルの処理がファイルを復号する処理であることが容易に判定できる。最初のファイルの処理がファイルを復号する処理であった場合には、ステップＳ３７０に移行し、最初のファイルの処理がファイル復号する処理でなかった場合、すなわちファイルを暗号化する処理の場合には、ファイルを暗号化する処理も、復号する処理もせずに、ステップＳ３９５に移行する。

【００５８】

ステップＳ３７０における処理対象のファイルは、ステップＳ３３０の判定により暗号化ファイルである。ステップＳ３７０では、認証情報入力部１３４は、暗号化ファイルに格納されている、どの認証情報入力方式を用いたかを示す識別子から、処理対象の暗号化

ファイルがどの認証情報入力方式で認証情報のユーザ入力がされたかを取得する。そして、処理対象の暗号化ファイルの識別子から得られる認証情報入力方式と、ステップＳ３２０で行われた認証情報入力方式とを比較し、一致すれば、ステップＳ３８０に移行し、一致しなければ、ファイルを暗号化する処理も、復号する処理もせずに、ステップＳ３９５に移行する。認証情報入力方式が不一致であれば、ステップＳ３２０で用いられた秘密鍵で復号できないので、ステップＳ３８０に移行する必要はないからである。

【００５９】

ステップＳ３８０では、復号処理部１４２は、ステップＳ３２０で用いられた秘密鍵のハッシュ値と、処理対象の暗号化ファイルに格納されているハッシュ値とを比較して、秘密鍵は一致するか否かを判定する。秘密鍵が一致する場合には、ステップＳ３９０に移行し、秘密鍵が一致しない場合には、ファイルを暗号化する処理も、復号する処理もせずに、ステップＳ３９５に移行する。

【００６０】

ステップＳ３９０では、復号処理部１４２は、ステップＳ３２０で用いられた秘密鍵を用いて暗号化ファイルを復号し、図２のステップＳ２７０と同様に、格納フォルダ１５０に格納する。

【００６１】

なお、最初のファイルに対する処理が復号処理であるが、秘密鍵が異なるため、最初のファイルの復号がエラーとなった場合、暗号処理プログラム１３０は、最初のファイルの復号で用いられた認証情報入力方式及び秘密鍵を有効として２番目以降のファイルを処理してもよい。この場合、２番目以降の暗号化ファイルについては、ステップＳ３７０、３８０では、対象の暗号化ファイルの認証情報入力方式及び秘密鍵が、最初のファイルに対する処理で用いられた認証情報入力方式及び秘密鍵と比較される。但し、暗号処理プログラム１３０は、最初のファイルの復号がエラーとなった場合、それ以降の処理を終了するように構成されていてもよい。

【００６２】

図１３は、第３の実施形態における複数のファイルの第１ドロップ領域へのドラッグ＆ドロップの一例を示す説明図である。図１３に示す例では、ｉｊｋｌ．ｐｄｆとｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃという２つのファイルが選択され、第１ドロップ領域３１０にドラッグされ、ドロップされている。このとき、カーソル２４２は、ｉｊｋｌ．ｐｄｆを指し示した状態でドラッグを始め、第１ドロップ領域３１０にドラッグされている。この場合、最初に処理されるファイルは、カーソル２４２により指し示されたｉｊｋｌ．ｐｄｆである。図１２のステップＳ３２０では、最初のファイルのｉｊｋｌ．ｐｄｆの暗号化処理が行われる。

【００６３】

２番目のファイルは、ｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃである。このファイルは、拡張子から暗号化ファイルであるので、図１２のステップＳ３３０では、「Ｙ」の判定であり、ステップＳ３６０に移行する。最初の処理が暗号化処理なので、ステップＳ３６０の判定は「Ｎ」であり、ｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃは何も処理がされずにステップＳ３９５に移行する。図１３に示す例では、３番目以降のファイルが存在しないため、暗号処理プログラム１３０は、処理を終了する。

【００６４】

図１４は、第３の実施形態の暗号化または復号の処理後における表示部に表示される画面の一例である。図１３と図１４とを比較すれば分かるように、ウインドウ５００のフォルダＳｅｃｕｒｅＬｏｃｋＭｏｂｉｌｅ２に暗号化されたｉｊｋｌ．ｐｄｆ．ｂｕｆｅｎｃという暗号化ファイルが生成されている。

【００６５】

図１５は、第３の実施形態における複数のファイルの第１ドロップ領域へのドラッグ＆ドロップの一例を示す説明図である。図１５に示す例では、ｉｊｋｌ．ｐｄｆとｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃと、ｑｒｓｔ．ｄｏｃ．ｂｕｆｅｎｃいう３つのファイルが選択

され、第１ドロップ領域３１０にドラッグされ、ドロップされている。このとき、カーソル２４２は、ｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃを指し示した状態でドラッグを始め、第１ドロップ領域３１０にドラッグされている。この場合、最初に処理されるファイルは、カーソル２４２により指し示されたｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃである。図１２のステップＳ３２０では、最初のファイルのｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃの復号処理が行われる。

【００６６】

２番目のファイルは、ｉｊｋｌ．ｐｄｆである。２番目のファイルは、拡張子から暗号化ファイルでないので、図１２のステップＳ３３０では、「Ｎ」の判定であり、ステップＳ３４０に移行する。最初の処理が復号処理なので、ステップＳ３４０の判定は「Ｎ」であり、ｉｊｋｌ．ｐｄｆは何も処理がされずにステップＳ３９５に移行する。図１３に示す例では、３番目のファイルｑｒｓｔ．ｄｏｃ．ｂｕｆｅｎｃが存在するため、暗号処理プログラム１３０は、処理を、ステップＳ３３０に移行する。

【００６７】

３番目のファイルは、ｑｒｓｔ．ｄｏｃ．ｂｕｆｅｎｃである。このファイルは、拡張子から暗号化ファイルであるので、図１２のステップＳ３３０では、「Ｙ」の判定であり、ステップＳ３６０に移行する。最初の処理が復号処理なので、ステップＳ３６０の判定は「Ｙ」であり、ステップＳ３７０に移行する。ステップＳ３７０では、認証情報入力部１３４は、ｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃに格納されている認証情報入力方式を示す識別子から、処理対象の暗号化ファイルがどの認証情報入力方式で認証情報のユーザ入力がされたかを取得する。そして、最初の処理を行ったときのｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃの認証情報入力方式と、今回の処理対象であるｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃの認証情報入力方式とを比較し、一致すれば、ステップＳ３８０に移行し、一致しなければ、ステップＳ３９５に移行する。ここで、ｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃの認証情報入力方式と、ｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃの認証情報入力方式とが一致するとする。この場合、暗号処理プログラム１３０は、処理をステップＳ３８０に移行する。

【００６８】

ステップＳ３８０では、復号処理部１４２は、最初のファイルｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃに格納されている秘密鍵のハッシュ値と、今回の処理対象であるファイルｑｒｓｔ．ｄｏｃ．ｂｕｆｅｎｃに格納されている秘密鍵のハッシュ値とを比較して、秘密鍵は一致するか否かを判定する。秘密鍵が一致する場合には、ステップＳ３９０に移行し、秘密鍵が一致しない場合には、ステップＳ３９５に移行する。ここでは、ｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃに格納されている秘密鍵のハッシュ値と、ｑｒｓｔ．ｄｏｃ．ｂｕｆｅｎｃに格納されている秘密鍵のハッシュ値とが一致し、秘密鍵が一致するとする。この場合、暗号処理プログラム１３０は、処理をステップＳ３９０に移行する。ステップＳ３９０では、復号処理部１４２は、最初のファイルｍｎｏｐ．ｐｄｆ．ｂｕｆｅｎｃの復号処理で用いられた秘密鍵を用いて今回の処理対象であるファイルｑｒｓｔ．ｄｏｃ．ｂｕｆｅｎｃを復号し、図２のステップＳ２７０と同様に、格納フォルダ１５０に格納する。

