(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-50511
(P2019-50511A)
(43)公開日　平成31年3月28日(2019.3.28)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/08	(2006.01)	H04L	9/00	601C	5J104
G09C	1/00	(2006.01)	G09C	1/00	640D	
H04L	9/32	(2006.01)	H04L	9/00	601F	
			H04L	9/00	675B	

審査請求 未請求　請求項の数 11　ＯＬ　（全 18 頁）

(21)出願番号　特願2017-174072 (P2017-174072)
(22)出願日　平成29年9月11日 (2017.9.11)

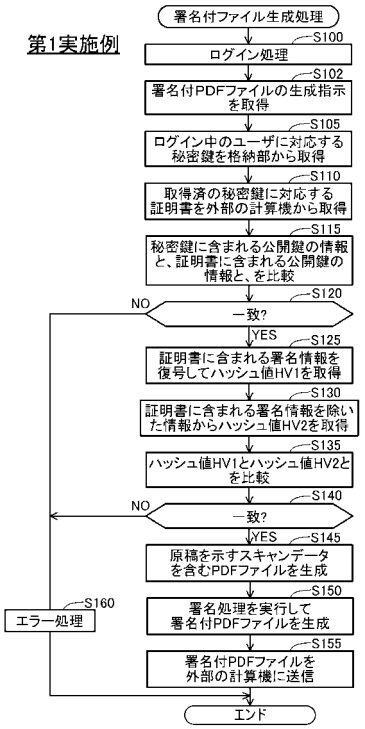
(71)出願人　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町１５番１号
(74)代理人　110001058
特許業務法人鳳国際特許事務所
(72)発明者　斉藤　健
名古屋市瑞穂区苗代町１５番１号　ブラザー工業株式会社内

Ｆターム(参考)　5J104 AA08 AA16 EA04 EA10 EA19 LA03 MA01 NA02 NA12 NA37 NA38 PA07 PA10

(54)【発明の名称】情報処理装置、および、コンピュータプログラム

(57)【要約】
【課題】秘密鍵と公開鍵とを用いる処理において不揮発性の格納部の容量を、セキュリティを損なうことなく低減する。
【解決手段】情報処理装置は、秘密鍵が格納される不揮発性の格納部と、情報処理装置とは異なる外部装置と通信するためのインタフェースと、格納部から秘密鍵を取得する秘密鍵取得部と、秘密鍵に対応する公開鍵を含む証明書を、インタフェースを介して特定の外部装置から取得する証明書取得部と、格納部から取得される秘密鍵を用いて変換処理を実行して変換済データを生成する変換部と、証明書を出力する出力部と、を備える。変換処理は、データを暗号化する処理と暗号化されたデータを復号する処理とのいずれかを含む。
【選択図】　図３

第1実施例



【特許請求の範囲】
【請求項１】
情報処理装置であって、
秘密鍵が格納される不揮発性の格納部と、
前記情報処理装置とは異なる外部装置と通信するためのインタフェースと、
前記格納部から前記秘密鍵を取得する秘密鍵取得部と、
前記秘密鍵に対応する公開鍵を含む証明書を、前記インタフェースを介して特定の外部装置から取得する証明書取得部と、
前記格納部から取得される前記秘密鍵を用いて変換処理を実行して変換済データを生成する変換部であって、前記変換処理は、データを暗号化する処理と、前記公開鍵を用いて暗号化されたデータを復号する処理と、のいずれかを含む、前記変換部と、
前記証明書と、を出力する出力部と、
を備える、情報処理装置。
【請求項２】
請求項１に記載の情報処理装置であって、さらに、
署名対象のデータを取得するデータ取得部と、
前記署名対象のデータに基づいて特定データを生成する生成部と、
を備え、
前記変換部は、前記変換処理として、前記秘密鍵を用いて前記特定データを暗号化する署名処理を実行して、前記変換済データとして署名データを生成し、
前記出力部は、前記署名対象のデータと、前記署名データと、前記証明書と、を含む署名付データを出力する、情報処理装置。
【請求項３】
請求項２に記載の情報処理装置であって、
前記出力部は、前記署名付きデータを、前記インタフェースを介して前記特定の外部装置に送信する、情報処理装置。
【請求項４】
請求項１～３のいずれかに記載の情報処理装置であって、
複数個の前記秘密鍵のそれぞれは、識別情報と対応付けられ、
前記秘密鍵取得部は、
第１の前記識別情報が指定される場合に、前記第１の識別情報に対応する第１の前記秘密鍵を前記格納部から取得し、
第２の前記識別情報が指定される場合に、前記第２の識別情報に対応する第２の前記秘密鍵を前記格納部から取得し、
前記証明書取得部は、
前記第１の識別情報が指定される場合に、前記第１の秘密鍵に対応する第１の前記公開鍵を含む前記証明書を、前記特定の外部装置から取得し、
前記第２の識別情報が指定される場合に、前記第２の秘密鍵に対応する第２の前記公開鍵を含む前記証明書を、前記特定の外部装置から取得する、情報処理装置。
【請求項５】
請求項１～４のいずれかに記載の情報処理装置であって、
複数個の前記秘密鍵のそれぞれは、対応する前記公開鍵を含む前記証明書のファイル名と対応付けられ、
前記証明書取得部は、
前記秘密鍵取得部によって特定の前記秘密鍵が取得される場合に、前記特定の秘密鍵に対応する特定の前記ファイル名を用いて、前記特定の秘密鍵に対応する特定の前記公開鍵を含む前記証明書を、前記特定の外部装置から取得する、情報処理装置。
【請求項６】
請求項１～４のいずれかに記載の情報処理装置であって、
前記格納部には、複数個の前記秘密鍵が格納され、

前記証明書取得部は、前記秘密鍵取得部によって特定の前記秘密鍵が取得される場合に、前記格納部に格納される複数個の前記証明書を、前記特定の外部装置から取得し、
前記情報処理装置は、さらに、
取得済の前記複数個の証明書の中から、前記特定の秘密鍵に対応する特定の前記公開鍵を含む前記証明書を選択する選択部を備える、情報処理装置。
【請求項７】
請求項１～６のいずれかに記載の情報処理装置であって、さらに、
前記特定の外部装置から取得される前記証明書が、前記格納部から取得される前記秘密鍵に対応する真正な証明書であるか否かを判断する判断部を備え、
前記出力部は、前記秘密鍵に対応する真正な証明書であると判断された前記証明書を出力する、情報処理装置。
【請求項８】
請求項７に記載の情報処理装置であって、
前記判断部は、
第１の判断方法を用いて、対象の前記証明書が真正な証明書であるか否かを判断する第１の判断処理を実行し、
前記第１の判断処理において、対象の前記証明書が真正な証明書であると判断される場合に、第２の判断方法を用いて、対象の前記証明書が真正な証明書であるか否かを判断する第２の判断処理であって、前記第１の判断処理よりも処理負荷が高い前記第２の判断処理を実行し、
前記第１の判断処理において、対象の前記証明書が真正な証明書でないと判断される場合に、前記第２の判断処理を実行しない、情報処理装置。
【請求項９】
請求項８に記載の情報処理装置であって、
前記秘密鍵は、対応する前記公開鍵の少なくとも一部を含み、
前記第１の判断処理は、前記格納部から取得される前記秘密鍵に含まれる前記公開鍵の少なくとも一部と、前記特定の外部装置から取得される前記証明書に含まれる前記公開鍵の少なくとも一部と、が同一であるか否かを判断する処理である、情報処理装置。
【請求項１０】
請求項１～９のいずれかに記載の情報処理装置であって、さらに、
前記証明書取得部によって前記特定の外部装置から取得される前記証明書を、前記出力部による前記証明書の出力後も、一時的に格納する一時格納部を備え、
前記出力部による前記証明書の出力後において、前記秘密鍵が再度取得される際に、再度取得される前記秘密鍵に対応する前記証明書が前記一時格納部に格納されている場合には、
前記証明書取得部は、前記特定の外部装置から前記証明書を再度取得せず、
前記出力部は、前記一時格納部に格納された前記証明書を出力する、情報処理装置。
【請求項１１】
秘密鍵が格納される不揮発性の格納部と、前記情報処理装置とは異なる外部装置と通信するためのインタフェースと、を備える情報処理装置のためのコンピュータプログラムであって、
前記格納部から前記秘密鍵を取得する秘密鍵取得機能と、
前記秘密鍵に対応する公開鍵を含む証明書を、前記インタフェースを介して特定の外部装置から取得する証明書取得機能と、
前記格納部から取得される前記秘密鍵を用いて変換処理を実行して変換済データを生成する変換部であって、前記変換処理は、データを暗号化する処理と、前記公開鍵を用いて暗号化されたデータを復号する処理と、のいずれかを含む、前記変換機能と、
前記証明書を出力する出力機能と、
をコンピュータに実現させる、コンピュータプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本明細書は、秘密鍵と公開鍵とを用いる処理を行う情報処理装置、および、当該処理を実行するためのコンピュータプログラムに関する。
【背景技術】
【０００２】
従来から、秘密鍵と公開鍵とを用いる処理が知られている。例えば、特許文献１には、秘密鍵と公開鍵とを用いて、電子商取引において用いられる文書として電子署名付き文書の発行と閲覧とを行う技術が開示されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００２－２１５８２７号公報
【特許文献２】特開２００６－１０１２１８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、例えば、ユーザごとに秘密鍵と公開鍵とを含む情報を格納する場合等には、これらの情報を格納する装置において、必要とされる不揮発性の格納部の容量が大きくなる可能性があった。
【０００５】
本明細書は、秘密鍵と公開鍵とを用いる処理において、必要とされる不揮発性の格納部の容量を、セキュリティを損なうことなく低減できる技術を開示する。
【課題を解決するための手段】
【０００６】
本明細書に開示された技術は、上述の課題の少なくとも一部を解決するためになされたものであり、以下の適用例として実現することが可能である。
【０００７】
［適用例１］情報処理装置であって、秘密鍵が格納される不揮発性の格納部と、前記情報処理装置とは異なる外部装置と通信するためのインタフェースと、前記格納部から前記秘密鍵を取得する秘密鍵取得部と、前記秘密鍵に対応する公開鍵を含む証明書を、前記インタフェースを介して特定の外部装置から取得する証明書取得部と、前記格納部から取得される前記秘密鍵を用いて変換処理を実行して変換済データを生成する変換部であって、前記変換処理は、データを暗号化する処理と、前記公開鍵を用いて暗号化されたデータを復号する処理と、のいずれかを含む、前記変換部と、前記証明書を出力する出力部と、を備える、情報処理装置。
【０００８】
上記構成によれば、秘密情報として管理すべき秘密鍵は、情報処理装置の格納部に格納されるので、セキュリティを確保できる。そして、秘密鍵と比較して秘密情報として管理すべき必要性が低い公開鍵を含む証明書は、外部装置から取得される。この結果、情報処理装置において、必要とされる不揮発性の格納部の容量を、セキュリティを損なうことなく低減できる。
【０００９】
なお、本明細書に開示される技術は、種々の形態で実現することが可能であり、例えば、複合機、スキャナ、処理方法、これら装置の機能または上記方法を実現するためのコンピュータプログラム、そのコンピュータプログラムを記録した記録媒体、等の形態で実現することができる。
【図面の簡単な説明】
【００１０】

【図１】システム１０００の構成を示すブロック図である。
【図２】複合機１００および計算機２００に格納される各種の情報の説明図である。
【図３】第１実施例の署名付ファイル生成処理のフローチャートである。
【図４】第２実施例の署名付ファイル生成処理のフローチャートである。
【図５】第３実施例の署名付ファイル生成処理のフローチャートである。
【図６】第４実施例の署名付ファイル生成処理のフローチャートである。
【発明を実施するための形態】
【００１１】
Ａ．第１実施例
Ａ－１：システム１０００の構成
次に、実施の形態を実施例に基づき説明する。図１は、システム１０００の構成を示すブロック図である。
【００１２】
システム１０００は、複合機１００と、計算機２００と、を備える。複合機１００と計算機２００とは、ローカルエリアネットワークＮＴに接続されている。複合機１００と計算機２００とは、ローカルエリアネットワークＮＴを介して、互いに通信可能である。
【００１３】
複合機１００は、複合機１００のコントローラとしてのＣＰＵ１１０と、ＤＲＡＭなどの揮発性記憶装置１２０と、ハードディスクやフラッシュメモリなどの不揮発性記憶装置１３０と、画像を表示する液晶ディスプレイなどの表示部１４０と、ユーザによる操作を取得するためのボタンやタッチパネルなどの操作部１５０と、印刷実行部１６０と、読取実行部１７０と、インタフェース１９０と、を備えている。
【００１４】
印刷実行部１６０は、ＣＰＵ１１０の制御に従って、印刷処理を実行する。印刷処理は、所定の方式（例えば、レーザ方式や、インクジェット方式）で、用紙（印刷媒体の一例）上に画像を印刷する処理である。読取実行部１７０は、ＣＰＵ１１０の制御に従って、読取処理を実行する。読取処理は、ＣＣＤやＣＭＯＳなどの光電変換素子を含むイメージセンサを用いて光学的に文書等の対象物を読み取ることによって、読み取った画像を表すスキャンデータを生成する処理である。
【００１５】
ＣＰＵ１１０は、データ処理を行う演算装置（プロセッサ）である。揮発性記憶装置１２０は、ＣＰＵ１１０が処理を行う際に生成される種々の中間データを一時的に格納するバッファ領域ＢＡ１を提供する。不揮発性記憶装置１３０には、コンピュータプログラムＰＧ１と、鍵管理情報ＫＭＩと、が格納されている。また、不揮発性記憶装置１３０の一部の領域は、鍵格納部ＳＫＳとして用いられている。鍵管理情報ＫＭＩと、鍵格納部ＳＫＳと、については後述する。
【００１６】
コンピュータプログラムＰＧ１は、例えば、複合機１００の製造時に不揮発性記憶装置１３０に予め格納されて提供され得る。これに代えて、コンピュータプログラムＰＧ１は、複合機１００のベンダによって運営されるサーバ（図示省略）からダウンロードされる形態で提供されても良く、ＣＤ－ＲＯＭなどに記録された形態で提供されても良い。
【００１７】
ＣＰＵ１１０は、コンピュータプログラムＰＧ１を実行することによって、複合機１００を制御する制御処理を実行する。例えば、ＣＰＵ１１０は、制御処理の一部として、印刷実行部１６０や読取実行部１７０を制御して、印刷処理や読取処理を実行させることができる。また、ＣＰＵ１１０は、制御処理の一部として、後述する署名付ファイル生成処理を実行することができる。
【００１８】
インタフェース１９０は、外部装置、例えば、計算機２００とデータ通信を行うためのインタフェースである。本実施例では、インタフェース１９０は、ローカルエリアネット

ワークＮＴに接続するためのインタフェース、具体的には、イーサネット（登録商標）やＷｉ－Ｆｉ規格に準拠した有線や無線のインタフェースである。

【００１９】

計算機２００は、例えば、パーソナルコンピュータなどの公知の計算機であり、例えば、ローカルエリアネットワークＮＴに接続可能な装置からアクセスされるファイルサーバとして機能している。計算機２００は、計算機２００のコントローラとしてのＣＰＵ２１０と、ＤＲＡＭなどの揮発性記憶装置２２０と、ハードディスクやフラッシュメモリなどの不揮発性記憶装置２３０と、液晶ディスプレイなどの表示部２４０と、ユーザによる操作を取得するためのマウスやキーボードなどの操作部２５０と、インタフェース２９０と、を備えている。

【００２０】

ＣＰＵ２１０は、データ処理を行う演算装置（プロセッサ）である。揮発性記憶装置２２０は、ＣＰＵ２１０が処理を行う際に生成される種々の中間データを一時的に格納するバッファ領域ＢＡ２を提供する。不揮発性記憶装置２３０には、コンピュータプログラムＰＧ２が格納されている。また、不揮発性記憶装置２３０の一部の領域は、証明書格納部ＣＴＳとスキャンデータ格納部ＳＤＳとして用いられている。スキャンデータ格納部ＳＤＳは、複合機１００にて生成されたスキャンデータを格納するための記憶領域である。証明書格納部ＣＴＳについては後述する。