【００６９】

図１６は、第３の実施形態の暗号化または復号の処理後における表示部に表示される画面の一例である。図１５と図１６とを比較すれば分かるように、格納フォルダ１５０に復号されたｍｎｏｐ．ｐｄｆとｑｒｓｔ．ｄｏｃの２つのファイルが新たに生成されている。なお、２番目のファイルであるｉｊｋｌ．ｐｄｆについては、暗号化されないので、ｉｊｋｌ．ｐｄｆ．ｂｕｆｅｎｃという名前のファイルは生成されていない。

【００７０】

図１７は、第３の実施形態におけるフォルダの第１ドロップ領域へのドラッグ＆ドロップの一例を示す説明図である。暗号処理プログラム１３０では、ファイルそのものではなく、ファイルを含むフォルダが、ドロップ領域（第１ドロップ領域３１０または第２ドロップ領域３２０）にドラッグ＆ドロップされたときでも、暗号化または復号を行うことができる。暗号処理プログラム１３０は、図１２のステップＳ３１０で、ＯＳ２２５からフ

ファイルの処理順を取得する。この場合、ドラッグ開始時にカーソルが指し示しているのはフォルダであり、ファイルではないので、ファイルの処理順は、ファイルのアルファベット順である。

【００７１】

図１７に示す例では、ｉｍａｇｅｓというフォルダが選択され、第１ドロップ領域にドラッグ＆ドロップされている。ｉｍａｇｅｓというフォルダには２つのファイルｐｉｃ０１．ｊｐｇとｐｉｃ０２．ｊｐｇの２つのファイルが含まれており、最初のファイルはｐｉｃ０１．ｊｐｇであり、２番目のファイルはｐｉｃ０２．ｊｐｇである。

【００７２】

図１２のステップ３２０では、最初のファイルｐｉｃ０１．ｊｐｇについて、図２のステップＳ１４０の判断と、その結果に応じて暗号化処理（ステップＳ１５０）または復号処理（ステップＳ２２０）が行われる。具体的は、最初のファイルｐｉｃ０１．ｊｐｇは、ステップＳ１４０において、拡張子から暗号化されていないファイルと判断されるので、暗号化処理（図２のステップＳ１５０）が行われ、格納フォルダ１５０（図１）に格納される。ステップＳ３３０では、２番目のファイルｐｉｃ０２．ｊｐｇは、拡張子から暗号化ファイルではない、と判定されるので、処理はステップＳ３４０に移行する。最初のファイルｐｉｃ０１．ｊｐｇに対する処理は暗号化処理なので、ステップＳ３４０の判定は「Ｙ」であり、ステップＳ３５０に移行する。ステップＳ３５０では、暗号化処理部１４０は、最初のファイルｐｉｃ０１．ｊｐｇについて、暗号化処理を行ったときと同じ秘密鍵を用いて、暗号化処理を行い、暗号化後の暗号化ファイルを格納フォルダ１５０に格納する。

【００７３】

図１８は、フォルダをドロップしたときの暗号化または復号の処理後における表示部に表示される画面の一例である。図１７と図１８とを比較すれば分かるように、ウインドウ５００の格納フォルダ１５０であるフォルダＳｅｃｕｒｅＬｏｃｋＭｏｂｉｌｅ２に、ｉｍａｇｅｓという子フォルダが形成され、ｉｍａｇｅｓという子フォルダに暗号化されたｐｉｃ０１．ｊｐｇ．ｂｕｆｅｎｃとｐｉｃ０２．ｊｐｇ．ｂｕｆｅｎｃという暗号化ファイルが生成されている。このように、フォルダがドラッグ＆ドロップされたときには、格納フォルダ１５０にドラッグ＆ドロップされたフォルダが形成され、格納フォルダ１５０からその形成されたフォルダを含めて相対パスで指定される場所に処理後のファイルが格納される。こうすれば、格納フォルダ１５０に暗号化処理を行う前のフォルダ構成を構成できるため、ユーザが暗号化後のファイルを見失ったり、同一のファイル名の暗号化ファイルが生成されたりすることを抑制できる。

【００７４】

以上、第３の実施形態によれば、複数のドロップ領域の１つに複数のファイルがドロップされたとき、暗号処理プログラム１３０は、以下のように処理するので、複数のファイルの暗号化、復号における利便性を向上させることができる。

（ａ－ｉ）最初のファイルが暗号処理プログラム１３０によって暗号化されていないファイルの場合には、最初のファイルを暗号化する。

（ａ－ｉｉ）２番目以降のファイルについては、

・当該ファイルが暗号処理プログラム１３０によって暗号化されていないファイルの場合には、（ａ－ｉ）の処理で用いたのと同一の秘密鍵を用いて当該ファイルを暗号化する。

・当該ファイルが暗号処理プログラム１３０によって暗号化された暗号化ファイルの場合には、暗号化も復号も実行しない

（ｂ－ｉ）最初のファイルが、暗号処理プログラム１３０によって暗号化された暗号化ファイルの場合には、最初のファイルを復号する。

（ｂ－ｉｉ）２番目以降のファイルについては、

・当該ファイルが暗号処理プログラムによって暗号化された暗号化ファイルの場合には、（ｂ－ｉ）の処理で用いたのと同一の秘密鍵を用いて当該ファイルを復号する。

・当該ファイルが暗号処理プログラム１３０によって暗号化されたファイルでない場合には、当該ファイルを暗号化も復号もしない。

【００７５】

・第４の実施形態：

図１９は、第４の実施形態における暗号処理プログラムを起動したときの表示部に表示される画面の一例である。第４の実施形態における処理ウインドウ３００の第１ドロップ領域３１０は、肉眼により識別可能な複数の小領域（小ドロップ領域３１０ｓ、３１０ｍ、３１０ｗ）を有し、第２ドロップ領域３２０は、肉眼により識別可能な複数の小領域（小ドロップ領域３２０ｓ、３２０ｍ、３２０ｗ）を有している。小ドロップ領域３１０ｓ、３１０ｍ、３１０ｗは、例えばグラデーションにより色分けされていてもよい。

【００７６】

第４の実施形態では、ファイルがどの小ブロック領域にドラッグ＆ドロップされるかにより、暗号化処理における暗号強度が異なる。具体的には、小ドロップ領域３１０ｍにファイルがドロップされたときを基準とすれば、小ドロップ領域３１０ｓファイルがドロップされたときは、暗号強度が強く、小ドロップ領域３１０ｗファイルがドロップされたときは、暗号強度が弱い。ここで、暗号強度をアルゴリズムで変えようとすると複数の暗号化処理部１４０、復号処理部１４２が必要となるので、暗号強度は、秘密鍵の鍵長により変えることが好ましい。例えば、暗号強度が最も強い小ドロップ領域３２０ｓにファイルがドロップされたときの鍵長を２５６ビット、暗号強度が中間の小ドロップ領域３２０ｍにファイルがドロップされたときの鍵長を１９２ビット、暗号強度が弱い小ドロップ領域３２０ｓにファイルがドロップされたときの鍵長を１２８ビットとしてもよい。鍵長が長いと、秘密鍵を解読されにくい。一方、鍵長が短いとファイルを暗号化する処理、復号する処理に時間がかからない、という利点がある。なお,鍵長は一例であり、鍵長を５１２ビット、３８４ビット、２５６ビットとしてもよい。