【００２１】

図２は、複合機１００および計算機２００に格納される各種の情報の説明図である。図２（Ａ）には、鍵格納部ＳＫＳの概念図が示されている。図２（Ａ）に示すように、複合機１００の鍵格納部ＳＫＳ（図１）には、複数個の秘密鍵ＳＫ１～ＳＫ３と、認証局の公開鍵ＰＫｃａが格納されている。

【００２２】

図２（Ｂ）には、証明書格納部ＣＴＳの概念図が示されている。図２（Ｂ）に示すように、計算機２００の証明書格納部ＣＴＳには、複数個の証明書ＣＴ１～ＣＴ３と、が格納されている。本実施例では、鍵格納部ＳＫＳに格納された複数個の秘密鍵ＳＫ１～ＳＫ３（図２（Ａ））と、証明書格納部ＣＴＳに格納された複数個の証明書ＣＴ１～ＣＴ３と、は、一対一で対応している。

【００２３】

なお、秘密鍵ＳＫ１～ＳＫ３、証明書ＣＴ１～ＣＴ３のそれぞれは、１個のファイルである。秘密鍵ＳＫ１～ＳＫ３、証明書ＣＴ１～ＣＴ３のファイル名は、符号と同じであるとする。例えば、秘密鍵ＳＫ１のファイル名は「ＳＫ１」であり、証明書ＣＴ１のファイル名は「ＣＴ１」であるとする。

【００２４】

例えば、ユーザＡは、自身の端末装置（図示省略）を用いて、秘密鍵ＳＫ１と、該秘密鍵ＳＫ１に対応する公開鍵ＰＫ１と、を生成する。ユーザＡは、端末装置を用いて、該公開鍵ＰＫ１を含む証明書署名要求（CSR：Certificate Signing Request）を生成し、当該要求を認証局（CA：Certification Authority）に送信する。これによって、ユーザＡは、認証局によって署名された証明書ＣＴ１の暗号化データを認証局から取得する。証明書ＣＴ１には、公開鍵ＰＫ１が含まれる。ユーザＡは、秘密鍵ＳＫ１を用いて該暗号化データ復号して証明書ＣＴ１を取得する。このようにして、秘密鍵ＳＫ１と証明書ＣＴ１との組が取得される。そして、ユーザＡの操作に基づいて、秘密鍵ＳＫ１は、複合機１００の鍵格納部ＳＫＳに格納・保存される。一方で、秘密鍵ＳＫ１に対応する証明書ＣＴ１は、計算機２００の証明書格納部ＣＴＳに格納・保存される。

【００２５】

同様にして、例えば、別のユーザＢによって、秘密鍵ＳＫ２と証明書ＣＴ２との組が取得され、ユーザＣによって、秘密鍵ＳＫ３と証明書ＣＴ３との組が取得される。そして、秘密鍵ＳＫ２、ＳＫ３は、複合機１００の鍵格納部ＳＫＳに格納・保存され、証明書ＣＴ２、ＣＴ３は、計算機２００の証明書格納部ＣＴＳに格納・保存される。このように、本

実施例では、秘密鍵ＳＫ１～ＳＫ３、および、対応する証明書ＣＴ１～ＣＴ３は、複合機１００の複数人のユーザに一対一で対応している。

【００２６】

図２（Ｂ）に示すように、証明書ＣＴ１は、公開鍵ＰＫ１と、署名情報ＳＮ１と、署名アルゴリズム情報ＡＩ１と、その他の情報ＯＩ１と、を含んでいる。公開鍵ＰＫ１は、上述した秘密鍵ＳＫ１に対応する公開鍵である。署名情報ＳＮ１は、認証局によって生成された情報であり、証明書ＣＴ１が真正であるか否かを判断するために用いられる。署名アルゴリズム情報ＡＩ１は、認証局が署名情報ＳＮ１を生成する際に用いられたアルゴリズム、具体的には、用いられたハッシュ関数と公開鍵暗号方式とを示す情報を含む。その他の情報ＯＩ１は、例えば、証明書のバージョン、証明書の有効期限、証明書を発行した認証局の名前などの各種の情報を含む。

【００２７】

署名情報ＳＮ１は、以下のように生成される。認証局は、証明書ＣＴ１に含まれる情報のうち、署名情報ＳＮ１を除いた情報（署名アルゴリズム情報ＡＩ１、公開鍵ＰＫ１、その他の情報ＯＩ１）を、署名アルゴリズム情報ＡＩ１にて示されるハッシュ関数を用いて、ハッシュ化して、ハッシュ値を生成する。認証局は、署名アルゴリズム情報ＡＩ１にて示される公開鍵暗号方式に従って、当該ハッシュ値を、認証局の秘密鍵ＳＫｃａ（図示省略、ユーザの秘密鍵ＳＫ１とは異なる）を用いて暗号化する。暗号化されたハッシュ値が、署名情報ＳＮ１である。ハッシュ関数のアルゴリズムには、例えば、「ＳＨＡ（Secure Hash Algorithm）１」、「ＳＨＡ２５６」が用いられる。公開鍵暗号方式のアルゴリズムには、例えば、「ＲＳＡ」が用いられる。認証局の秘密鍵ＳＫｃａは、図２（Ａ）の鍵格納部ＳＫＳに格納された認証局の公開鍵ＰＫｃａに対応する秘密鍵である。

【００２８】

図示は省略するが、証明書ＣＴ２、ＣＴ３も、それぞれ同様に、公開鍵と、署名情報と、署名アルゴリズム情報と、その他の情報と、を含んでいる。

【００２９】

図２（Ｃ）には、鍵管理情報ＫＭＩの概念図が示されている。図２（Ｃ）に示すように、鍵管理情報ＫＭＩは、管理テーブルＫＭＴと、証明書保存先情報ＣＴＩと、を含む。管理テーブルＫＭＴは、鍵格納部ＳＫＳに格納された各秘密鍵に対応するエントリＥＮを含む。各エントリＥＮは、秘密鍵の所有者であるユーザの表示名（例えば、「Ａｌｉｃｅ」）と、秘密鍵のファイル名（例えば、「ＳＫ１」）と、秘密鍵に対応する証明書のファイル名（例えば、「ＣＴ１」）と、秘密鍵の所有者であるユーザの識別子であるユーザＩＤ（例えば、「ＵＳＥＲ１」）と、を含む。例えば、秘密鍵と証明書の組（例えば、秘密鍵ＳＫ１と証明書ＣＴ１）とが、鍵格納部ＳＫＳと証明書格納部ＣＴＳに格納・保存されたときに、当該秘密鍵に対応するエントリＥＮが、複合機１００の管理者によって管理テーブルＫＭＴに記録される。

【００３０】

以上のように、鍵管理情報ＫＭＩにおいて、複数個の秘密鍵ＳＫ１～ＳＫ３は、識別情報としてのユーザＩＤ（例えば、「ＵＳＥＲ１」）、および、表示名（例えば、「Ａｌｉｃｅ」）と、対応付けられている。そして、複数個の秘密鍵ＳＫ１～ＳＫ３は、対応する公開鍵を含む証明書ＣＴ１～ＣＴ３のファイル名と対応付けられている。

【００３１】

証明書保存先情報ＣＴＩは、証明書ＣＴ１～ＣＴ３が格納された計算機２００の証明書格納部ＣＴＳに、複合機１００のＣＰＵ１１０がアクセスするための情報である。本実施例では、ＣＰＵ１１０は、ＦＴＰ（File Transfer Protocol）を用いて、計算機２００の証明書格納部ＣＴＳにアクセスするので、証明書保存先情報ＣＴＩは、ＦＴＰによるアクセスに必要な情報、例えば、アカウント名と、パスワードと、サーバ名と、を含む。さらに、証明書保存先情報ＣＴＩは、計算機２００における証明書格納部ＣＴＳの位置を示す情報、具体的には、証明書ＣＴ１～ＣＴ３が格納されたフォルダを示すフォルダパスを含む。