【００７７】

本実施形態における動作フローチャートは、図２に示すものと同じである。ただし、処理内容において、以下の点が異なる。ステップＳ１９０では、各ドロップ領域（第１ドロップ領域３１０、第２ドロップ領域３２０）のどの小ドロップ領域にファイルがドロップされたかにより、生成される秘密鍵の鍵長が異なる。また、ステップ２００の暗号化処理においては、鍵長が暗号化後の暗号化ファイルに書き込まれる。鍵長の代わりに鍵長を示す符号であってもよい。また、ステップＳ２５０の秘密鍵（秘密鍵）の生成では、秘密鍵生成部１３８は、暗号化ファイルから、鍵長を取得し、認証情報のユーザ入力からその鍵長に応じた秘密鍵を生成する。したがって、ユーザは、復号時に、鍵長を意識する必要は無い。

【００７８】

一般に暗号強度を強くすれば、暗号化や復号の処理時間がかかる。第４の実施形態によれば、処理時間はかかるが暗号強度を強くするか、暗号強度は弱いが処理時間を短くするか、ユーザが選択あるいは決めることができ、ファイルの暗号化における利便性及びセキュリティを向上させることができる。

【００７９】

・第５の実施形態：

図２０は第５の実施形態における暗号処理プログラムを起動したときの表示部に表示される画面の一例である。第１から第４の実施形態では、処理ウインドウ３００の第１ドロップ領域３１０と第２ドロップ領域３２０は、重ならず独立していたが、第５の実施形態では第１ドロップ領域３１０と第２ドロップ領域３２０は、一部が重なり重複領域３１５を形成している。

【００８０】

図２１は、第５の実施形態における動作フローチャートである。ここでは、１つのファイルがドラッグ＆ドロップされるのを例にとって説明する。最初に、図２のステップＳ１００からＳ１４０が実行される。ステップＳ１４０の判定結果に基づいて、ステップＳ５

００、またはＳ５８０に移行する。具体的には、暗号処理プログラム１３０により暗号化された暗号化ファイルが、ドロップ領域（第１ドロップ領域３１０、第２ドロップ領域３２０、重複領域３１５を問わない）にドロップされたと判定された場合には、ステップＳ５８０に移行し、暗号処理プログラム１３０により暗号化されていないファイルが、ドロップ領域にドロップされたと判定された場合には、ステップＳ５００に移行する。

【００８１】

ステップＳ５００は、ステップＳ５０５からＳ５７０までのステップが含まれ、ファイルを暗号化する処理が行われる。ステップＳ５０５では、認証情報入力部１３４は、ファイルがドロップされた領域が重複領域３１５（図２０）であるか否かを判定する。重複領域３１５の場合には、ステップＳ５２０に移行し、重複領域３１５でない場合（第２ドロップ領域３２０と重なっていない第１ドロップ領域３１０、または、第１ドロップ領域３１０と重なっていない第２ドロップ領域３２０の場合）には、ステップＳ５１０に移行する。ステップＳ５１０に移行した場合は、第１の実施形態において、暗号化されていないファイルが第１ドロップ領域３１０あるいは第２ドロップ領域３２０にドラッグ＆ドロップされた場合と同じであり、図２のステップＳ１５０のファイルを暗号化する処理が実行される。

【００８２】

ステップＳ５２０では、認証情報入力部１３４は、重複領域３１５のうちの最初のドロップ領域である第１ドロップ領域３１０に対応する第１認証情報入力ウインドウ６００（図５）を表示部２４０に表示し、第１の認証情報のユーザ入力（第１のユーザ入力）を受け付ける。ステップＳ５３０では、認証情報入力部１３４は、重複領域３１５のうちの次のドロップ領域である第２ドロップ領域３２０に対応する第２認証情報入力ウインドウ７００（図６）を表示部２４０に表示し、第２の認証情報のユーザ入力（第２のユーザ入力）を受け付ける。ステップＳ５４０では、認証情報入力部１３４は、重複領域３１５を形成する全てのドロップ領域に対応する認証情報（ユーザ入力）が完了したか否かを判定する。重複領域３１５を形成する全てのドロップ領域に対応する認証情報（ユーザ入力）が完了していない場合には、ステップＳ５３０に移行し、完了している場合には、ステップＳ５５０に移行する。

【００８３】

ステップＳ５５０では、秘密鍵生成部１３８は、ステップＳ５２０、Ｓ５３０で入力された全ての認証情報のユーザ入力から１つの秘密鍵を生成する。ステップＳ５６０、Ｓ５７０では、図２のステップＳ２００、Ｓ２１０と同様に、ファイルの暗号化処理及び格納フォルダ１５０（図１）への暗号化ファイルの格納を行う。

【００８４】

ステップＳ１４０で暗号処理プログラム１３０により暗号化された暗号化ファイルが、ドロップ領域（第１ドロップ領域３１０、第２ドロップ領域３２０、重複領域３１５を問わない）にドロップされたと判定された場合には、ステップＳ５８０のファイルを復号する処理が実行される。ステップＳ５８０のファイルを復号する処理は、以下に説明する点を除き、図２に示したステップＳ２２０のファイルを復号する処理とほぼ同じである。認証情報入力部１３４は、暗号化ファイルに格納されている、どの認証情報入力方式を用いたかを示す識別子から、１又は複数の認証情報入力方式を特定する。そして、特定された全ての認証情報入力方式によるユーザ入力を受け付ける。秘密鍵生成部１３８は、ステップＳ５５０と同様に、入力された全ての認証情報のユーザ入力から１つの秘密鍵を生成する。これ以外の処理については、図２のステップＳ２２０の復号処理と同じである。

【００８５】

以上、第５の実施形態によれば、複数のドロップ領域３１０、３２０は、一部が重なって重複領域３１５を形成しており、暗号処理プログラム１３０は、互いに重なったＮ個（Ｎは２以上の整数であり、第５の実施形態ではＮ＝２である）のドロップ領域の重複部分（重複領域３１５）に暗号化を行いたいファイルがドロップされたとき、Ｎ個のドロップ領域に対応するＮ個の認証情報入力方法によるＮ個の認証情報のユーザ入力を受け付ける

処理と、Ｎ個の認証情報から１つの秘密鍵を生成する処理と、を電子機器２００に実行させるので、認証情報のユーザ入力が解読されにくく、ファイルの暗号化における利便性を及びセキュリティを向上させることができる。

【００８６】

・第６の実施形態：

図２２は、第６の実施形態の外部記憶装置１０６と、電子機器２００を示す説明図である。第６の実施形態の外部記憶装置１０６は、第１の実施形態の外部記憶装置１００と比較すると、ファイルサイズ取得部１４６を備えている点が異なる。ファイルサイズ取得部１４６は、ドロップ領域（第１ドロップ領域３１０、第２ドロップ領域３２０）のいずれかにドロップされたファイルのファイルサイズを取得する。

【００８７】

図２３は、第６の実施形態における動作フローチャートである。ステップＳ１３０までの処理は、第１の実施形態における処理と同じである。ステップＳ６００では、ファイルサイズ取得部１４６は、ドロップされたファイルのファイルサイズを取得する。

【００８８】

ステップＳ６１０では、暗号化処理部１４０は、ステップＳ６００で取得されたファイルサイズが予め定められた大きさ以上の場合には、ステップＳ６２０に移行し、ファイルサイズが予め定められた大きさ未満の場合には、ステップＳ６４０に移行する。ここで、ドロップ領域（第１ドロップ領域３１０、第２ドロップ領域３２０）にドロップされたファイルが複数ある場合には、ファイルサイズは、複数のファイルのファイルサイズの合計である。ステップＳ６４０では、図１２のステップＳ３００に移行する。

【００８９】

ステップＳ６２０では、暗号処理プログラム１３０は、ファイルを暗号化する処理または復号する処理に時間がかかるため、処理するファイルの数を減らすか、処理する容量を減らしてやり直すべき旨を表示部２４０（図２２）に表示する。暗号処理プログラム１３０は、ユーザからの処理の中止の同意を待ってステップＳ６３０に移行し、処理を中止する。なお、ステップＳ６２０において、ユーザの同意が入力されない場合には、暗号処理プログラム１３０は、暗号化や復号の処理を実行せずに、同意が入力されるまで待機する。