【００３２】
Ａ－２：署名付ファイル生成処理
図３は、第１実施例の署名付ファイル生成処理のフローチャートである。署名付ファイル生成処理は、例えば、ユーザの指示に基づいて、原稿を読取実行部１７０を用いて読み取ることによって生成されるスキャンデータを取得し、該スキャンデータを含む署名付ＰＤＦファイルを生成する処理である。
【００３３】
Ｓ１００では、ＣＰＵ１１０は、ログイン処理を実行する。本実施例では、署名付ファイル生成処理は、ログイン中のユーザの指示に基づいて実行されるため、署名付ＰＤＦファイルの生成を望むユーザは、複合機１００へのログインを行う。具体的には、ＣＰＵ１１０は、ユーザのログイン要求に応じて、図示しないログイン画面を操作部１５０に表示して、該ログイン画面を介して、認証情報（例えば、ユーザＩＤとパスワード）を取得する。ＣＰＵ１１０は、認証情報に基づいて、特定のユーザのログインを許容するか否かを判断する。ＣＰＵ１１０は、ログインを許容する場合には、特定のユーザのログイン状態に遷移し、ログインを許容しない場合には、エラー処理を実行する。以下では、図２（Ｃ）のユーザＩＤ「ＵＳＥＲ１」、表示名「Ａｌｉｃｅ」を有するユーザのログインが許容されたとして説明を続ける。
【００３４】
Ｓ１０２では、ＣＰＵ１１０は、操作部１５０を介して、ユーザから署名付ＰＤＦファイルの生成指示を取得する。例えば、ユーザは、原稿を読取実行部１７０の原稿台に載置した状態で、操作部１５０に、署名付ＰＤＦファイルの生成指示を入力する。Ｓ１０５では、ＣＰＵ１１０は、ログイン中のユーザに対応する秘密鍵を鍵格納部ＳＫＳから取得する。具体的には、ＣＰＵ１１０は、管理テーブルＫＭＴにおいて、現在ログイン中のユーザを示すユーザＩＤ（例えば、「ＵＳＥＲ１」）を検索し、該ユーザＩＤを含むエントリＥＮを参照して、該ユーザＩＤに対応付けられた秘密鍵が、秘密鍵ＳＫ１であることを特定する。ＣＰＵ１１０は、複合機１００の鍵格納部ＳＫＳ（図２（Ｃ））から特定済みの秘密鍵ＳＫ１を取得する。取得済みの秘密鍵ＳＫ１は、揮発性記憶装置１２０のバッファ領域ＢＡ１に格納される。
【００３５】
Ｓ１１０では、ＣＰＵ１１０は、取得済みの秘密鍵に対応する証明書を外部の計算機２００から取得する。例えば、ＣＰＵ１１０は、管理テーブルＫＭＴの現在ログイン中のユーザに対応するエントリＥＮを参照して、取得済みの秘密鍵ＳＫ１に対応する証明書のファイル名が「ＣＴ１」であることを特定する。ＣＰＵ１１０は、当該証明書のファイル名を用いて、秘密鍵に対応する証明書を外部の計算機２００から取得する。具体的には、ＣＰＵ１１０は、図２（Ｃ）の証明書保存先情報ＣＴＩに含まれるアカウント名とパスワードとサーバ名とを用いて、計算機２００にアクセスする。ＣＰＵ１１０は、証明書保存先情報ＣＴＩに含まれるフォルダパスによって示されるフォルダ（すなわち、図２（Ｂ）の証明書格納部ＣＴＳ）内のファイルであって、ファイル名「ＣＴ１」を有するファイルを、計算機２００に要求する。これによって、ＣＰＵ１１０は、計算機２００から証明書ＣＴ１を取得する。証明書ＣＴ１の取得は、上述したように、例えば、ＦＴＰに従って実行される。なお、変形例としては、ＦＴＰに代えて、他のプロトコル、例えば、ＳＭＴＰ（Simple Mail Transfer Protocol）や、ＣＩＦＳ（Common Internet File System）に従って、証明書ＣＴ１の取得が実行されても良い。取得済みの証明書ＣＴ１は、揮発性記憶装置１２０のバッファ領域ＢＡ１に格納される。このように、ＣＰＵ１１０は、秘密鍵に対応する証明書のファイル名を用いて、対応する証明書を、適切に、計算機２００から取得することができる。
【００３６】
Ｓ１１５～Ｓ１４０では、ＣＰＵ１１０は、Ｓ１１０にて取得済みの証明書ＣＴ１が、Ｓ１０５にて取得済みの秘密鍵ＳＫ１と対応する真正な証明書であるか否かを判断する。これによって、後述するＳ１５５にて出力される証明書が、真正な証明書であるか否かが

判断されるので、外部装置である計算機２００から証明書を取得する場合であっても、適切な証明書を出力できる。

【００３７】

取得済みの証明書ＣＴ１が真正な証明書であるか否かの判断は、２段階で行われる。Ｓ１１５、Ｓ１２０では、１段階目の判断として第１の判断方法を用いて簡易的な判断が行われる。Ｓ１２５～Ｓ１４０では、２段階目の判断として１段階目より複雑な第２の判断方法を用いて判断が行われる。以下により詳しく説明する。

【００３８】

Ｓ１１５では、ＣＰＵ１１０は、秘密鍵ＳＫ１に含まれる公開鍵の情報と、証明書ＣＴ１に含まれる公開鍵の情報と、を比較する。ＲＳＡの秘密鍵ＳＫ１は、「modulus」、「publicExponent」、「privateExponent」、「prime1」、「prime2」などの複数個の情報を含んでいる。そして、秘密鍵ＳＫ１に対応する公開鍵（対応する証明書ＣＴ１に含まれる公開鍵）は、秘密鍵ＳＫ１に含まれる情報のうち、「modulus」と、「publicExponent」と、を抜き出したものである。このように、秘密鍵ＳＫ１および証明書ＣＴ１は、共通の情報として、公開鍵の情報（具体的には、「modulus」、「publicExponent」）を含む。Ｓ１１０にて取得済みの証明書ＣＴ１が、秘密鍵ＳＫ１に対応する真正な証明書ＣＴ１である場合には、秘密鍵ＳＫ１に含まれる公開鍵と、証明書ＣＴ１に含まれる公開鍵とは、同一の公開鍵ＰＫ１である。したがって、この場合には、秘密鍵ＳＫ１に含まれる公開鍵の情報と、証明書ＣＴ１に含まれる公開鍵の情報とは、一致する。本実施例では、ＣＰＵ１１０は、秘密鍵ＳＫ１に含まれる公開鍵の「modulus」の値と、証明書ＣＴ１に含まれる公開鍵の「modulus」の値と、を比較する。

【００３９】

Ｓ１２０では、ＣＰＵ１１０は、秘密鍵ＳＫ１に含まれる公開鍵の情報と、証明書ＣＴ１に含まれる公開鍵の情報と、が一致したか否かを判断する。これらの情報が一致した場合には（Ｓ１２０：ＹＥＳ）、ＣＰＵ１１０は、２段階目の判断（Ｓ１２５～Ｓ１４０）に処理を進める。これらの情報が一致しない場合には（Ｓ１２０：ＮＯ）、Ｓ１１０にて取得済みの証明書ＣＴ１は、秘密鍵ＳＫ１に対応する真正な証明書ＣＴ１ではないと考えられる。このために、この場合には、ＣＰＵ１１０は、Ｓ１６０にてエラー処理を実行して、署名付ファイル生成処理を終了する。エラー処理では、例えば、ユーザに、秘密鍵ＳＫ１に対応する真正な証明書ＣＴ１が取得できない旨が通知される。

【００４０】

Ｓ１２５では、ＣＰＵ１１０は、証明書ＣＴ１に含まれる署名情報ＳＮ１を、認証局の公開鍵ＰＫｃａ（図２（Ａ））を用いて復号して、ハッシュ値ＨＶ１を取得する。

【００４１】

Ｓ１３０では、ＣＰＵ１１０は、証明書ＣＴ１に含まれる情報のうち、署名情報ＳＮ１を除いた情報（署名アルゴリズム情報ＡＩ１、公開鍵ＰＫ１、その他の情報ＯＩ１）を、署名アルゴリズム情報ＡＩ１にて示されるハッシュ関数を用いてハッシュ化して、ハッシュ値ＨＶ２を取得する。