【００９０】

以上、第６の実施形態によれば、暗号処理プログラム１３０は、複数のドロップ領域３１０、３２０のいずれかにドロップされたファイルのファイルサイズを取得し、ファイルサイズが予め定められた大きさ以上の場合には、認証情報入力方法によるユーザ入力を受け付ける前にユーザに処理するファイルの数を減らすか、処理する容量を減らしてやり直すべき旨を表示部２４０に表示し、暗号化または復号する処理を中止する旨の同意を受け付ける。すなわち、ドロップされたファイルのファイルサイズが大きい場合には、暗号化、あるいは復号する処理に時間がかかると予想される。かかる場合、暗号化あるいは復号する処理を実行しても、時間がかかるため、途中でキャンセルされ、その後、ユーザがファイルの数を少なくして、暗号化、あるいは復号をやり直す場合も有り得る。このように処理すべきファイルサイズが大きい場合には、処理に時間がかかる旨の警告を発し、ユーザの同意を得て処理を中止する。ユーザは、暗号化や復号に時間がかかることが予め分かるので、暗号化や復号の処理を開始した後にユーザが終了するよりも、ユーザビリティが向上し、暗号化、復号における利便性を向上させることができる。なお、ファイルサイズだけで無く、ファイル数が多い場合においても同様に処理を行ってもよい。ファイルサイズの合計が同じであっても、ファイル数が多い場合には、処理時間がかかるからである。

【００９１】

第６の実施形態において、処理後のファイルは、外部記憶装置１０６の格納フォルダ１５０に格納される。ここで、ステップＳ６００で得られたファイルサイズから、処理後のファイルサイズを算出し、処理後のファイルサイズが外部記憶装置１０６の記憶部１２０の空き容量よりも大きい場合には、その旨を表示部２４０に表示して、処理を中止しても

よい。処理後のファイルが外部記憶装置１０６の記憶部１２０に格納できないからである。

【００９２】

上記第１から第６の実施形態の説明において、暗号プログラムにおける暗号方式（暗号アルゴリズム）については、説明をしていない。すなわち、第１から第６の実施形態においては、暗号方式は、特定の暗号方式に限定されることはない。第１から第６の実施形態では、例えば、ＡＥＳ（Advanced Encryption Standard）、ＤＥＳ（Data Encryption Standard）、３ＤＥＳ、ＩＤＥＡ（International Data Encryption Algorithm）などの共通鍵（秘密鍵）方式の暗号方式が利用可能である。また、暗号方式は、ＲＳＡや楕円曲線暗号のような公開鍵暗号方式であってもよい。公開鍵暗号方式の場合、暗号鍵と復号鍵のうち一方（通常は暗号鍵）が公開され、他方（復号鍵）が秘密にされるが、本実施形態では、暗号鍵も公開されなくても良い。なお、公開鍵暗号方式は、共通鍵（秘密鍵）方式による暗号と同程度の暗号強度を得ようとする場合、共通鍵（秘密鍵）方式に比べて鍵長が長くなり、暗号化処理、復号処理に時間がかかる。そのため、共通鍵（秘密鍵）方式の暗号方式を利用することが好ましい。ここで、例えば、ＡＥＳは、鍵長（１２８ビット、１９２ビット、２５６ビット）のみを変えることで暗号強度を変えられるので、暗号方式として、ＡＥＳを用いることが好ましい。

【００９３】

・変形例：

上記第１から第６の実施形態においては、処理ウインドウ３００に形成されるドロップ領域として、第１ドロップ領域３１０と第２ドロップ領域３２０の２つのドロップ領域を有するものを例にとって説明したが、ドロップ領域は、３つ以上あってもよい。この場合、認証情報入力方式として、パスワード方式、パターン方式の他、ＮＦＣ（Near Field Communication）や生体認証を利用可能である。

【００９４】

上記各実施形態において、電子機器２００が複数のコネクタ２７０を有しており、複数の外部記憶装置１００が電子機器２００に接続されている場合、暗号化ファイル及び復号されたファイルの格納場所は、その起動した暗号処理プログラム１３０のあった外部記憶装置１００の格納フォルダ１５０である。例えば、電子機器２００に、第１の暗号処理プログラム１３０を有する第１の外部記憶装置１００と、第２の暗号処理プログラム１３０を有する第２の外部記憶装置１００とが接続されている場合、第１の暗号処理プログラム１３０が作成した第１の処理ウインドウにファイルがドロップされた場合には、暗号化ファイルは、第１の外部記憶装置１００の第１の格納フォルダ１５０に格納され、第２の暗号処理プログラム１３０が作成した第２の処理ウインドウにファイルがドロップされた場合には、暗号化ファイルは、第２の外部記憶装置１００の第２の格納フォルダ１５０に格納される。ファイルが復号される場合も同様に、復号されたファイルは、その起動した暗号処理プログラム１３０のあった外部記憶装置１００の格納フォルダ１５０に格納される。

【００９５】

上記各実施形態において、ユーザは、パスワードやパターンは管理するが、秘密鍵そのものは管理せず、また、パスワードやパターンが分かっても秘密鍵は、取り出せないので、ユーザから秘密鍵が知られるおそれが少ない。

【００９６】

上記各実施形態において、ユーザは、ファイルを暗号化または複合したい場合、ドロップ領域（例えば、第１ドロップ領域３１０）にそのファイルをドラッグ＆ドロップすることで、ファイルをドロップ領域に送っていた。ユーザは、ファイルをドラッグ＆ドロップする代わりに、ファイルをコピーし、ドロップ領域にはりつけることで、ドロップ領域にファイルを送ってもよい。具体的には、ユーザは、ファイルをコピーし、その後、ドロップ領域にファイルをペーストする（はりつける）。ドロップ領域は、ファイルがはりつけられるためのはりつけ領域である。なお、複数のファイルが選択されたときの処理される

ファイルの順番には、最初に処理されるファイルは、コピーのときに最初に選択したファイルであり、２番目以降は、アルファベット順である。また、フォルダが選択された場合には、アルファベット順である。また、ユーザは、ファイルをカットし、その後、ドロップ領域にファイルをペーストしてもよい（はりつけてもよい）。ファイルをコピーではなくカットした場合、ファイルが暗号化または複合された場合には、その暗号化前または複合前のファイルは削除される。但し、例えばファイルサイズが大きい等の理由により暗号化、または複合できなかった場合、あるいは、秘密鍵が異なるために複合できなかった場合には、その暗号化前または複合前のファイルは削除されないことが好ましい。

【００９７】

上記各実施形態において、暗号処理プログラム１３０は、外部記憶装置１００に格納されているとしたが、記憶媒体に格納されていてもよい。この場合、暗号処理プログラム１３０は、記憶媒体から外部記憶装置１００の記憶部１２０にコピーあるいはインストールされると、実行可能となる。ここで、記憶媒体とは、データを記憶させるための媒体であり、「記憶メディア」、「記録メディア」とも呼ばれる。記憶媒体は、磁気的、光学的にデータを書き込むものが多く、前者には例えばフレキシブルディスクがあり、後者には例えばＣＤ－ＲＯＭやＭＯディスクがある。また、記憶媒体には、メモリーカード、本実施形態の外部記憶装置も含まれる。

【００９８】

また、暗号処理プログラム１３０は、外部記憶装置１００を販売する会社のウェブサイトからダウンロードする、電子メールで受け取る等ネットワークを介して取得できるようになっていてもよい。

【００９９】

上記各実施形態において、暗号処理プログラム１３０が実行される場合には、暗号処理プログラム１３０は電子機器２００の記憶部２２０にコピーされてから起動してもよい。格納フォルダ１５０が外部記憶装置１００の記憶部１２０以外の場所に格納されている場合には、暗号処理プログラムを起動中であっても外部記憶装置１００を電子機器２００から取り外すことが可能となる。

【０１００】

本発明は、上述の実施形態に限られるものではなく、その趣旨を逸脱しない範囲において種々の構成で実現することができる。例えば、発明の概要の欄に記載した各形態中の技術的特徴に対応する実施形態の技術的特徴は、上述の課題の一部又は全部を解決するために、或いは、上述の効果の一部又は全部を達成するために、適宜、差し替えや、組み合わせを行うことが可能である。また、その技術的特徴が本明細書中に必須なものとして説明されていなければ、適宜、削除することが可能である。

【符号の説明】

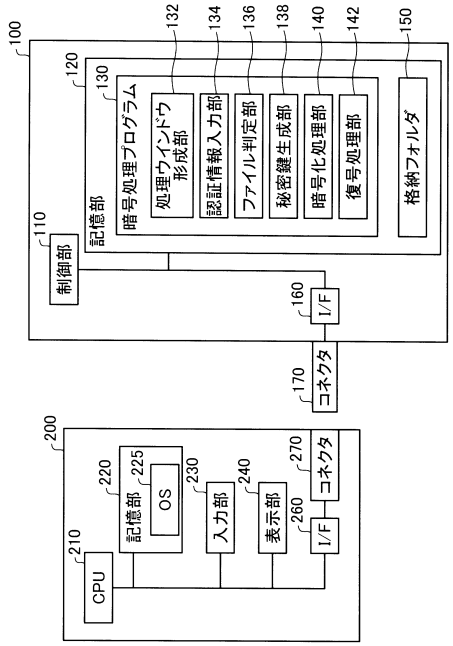
【０１０１】

１００…外部記憶装置
１０２…外部記憶装置
１０６…外部記憶装置
１１０…制御部
１２０…記憶部
１３０…暗号処理プログラム
１３２…処理ウインドウ形成部
１３４…認証情報入力部
１３６…ファイル判定部
１３８…秘密鍵生成部
１４０…暗号化処理部
１４２…復号処理部
１４４…機器識別部
１４６…ファイルサイズ取得部

１５０…格納フォルダ
１６０…インターフェース
１７０…コネクタ
１８０…機器識別子
２００…電子機器
２１０…ＣＰＵ
２２０…記憶部
２２５…オペレーティングシステム
２３０…入力部
２４０…表示部
２４２…カーソル
２６０…インターフェース
２７０…コネクタ
３００…処理ウインドウ
３１０…第１ドロップ領域
３１０ｍ…小ドロップ領域
３１０ｓ…小ドロップ領域
３１０ｗ…小ドロップ領域
３１１…イメージパターン
３１５…重複領域
３２０…第２ドロップ領域
３２０ｍ…小ドロップ領域
３２０ｓ…小ドロップ領域
３２０ｗ…小ドロップ領域
３２１…イメージパターン
３３０…ステータスバー
３４０…パス
４００…ウインドウ
５００…ウインドウ
６００…第１認証情報入力ウインドウ
６１０…識別情報入力部
６２０…完了ボタン
６３０…クリアボタン
７００…第２認証情報入力ウインドウ
７１０…識別情報入力部
７２０…完了ボタン
７３０…クリアボタン
５１３０…アイコン
５１５０…アイコン