【００４２】

Ｓ１３５では、ＣＰＵ１１０は、Ｓ１２５にて取得済のハッシュ値ＨＶ１と、Ｓ１３０にて取得済のハッシュ値ＨＶ２と、を比較する。

【００４３】

Ｓ１４０では、ＣＰＵ１１０は、ハッシュ値ＨＶ１とハッシュ値ＨＶ２とが一致したか否かを判断する。ハッシュ値ＨＶ１とハッシュ値ＨＶ２とが一致した場合には（Ｓ１４０：ＹＥＳ）、ＣＰＵ１１０は、Ｓ１４５に処理を進める。ハッシュ値ＨＶ１とハッシュ値ＨＶ２とが一致しない場合には（Ｓ１４０：ＮＯ）、Ｓ１１０にて取得済みの証明書ＣＴ１は、秘密鍵ＳＫ１に対応する真正な証明書ＣＴ１ではないと考えられる。このために、この場合には、ＣＰＵ１１０は、Ｓ１６０にてエラー処理を実行して、署名付ファイル生成処理を終了する。

【００４４】

以上の説明から解るように、第１の判断方法（Ｓ１１５、Ｓ１２０）は、秘密鍵ＳＫ１に対応する公開鍵の情報と、証明書ＣＴ１に含まれる公開鍵の情報と、を比較するだけであるが、第２の判断方法（Ｓ１２５～Ｓ１４０）は、ハッシュ関数を用いてハッシュ値ＨＶ２を生成する処理や署名情報ＳＮ１を復号する処理を含む。このために第２の判断方法は、第１の判断方法よりも処理負荷が高い。

【００４５】

Ｓ１４５では、ＣＰＵ１１０は、原稿を示すスキャンデータＳＤを含むＰＤＦファイルＰＦ（図示省略）を生成する。具体的には、ＣＰＵ１１０は、読取実行部１７０に原稿を読み取らせることによって、読取実行部１７０から原稿を示すスキャンデータＳＤを取得する。ＣＰＵ１１０は、当該スキャンデータＳＤを含むＰＤＦファイルＰＦを生成して、揮発性記憶装置１２０のバッファ領域ＢＡ１に格納する。

【００４６】

Ｓ１５０では、ＰＤＦファイルＰＦを用いて署名処理を実行して、署名付ＰＤＦファイルＳＰＦを生成する。図２（Ｄ）には、署名付ＰＤＦファイルＳＰＦの一例が示されている。署名付ＰＤＦファイルＳＰＦは、スキャンデータＳＤと、証明書ＣＴ１と、署名情報ＳＮｕと、を含む。具体的には、ＣＰＵ１１０は、Ｓ１４５にて生成されたＰＤＦファイルＰＦを、署名アルゴリズム情報ＡＩ１にて示されるハッシュ関数を用いてハッシュ化して、ハッシュ値ＨＶｕを取得する。ＣＰＵ１１０は、署名アルゴリズム情報ＡＩ１にて示される公開鍵暗号方式に従って、当該ハッシュ値ＨＶｕを、ログイン中のユーザの秘密鍵ＳＫ１を用いて暗号化する。暗号化されたハッシュ値ＨＶｕが、署名情報ＳＮｕである。ＣＰＵ１１０は、ＰＤＦファイルＰＦに、署名情報ＳＮｕと、署名情報ＳＮｕの生成に用いた秘密鍵ＳＫ１に対応する証明書ＣＴ１と、を格納することによって、署名付ＰＤＦファイルＳＰＦ（図２（Ｄ））を生成する。

【００４７】

Ｓ１５５では、ＣＰＵ１１０は、生成済の署名付ＰＤＦファイルＳＰＦを、外部の計算機２００に送信する。署名付ＰＤＦファイルＳＰＦの送信は、例えば、ＦＴＰに従って、実行される。変形例としては、ＦＴＰに代えて、他のプロトコル、例えば、ＳＭＴＰや、ＣＩＦＳに従って、署名付ＰＤＦファイルＳＰＦの送信が実行されても良い。署名付ＰＤＦファイルＳＰＦを受信した計算機２００のＣＰＵ２１０は、署名付ＰＤＦファイルＳＰＦを、指定されたフォルダ（図１のスキャンデータ格納部ＳＤＳ）に格納する。計算機２００に格納された署名付ＰＤＦファイルＳＰＦは、ユーザの利用に供される。

【００４８】

以上説明した第１実施例によれば、複合機１００（ＣＰＵ１１０）は、自身の不揮発性記憶装置１３０の鍵格納部ＳＫＳから秘密鍵ＳＫ１を取得し（Ｓ１０５）、秘密鍵ＳＫ１に対応する公開鍵ＰＫ１を含む証明書ＣＴ１を、インタフェース１９０を介して計算機２００から取得する（Ｓ１１０）。複合機１００は、秘密鍵ＳＫ１を用いて、ハッシュ値ＨＶｕを暗号化して署名情報ＳＮｕを生成する処理を含む署名処理を実行する（Ｓ１５０）。複合機１００は、署名情報ＳＮｕと、証明書ＣＴ１と、スキャンデータＳＤと、を含む署名付ＰＤＦファイルを、計算機２００に出力する。この構成によれば、秘密情報として管理すべき秘密鍵ＳＫ１は、秘密鍵ＳＫ１を使用する複合機１００の鍵格納部ＳＫＳに格納されるので、セキュリティを確保できる。そして、秘密鍵ＳＫ１と比較して秘密情報として管理すべき必要性が低い公開鍵ＰＫ１を含む証明書ＣＴ１は、外部の計算機２００から取得される。この結果、証明書ＣＴ１は、複合機１００の不揮発性記憶装置１３０に格納・保存される必要がない。したがって、複合機１００において、必要とされる不揮発性記憶装置１３０の容量を、セキュリティを損なうことなく低減できる。例えば、秘密鍵ＳＫ１と、対応する証明書ＣＴ１と、の両方を、複合機１００の不揮発性記憶装置１３０に格納・保存する場合と比較して、必要とされる不揮発性記憶装置１３０の容量を低減できる。特に、本実施例では、署名付きデータ（具体的には、署名付ＰＤＦファイルＳＰＦ）を出力するために、秘密鍵と証明書とを用いるので、例えば、ユーザごとに秘密鍵と証明書とを管理する場合があり得る。このような場合に、仮に、複合機１００自身に、秘密鍵

と証明書とを保存する場合には、複合機１００において必要とされる不揮発性記憶装置１３０の容量が大きくなりがちであるが、本実施例では、セキュリティを損なうことなく、必要な不揮発性記憶装置１３０の低減できる。

【００４９】

さらに、本実施例によれば、複合機１００は、署名付ＰＤＦファイルＳＰＦを、証明書ＣＴ１を格納する計算機２００に送信する（Ｓ１５５）。したがって、署名付ＰＤＦファイルＳＰＦと、証明書ＣＴ１と、は、同じ計算機２００にて格納・保存することができる。したがって、証明書ＣＴ１を格納するためだけに外部装置を用意する必要がなく、システム１０００を簡素化できる。

【００５０】

さらに、上記実施例によれば、図２（Ｃ）の管理テーブルＫＭＴにおいて、複数個の秘密鍵ＳＫ１～ＳＫ３は、ユーザＩＤ（例えば、「ＵＳＥＲ１」、「ＵＳＥＲ２」）と対応付けられている。そして、特定のユーザＩＤ（例えば、「ＵＳＥＲ１」）を用いたログイン処理（Ｓ１００）が行われることで、当該特定のユーザＩＤが指定される。そして、当該特定のユーザＩＤ（例えば、「ＵＳＥＲ１」）に対応する秘密鍵ＳＫ１が取得され（Ｓ１０５）、秘密鍵ＳＫ１に対応する公開鍵ＰＫ１を含む証明書ＣＴ１が計算機２００から取得される（Ｓ１１０）。すなわち、複合機１００は、第１のユーザＩＤ（例えば、「ＵＳＥＲ１」）が指定される場合に、第１のユーザＩＤに対応する第１の秘密鍵（例えば、秘密鍵ＳＫ１）を鍵格納部ＳＫＳから取得し、第２のユーザＩＤ（例えば、「ＵＳＥＲ２」）が指定される場合に、第２のユーザＩＤに対応する第２の秘密鍵（例えば、秘密鍵ＳＫ２）を鍵格納部ＳＫＳから取得する。そして、複合機１００は、第１のユーザＩＤが指定される場合に、第１の秘密鍵に対応する第１の公開鍵を含む証明書（例えば、証明書ＣＴ１）を計算機２００から取得し、第２のユーザＩＤが指定される場合に、第２の秘密鍵に対応する第２の公開鍵を含む証明書（例えば、証明書ＣＴ２）を計算機２００から取得する。この結果、複数個の秘密鍵ＳＫ１、ＳＫ２と、複数個の証明書ＣＴ１、ＣＴ２と、が用いられる場合であっても、必要とされる不揮発性記憶装置１３０の容量を、セキュリティを損なうことなく低減できる。例えば、本実施例のように、ユーザごとに秘密鍵と証明書とを管理する場合に、管理すべき秘密鍵と証明書の個数が多くなりがちである。このような場合においても必要とされる不揮発性記憶装置１３０の容量を低減できる。