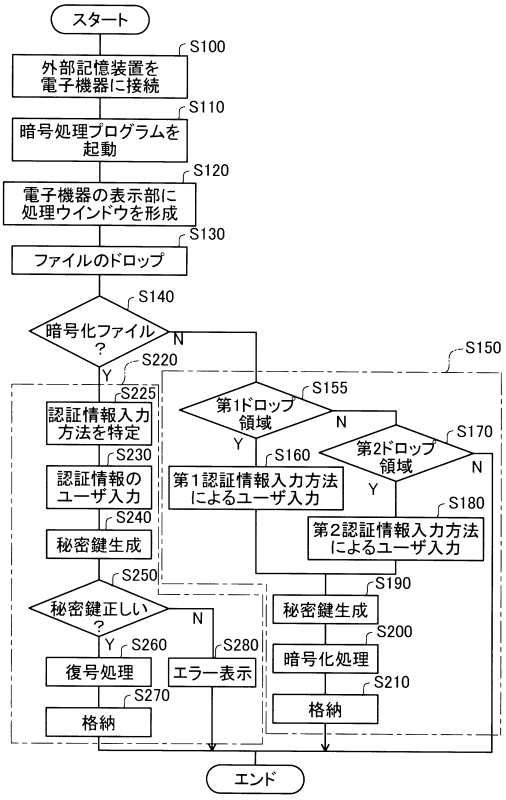
【図１】

図1



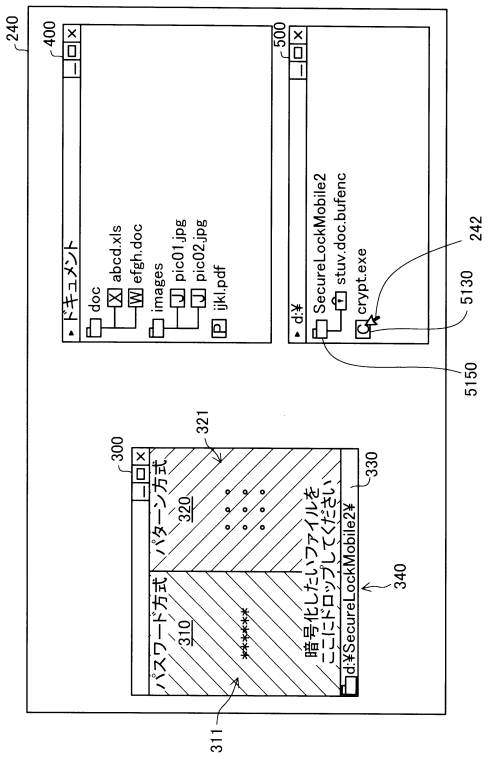
【図２】

図2



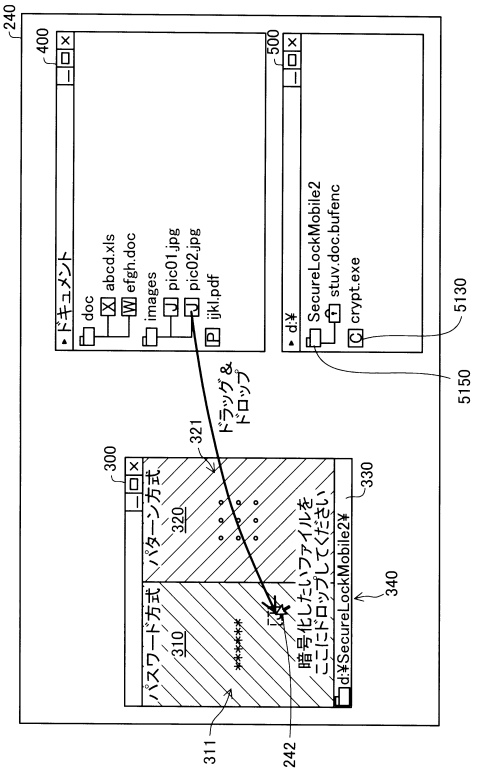
【図３】

図3



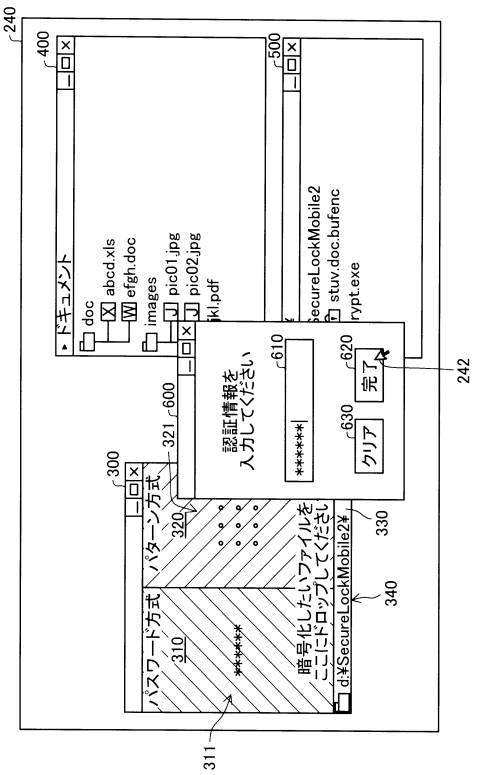
【図４】

図4



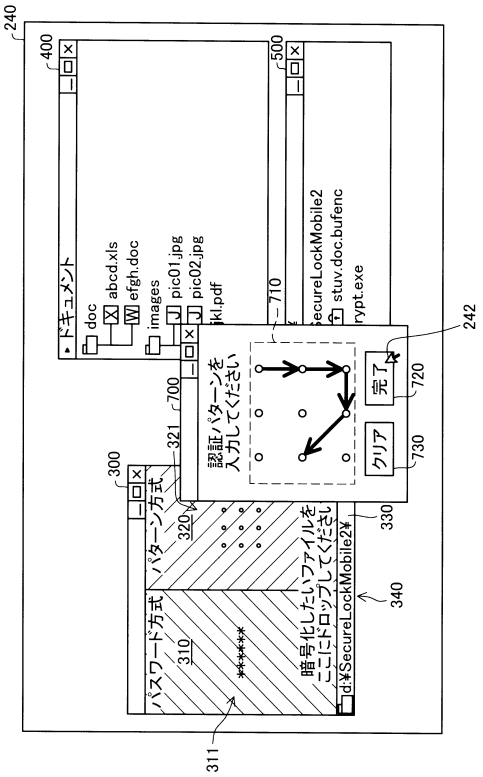
【図５】

図5



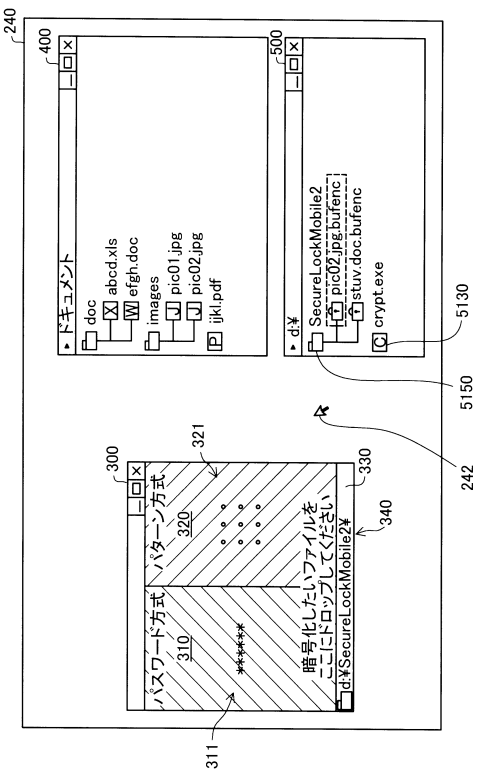
【図６】

図6



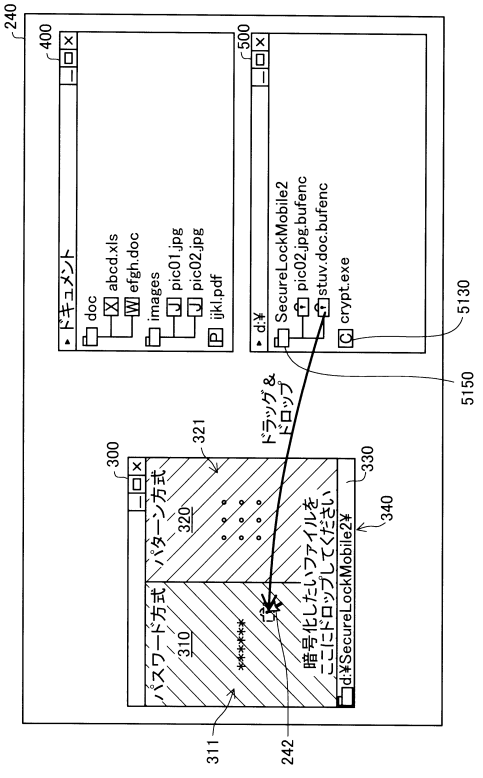
【図７】

図7



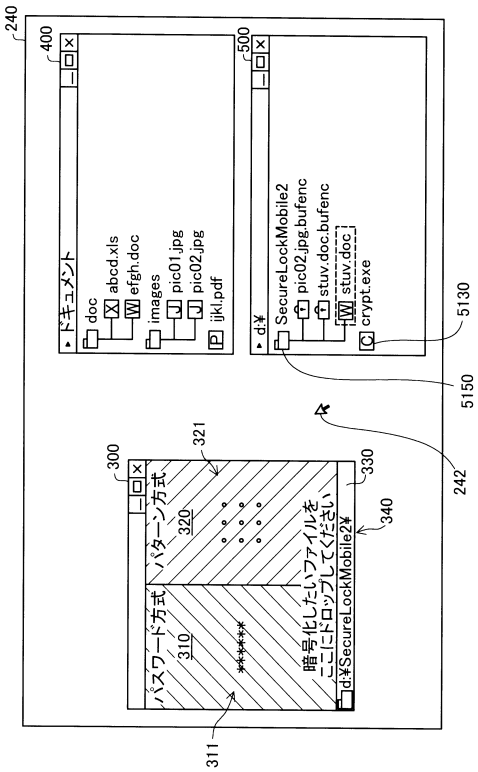
【図８】

図8



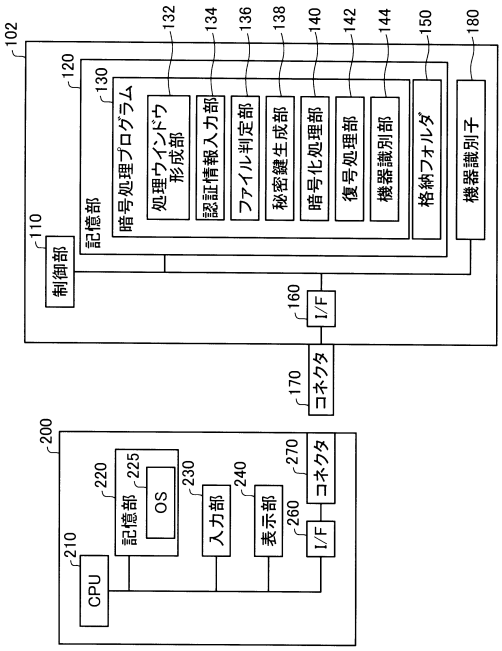
【図９】

図9



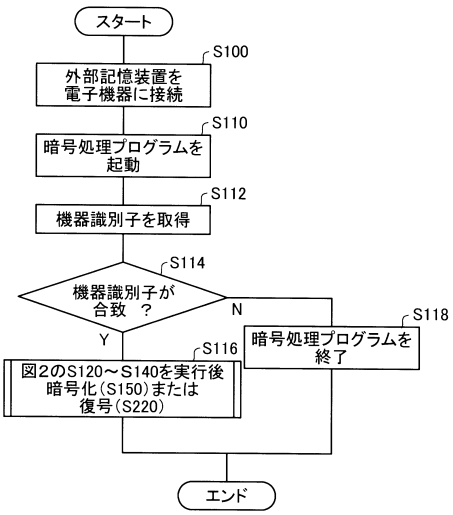