【００５１】

さらに、上記実施例では、複合機１００は、第１の判断方法を用いて、証明書ＣＴ１が真正な証明書であるか否かを判断する第１の判断処理（Ｓ１１５、Ｓ１２０）を実行する。複合機１００は、第１の判断処理において、証明書ＣＴ１が真正な証明書であると判断される場合に（Ｓ１２０：ＹＥＳ）、第２の判断方法を用いて、証明書ＣＴ１が真正な証明書であるか否かを判断する第２の判断処理（Ｓ１２５～Ｓ１４０）を実行する。第１の判断処理において、証明書ＣＴ１が真正な証明書でないと判断される場合に（Ｓ１２０：ＮＯ）、第１の判断処理よりも処理負荷が高い第２の判断処理は、実行されない。この結果、効率的に、証明書ＣＴ１が真正な証明書であるか否かを判断できる。

【００５２】

さらに、上記実施例では、Ｓ１１５、Ｓ１２０の第１の判断処理は、秘密鍵ＳＫ１に含まれる公開鍵ＰＫ１の「modulus」と、証明書ＣＴ１に含まれる公開鍵ＰＫ１の「modulus」と、が同一であるか否かを判断する。この結果、比較的簡易に、証明書ＣＴ１が真正な証明書であるか否かの一応の判断ができる。

【００５３】

Ｂ．第２実施例

第２実施例では、図２（Ｃ）の管理テーブルＫＭＴにおいて、各エントリＥＮには、証明書のファイル名は含まれない。すなわち、鍵格納部ＳＫＳに格納された複数個の秘密鍵ＳＫ１～ＳＫ３のそれぞれには、対応する証明書ＣＴ１～ＣＴ３のファイル名は対応付けられていない。第２実施例のシステムの他の構成は、第１実施例のシステム１０００と同じである。

【００５４】
第２実施例では、複合機１００は、図３の署名付ファイル生成処理とは異なる署名付ファイル生成処理を実行する。図４は、第２実施例の署名付ファイル生成処理のフローチャートである。
【００５５】
Ｓ１１０Ｂにて、図３のＳ１１０～Ｓ１０５が実行された後のＳ１１０Ｂでは、ＣＰＵ１１０は、指定されたフォルダ、すなわち、証明書保存先情報ＣＴＩに含まれるフォルダパスによって示されるフォルダ内の全ての証明書を、計算機２００から取得する。具体的には、ＣＰＵ１１０は、ＦＴＰに従って、計算機２００にアクセスして、当該フォルダ内の全てのファイルを計算機２００に要求する。計算機２００は、指定されたファイル内の全てのファイル、すなわち、証明書格納部ＣＴＳに格納された証明書ＣＴ１～ＣＴ３を含む全ての証明書を、複合機１００に送信する。取得済みの全ての証明書は、揮発性記憶装置１２０のバッファ領域ＢＡ１に格納される。
【００５６】
Ｓ１１２Ｂでは、ＣＰＵ１１０は、取得済みの全ての証明書から１個の注目する証明書を選択する。Ｓ１１５Ｂでは、ＣＰＵ１１０は、図３の１１５と同様に、Ｓ１０５にて取得済みの秘密鍵ＳＫ１に含まれる公開鍵ＰＫ１の情報と、注目する証明書に含まれる公開鍵の情報と、を比較する。
【００５７】
Ｓ１２０Ｂでは、ＣＰＵ１１０は、秘密鍵ＳＫ１に含まれる公開鍵ＰＫ１の情報と、注目する証明書に含まれる公開鍵の情報と、が一致したか否かを判断する。これらの情報が一致した場合には（Ｓ１２０Ｂ：ＹＥＳ）、ＣＰＵ１１０は、２段階目の判断（Ｓ１２５～Ｓ２４０）に処理を進める。これらの情報が一致しない場合には（Ｓ１２０Ｂ：ＮＯ）、ＣＰＵ１１０は、Ｓ１２２Ｂに処理を進める。
【００５８】
Ｓ１２２Ｂでは、ＣＰＵ２１０は、取得済みの全ての証明書を注目する証明書として選択したか否かを判断する。全ての証明書が選択済みである場合には（Ｓ１２２Ｂ：ＹＥＳ）、ＣＰＵ２１０は、Ｓ１６０にてエラー処理を実行して、署名付ファイル生成処理を終了する。未選択の証明書がある場合には（Ｓ１２２Ｂ：ＮＯ）、ＣＰＵ２１０は、Ｓ１１２Ｂに戻って、未選択の証明書を新たな注目する証明書として選択する。
【００５９】
Ｓ１２５～Ｓ２４０では、注目する証明書について、図３のＳ１２５～Ｓ２４０と同様の処理が実行される。そして、Ｓ１７０Ｂでは、図３のＳ１４５～Ｓ１５５と同様の処理が行われて、署名付ＰＤＦファイルＳＰＦの生成・出力が行われる。
【００６０】
以上説明した第２実施例によれば、複合機１００は、計算機２００の証明書格納部ＣＴＳに格納される複数個の証明書を、計算機２００から取得し（Ｓ１１０Ｂ）、取得済の複数個の証明書の中から、秘密鍵ＳＫ１に対応する証明書ＣＴ１を選択する（Ｓ１１２Ｂ～Ｓ１２２Ｂ）。この結果、例えば、秘密鍵ＳＫ１に対応する証明書ＣＴ１のファイル名が予め鍵管理情報ＫＭＩに記録されていない場合であっても複数個の証明書の中から、適切な証明書を取得することができる。
【００６１】
Ｃ．第３実施例
第３実施例のシステムの構成は、第２実施例のシステムと同じである。第３実施例では、複合機１００は、図４の第２実施例の署名付ファイル生成処理とは異なる署名付ファイル生成処理を実行する。図５は、第３実施例の署名付ファイル生成処理のフローチャートである。
【００６２】
図５の署名付ファイル生成処理では、図５のＳ１００ＢとＳ１１０Ｂとの間に、Ｓ１０８Ｃが追加されている点が、図４の署名付ファイル生成処理と異なる。図５の署名付ファ