【図１０】

図10



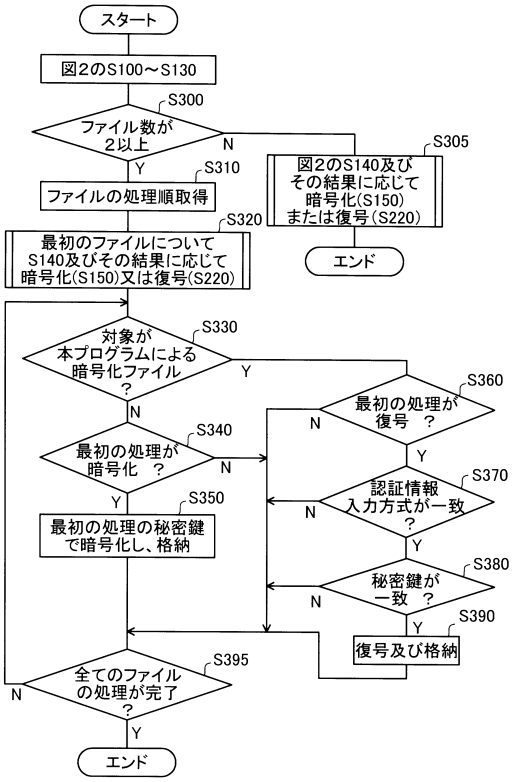
【図１１】

図11



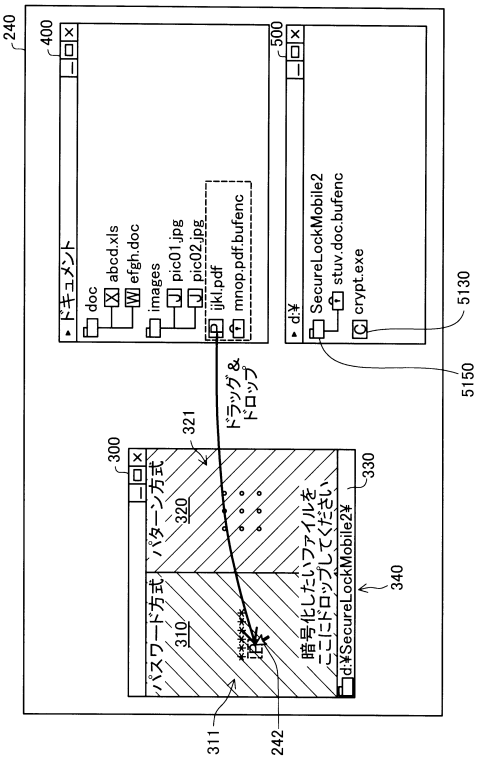
【図１２】

図12



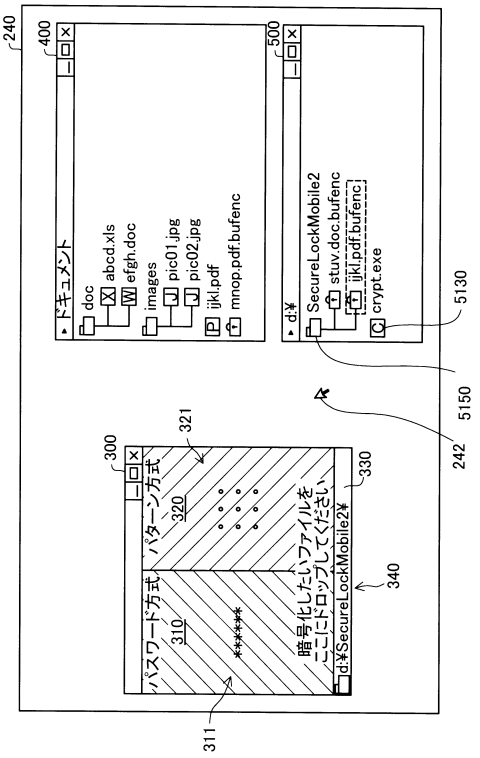
【図１３】

図13



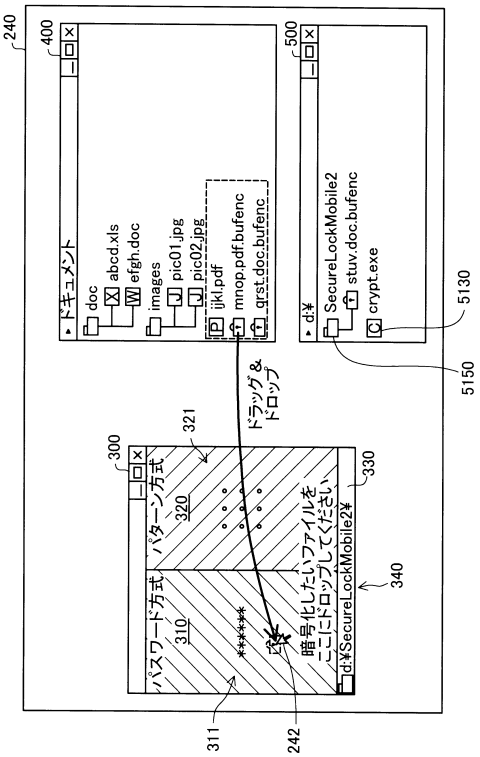
【図１４】

図14



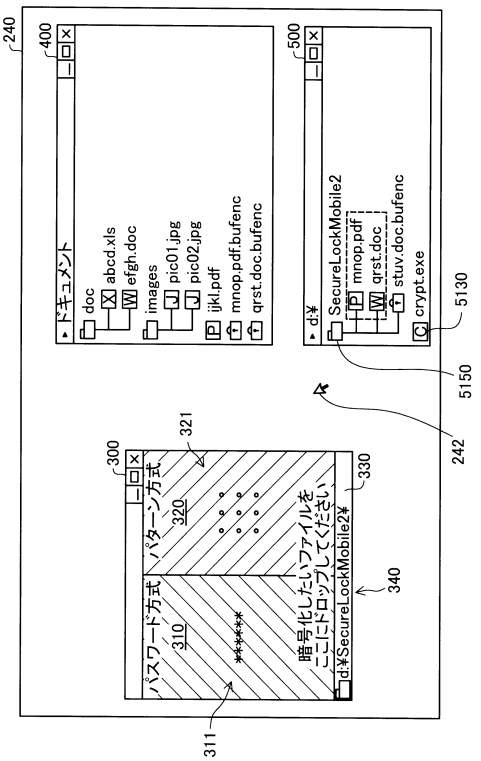
【図１５】

図15



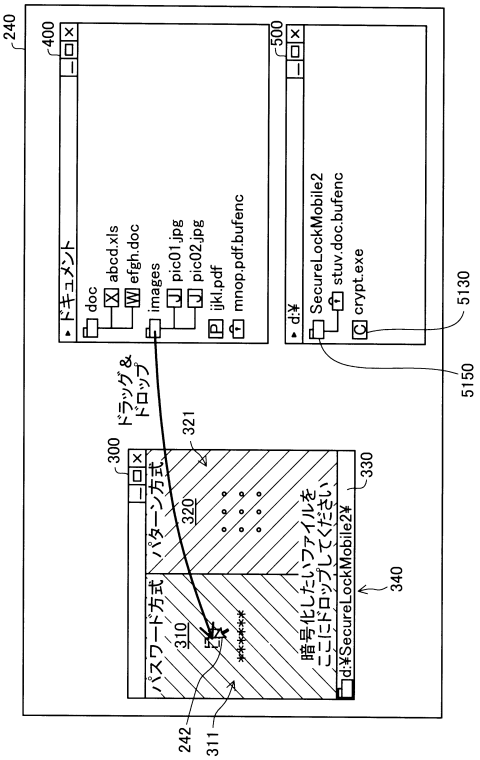
【図１６】

図16



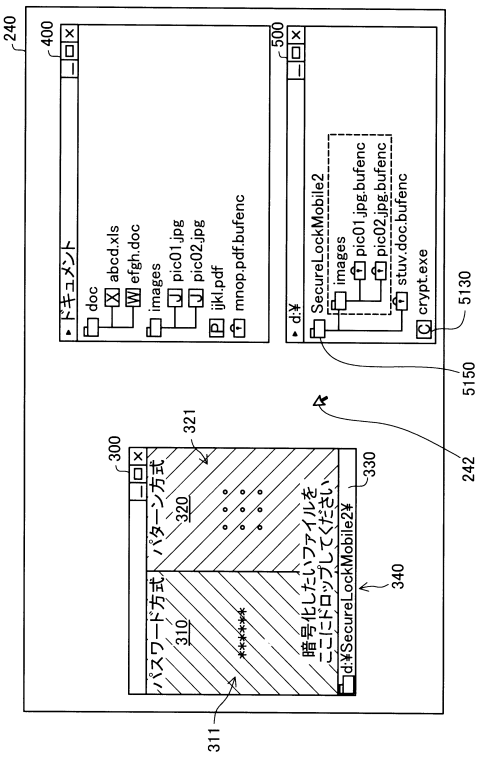
【図１７】

図17



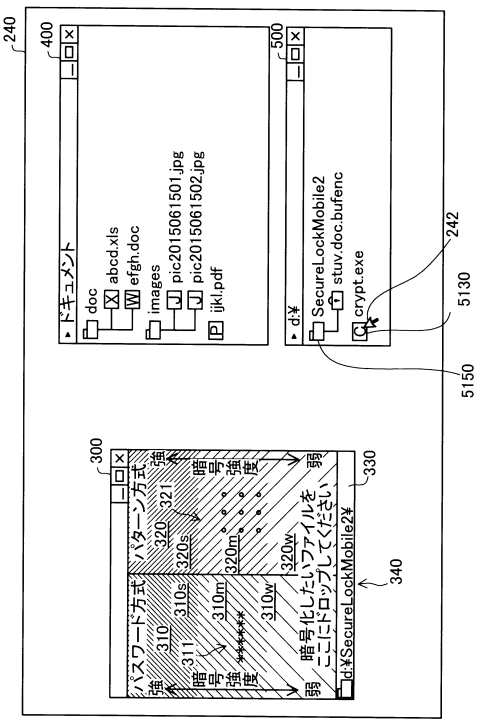
【図１８】

図18



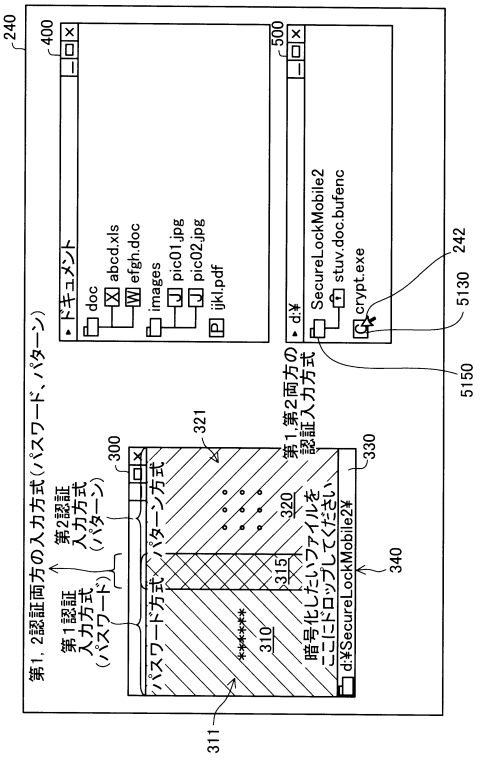
【図１９】

図19