イル生成処理のその他の処理は、図４の署名付ファイル生成処理と同一である。
【００６３】
Ｓ１０８Ｃでは、ＣＰＵ１１０は、既に実行済みの署名付ファイル生成処理のＳ１１０Ｂにて取得済みの複数個の証明書が、揮発性記憶装置１２０のバッファ領域ＢＡ１に格納されている否かを判断する。本実施例では、以下の契機で、バッファ領域ＢＡ１から取得済みの複数個の証明書が消去される。そして、以下の契機が生じない限り、取得済みの複数個の証明書は、バッファ領域ＢＡ１に保持される。このために、Ｓ１０８Ｃの時点で、取得済みの複数個の証明書がバッファ領域ＢＡ１に残っている場合がある。
（１）複合機１００の電源が落とされたとき
（２）複合機１００が再起動されたとき
（３）他の処理（例えば、ファクシミリ処理や印刷処理）の実行のためにバッファ領域ＢＡ１の領域を確保する必要があるとき
【００６４】
取得済みの複数個の証明書がバッファ領域ＢＡ１に格納されていない場合には（Ｓ１０８Ｃ：ＮＯ）、Ｓ１１０Ｂにて、ＣＰＵ１１０は、指定されたフォルダ、すなわち、証明書保存先情報ＣＴＩに含まれるフォルダパスによって示されるフォルダ内の全ての証明書を、計算機２００から取得する。取得済みの複数個の証明書がバッファ領域ＢＡ１に格納されている場合には（Ｓ１０８Ｃ：ＹＥＳ）、Ｓ１１０Ｂはスキップされる。
【００６５】
このように、第３実施例では、複合機１００は、実行済みの署名付ファイル生成処理のＳ１１０Ｂにおいて、計算機２００から取得済みの複数個の証明書を、実行済みの署名付ファイル生成処理にて該署名付ＰＤＦファイルＳＰＦが出力された後も、バッファ領域ＢＡ１に一時的に格納しておく。そして、複合機１００は、その後に、署名付ファイル生成処理が再度実行されることによって、Ｓ１０５にて、秘密鍵が再度取得される際に、対応する証明書がバッファ領域ＢＡ１に格納されている場合には（Ｓ１０８Ｃ：ＹＥＳ）、複合機１００は、計算機２００から証明書を再度取得せず、バッファ領域ＢＡ１に格納された証明書を用いて、署名付ＰＤＦファイルＳＰＦの生成・出力を行う。この結果、計算機２００への無駄なアクセスを抑制して、証明書が計算機２００に格納されている場合であっても、効率良く、署名付ＰＤＦファイルＳＰＦの生成や出力を実行できる。
【００６６】
Ｄ．第４実施例
第４実施例のシステムの構成は、第１実施例のシステムと同じである。第４実施例では、複合機１００は、図３の第１実施例の署名付ファイル生成処理とは異なる署名付ファイル生成処理を実行する。図６は、第４実施例の署名付ファイル生成処理のフローチャートである。
【００６７】
図６の署名付ファイル生成処理では、図６のＳ１００ＤとＳ１１０との間に、Ｓ１０８Ｄが追加されている点が、図３の署名付ファイル生成処理と異なる。図６の署名付ファイル生成処理のその他の処理は、図３の署名付ファイル生成処理と同一である。
【００６８】
Ｓ１０８Ｄでは、ＣＰＵ１１０は、既に実行済みの署名付ファイル生成処理のＳ１１０にて計算機２００から取得され、さらに、Ｓ１１５～Ｓ１４０にて真正であることを検証済みの証明書であって、直前のＳ１０５にて取得済の秘密鍵に対応する証明書が、揮発性記憶装置１２０のバッファ領域ＢＡ１に格納されている否かを判断する。本実施例では、以下の契機で、バッファ領域ＢＡ１から検証済みの証明書が消去される。そして、以下の契機が生じない限り、検証済みの複数個の証明書は、バッファ領域ＢＡ１に保持される。このために、Ｓ１０８Ｄの時点で、検証済みの１以上の証明書がバッファ領域ＢＡ１に残っている場合がある。
（１）複合機１００の電源が落とされたとき
（２）複合機１００が再起動されたとき

（３）他の処理（例えば、ファクシミリ処理や印刷処理）の実行のためにバッファ領域ＢＡ１の領域を確保する必要があるとき

【００６９】

なお、上記（１）～（３）の契機に代えて、あるいは、これらの契機とともに、例えば、バッファ領域ＢＡ１に格納された検証済みの証明書の個数が特定数（例えば、２個）を超えた場合に、バッファ領域ＢＡ１に格納された時期が早い順に、１個ずつ検証済みの証明書が消去されても良い。

【００７０】

検証済みの対応する証明書がバッファ領域ＢＡ１に格納されていない場合には（Ｓ１０８Ｄ：ＮＯ）、Ｓ１１０にて、ＣＰＵ１１０は、取得済みの秘密鍵に対応する証明書を外部の計算機２００から取得する。検証済みの対応する証明書がバッファ領域ＢＡ１に格納されている場合には（Ｓ１０８Ｄ：ＹＥＳ）、ＣＰＵ１１０は、Ｓ１１０～Ｓ１４０をスキップして、処理をＳ１７０Ｄに進める。Ｓ１７０Ｄでは、図３のＳ１４５～Ｓ１５５の処理が実行される。すなわち、ＣＰＵ１１０は、バッファ領域ＢＡ１に格納されている検証済みの対応する証明書を用いて、署名付ＰＤＦファイルＳＰＦの生成や出力を実行する。

【００７１】

このように、第４実施例では、複合機１００は、実行済みの署名付ファイル生成処理のＳ１１０において取得され、Ｓ１１５～Ｓ１４０にて真正であることが検証済みの証明書を、実行済みの署名付ファイル生成処理にて該署名付ＰＤＦファイルＳＰＦが出力された後も、バッファ領域ＢＡ１に一時的に格納しておく。そして、複合機１００は、その後に、署名付ファイル生成処理が再度実行されることによって、Ｓ１０５にて、秘密鍵が再度取得される際に、検証済みで、かつ、対応する証明書がバッファ領域ＢＡ１に格納されている場合には（Ｓ１０８Ｄ：ＹＥＳ）、複合機１００は、計算機２００から証明書を再度取得せず、かつ、証明書の検証のための処理（Ｓ１１０～Ｓ１４０）を行わず、バッファ領域ＢＡ１に格納された証明書を用いて、署名付ＰＤＦファイルＳＰＦの生成・出力を行う。（Ｓ１７０Ｄ）。この結果、計算機２００への無駄なアクセスを抑制できるとともに、証明書の無駄な検証処理の実行を抑制できる。この結果、証明書が計算機２００に格納されている場合であっても、より効率良く、署名付ＰＤＦファイルＳＰＦの生成や出力を実行できる。

【００７２】

Ｅ.変形例

（１）上記各実施例では、秘密鍵と証明書とは、スキャンデータＳＤを含むＰＤＦファイルに対して署名するために用いられている。これに代えて、秘密鍵と証明書とは、他の処理のために用いられても良い。

【００７３】

例えば、複合機１００は、ユーザの端末装置（図示省略）をクライアントとして通信を行うサーバとして機能する場合がある。この場合において、複合機１００は、自身のサーバ証明書を、計算機２００の証明書格納部ＣＴＳに格納し、該サーバ証明書に対応する秘密鍵を複合機１００の鍵格納部ＳＫＳに格納する。そして、複合機１００は、ユーザの端末装置から接続要求があると、計算機２００にアクセスして計算機２００からサーバ証明書を取得する。複合機１００は、例えば、図３のＳ１２５～Ｓ１４０を実行して、サーバ証明書が真正であるか否かを判断し、サーバ証明書が真正である場合には、該サーバ証明書を端末装置に対して送信する。

【００７４】

端末装置は、該サーバ証明書を受信すると、例えば、図３のＳ１２５～Ｓ１４０を実行して、該サーバ証明書が真正であるか否かを判断する。そして、端末装置は、サーバ証明書が真正である場合には、該サーバ証明書に含まれる公開鍵を用いて、共通鍵を暗号化して、暗号化された共通鍵を、複合機１００に対して送信する。

【００７５】

複合機１００は、暗号化された共通鍵を受信すると、該暗号化された共通鍵を、サーバ証明書に対応する秘密鍵であって鍵格納部ＳＫＳに格納されている秘密鍵を用いて、復号する。これによって複合機１００は、共通鍵を取得する。この結果、複合機１００と端末装置との両方が、該共通鍵を所有した状態となるので、複合機１００と端末装置との間で、該共通鍵を用いた暗号通信を行うことができる。

【００７６】

以上の説明から解るように、上記各実施例では、ハッシュ値ＨＶｕを暗号化して署名情報ＳＮｕを生成する処理（図３のＳ１５０）が、変換処理の例であり、上記変形例では、暗号化された共通鍵を復号して共通鍵を取得する処理が、変換処理の例である。そして、上記各実施例では、署名情報ＳＮｕと証明書ＣＴ１とを含む署名付ＰＤＦファイルＳＰＦの送信（図３のＳ１５５）が、変換済みデータと証明書との出力の例であり、上記変形例では、端末装置へのサーバ証明書の送信が証明書の出力の例である。

【００７７】

また、上記各実施例では、秘密鍵と証明書とは、スキャンデータＳＤを含むＰＤＦファイルとは異なるデータに対して署名することによって、署名付データを生成するために用いられても良い。ＰＤＦファイルとは異なるデータは、例えば、テキストファイル、描画アプリケーションによって生成された画像ファイル、文書作成アプリケーションによって生成された文書ファイルを含む。