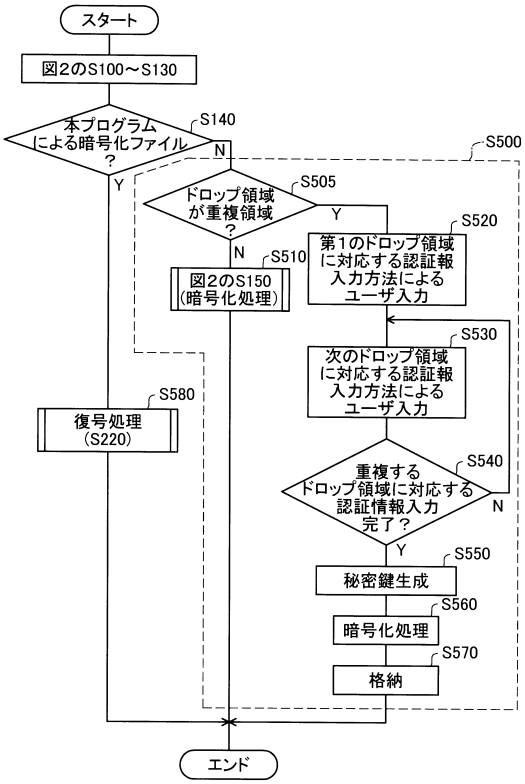
【図２０】

図20



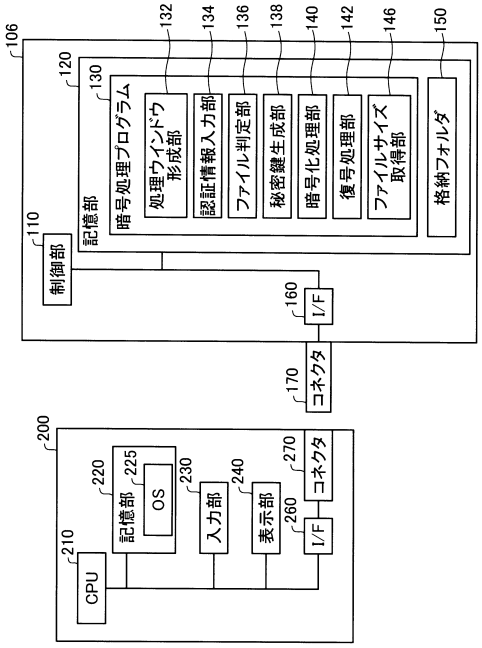
【図２１】

図21



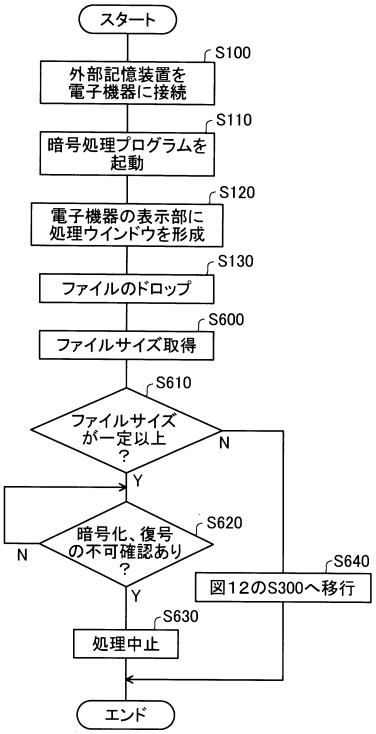
【図２２】

図22



【図２３】

図23



フロントページの続き

(56)参考文献 特開２０１１－１７０７１９（ＪＰ，Ａ）
特開平０７－０９２９０８（ＪＰ，Ａ）
特開２００８－０５９２８６（ＪＰ，Ａ）
米国特許第０５５７７１２５（ＵＳ，Ａ）
米国特許第０６０２３５０６（ＵＳ，Ａ）
データを暗号化して守る(SecureLock Mobile2)，データを暗号化して守る(SecureLock Mobile2) Ver.01，株式会社バッファロー，２０１６年 6月２３日，p.1-p.10，ＵＲＬ，http://manual.buffalo.jp/buf-doc/35021181-01.pdf

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