【００７８】

（２）上記各実施例では、証明書ＣＴ１～ＣＴ３を格納する証明書格納部ＣＴＳ（図２（Ｂ）は、計算機２００に備えられている。これに代えて、証明書ＣＴ１～ＣＴ３は、他の外部装置、例えば、ＵＳＢインタフェースを介して複合機１００と接続されるハードディスクやＵＳＢメモリなどの外部ストレージに格納されても良い。また、証明書ＣＴ１～ＣＴ３は、複合機１００とインターネットを介して接続されるクラウドサーバに格納されても良い。

【００７９】

（３）上記各実施例では、ユーザによって入力されるユーザＩＤを用いてログイン処理（図３のＳ１００）を行うことによって、秘密鍵に対応付けられた識別情報としてのユーザＩＤが指定され、該ユーザＩＤに対応する秘密鍵が取得される（図３のＳ１０５）。ログイン処理に代えて、例えば、複合機１００は、図３のＳ１０２の後に、秘密鍵に対応付けられた識別情報としてのユーザの表示名（例えば「Ａｌｉｃｄ」）のリストを含む選択画面（図示省略）を表示部１４０に表示し、該選択画面を介して表示名の指定指示を取得しても良い。この場合には、Ｓ１０５にて、複合機１００は、指定された表示名（例えば「Ａｌｉｃｅ」）に対応する秘密鍵を取得する。また、このとき表示される選択画面は、ユーザの表示名のリストに代えて、証明書のファイル名のリストを含んでいても良い。

【００８０】

（４）上記各実施例では、証明書ＣＴ１～ＣＴ３を格納する外部装置と、署名付ＰＤＦファイルＳＰＦを格納する装置とは、ともに計算機２００である。これに代えて、証明書ＣＴ１～ＣＴ３を格納する外部装置と、署名付ＰＤＦファイルＳＰＦを格納する装置とは、別の装置であっても良い。例えば、証明書ＣＴ１～ＣＴ３を格納する外部装置と、署名付ＰＤＦファイルＳＰＦを格納する装置と、のうちの一方は、ＵＳＢインタフェースを介して複合機１００に接続されたＵＳＢメモリであり、他方は、計算機２００であっても良い。

【００８１】

（５）上記各実施例では、複合機１００は、複数個の秘密鍵ＳＫ１～ＳＫ３と、対応する複数個の証明書ＣＴ１～ＣＴ３と、を管理している。これに代えて、複合機１００は、１個の秘密鍵と、対応する１個の証明書と、のみを管理していても良い。この場合には、例えば、図２（Ｃ）の管理テーブルＫＭＴは、無くても良い。

【００８２】

（６）上記各実施例では、複合機１００は、計算機２００から取得された証明書が真正で

あるか否かを判断する処理（例えば、図３のＳ１１５～Ｓ１４０）を実行しているが、これらの処理の全部または一部は省略されても良い。例えば、図３のＳ１１５～Ｓ１４０、および、Ｓ１６０は、省略されても良い。また、図３のＳ１１５、Ｓ１２０のみが省略されても良い。また、図３のＳ１２５～Ｓ１４０のみが省略されても良い。

【００８３】

（７）図３のＳ１１５では、秘密鍵ＳＫ１に含まれる公開鍵ＰＫ１の「modulus」の値と、証明書ＣＴ１に含まれる公開鍵ＰＫ１の「modulus」の値と、を比較している。これに代えて、あるいは、これと共に、例えば、秘密鍵ＳＫ１に含まれる公開鍵ＰＫ１の「publicExponent」の値と、証明書ＣＴ１に含まれる公開鍵ＰＫ１の「publicExponent」の値と、を比較しても良い。

【００８４】

（８）上記各実施例では、各秘密鍵とユーザとは、一対一で対応しているが、これに限られない。例えば、１個の秘密鍵が複数人のユーザと対応していても良い。また、一人のユーザが複数個の秘密鍵と対応していても良い。例えば、ログイン中のユーザに複数個の秘密鍵が対応している場合には、複合機１００は、図３のＳ１０５にて、当該複数個の秘密鍵（または対応する証明書）のリストを含む選択画面を表示して、ユーザの選択指示を取得し、ユーザの選択指示に従って１個の秘密鍵を取得すれば良い。

【００８５】

（９）上記各実施例では、署名付ファイル生成処理を行う情報処理装置は、複合機１００であるが、単体のスキャナであっても良い。また、情報処理装置は、パーソナルコンピュータやスマートフォンなどの端末装置であっても良い。この場合には、例えば、端末装置は、自身の不揮発性記憶装置に予め保存されたファイルに対して署名を行って、署名付ファイルを生成しても良い。あるいは、端末装置は、複合機やスキャナからスキャンデータＳＤを取得して、該スキャンデータＳＤを含むファイルに対して署名を行って、署名付ファイルを生成しても良い。また、情報処理装置は、ファイルサーバであっても良い。この場合には、ファイルサーバは、例えば、所定のフォルダに格納されたファイルに対して署名を行って、署名付ファイルを生成しても良い。この場合には、ファイルサーバは、署名付ファイルを、自身のハードディスクに格納し、クライアントからの要求に応じて、該クライアントに対して署名付ファイルを出力する。この場合に、ファイルサーバは、ネットワークを介して互いに通信可能な複数個の装置（例えば、コンピュータ）を含む、いわゆるクラウドサーバであっても良い。

【００８６】

（１０）上記各実施例において、ハードウェアによって実現されていた構成の一部をソフトウェアに置き換えるようにしてもよく、逆に、ソフトウェアによって実現されていた構成の一部あるいは全部をハードウェアに置き換えるようにしてもよい。

【００８７】

（１１）本発明の機能の一部または全部がコンピュータプログラムで実現される場合には、そのプログラムは、コンピュータ読み取り可能な記録媒体（例えば、一時的ではない記録媒体）に格納された形で提供することができる。プログラムは、提供時と同一または異なる記録媒体（コンピュータ読み取り可能な記録媒体）に格納された状態で、使用され得る。「コンピュータ読み取り可能な記録媒体」は、メモリーカードやＣＤ－ＲＯＭのような携帯型の記録媒体に限らず、各種ＲＯＭ等のコンピュータ内の内部記憶装置や、ハードディスクドライブ等のコンピュータに接続されている外部記憶装置も含み得る。

【００８８】

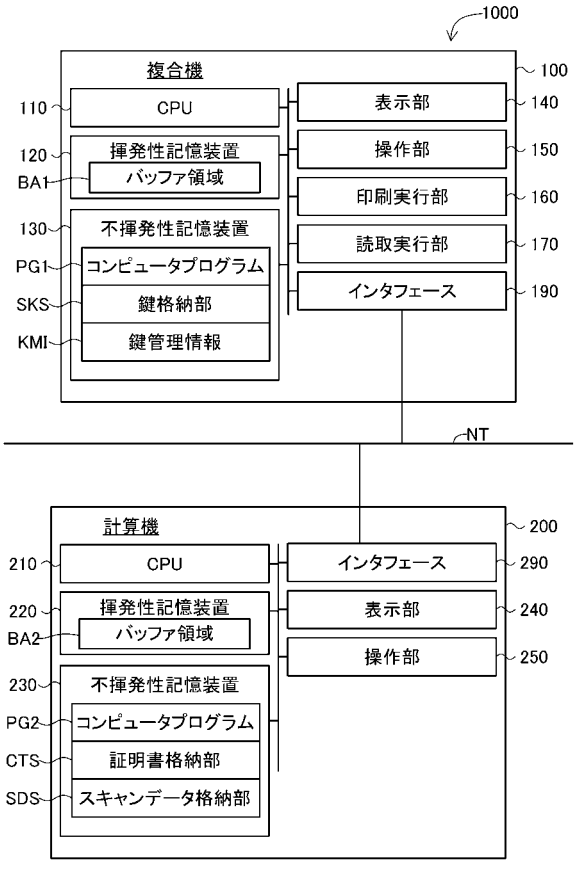
以上、実施例、変形例に基づき本発明について説明してきたが、上記した発明の実施の形態は、本発明の理解を容易にするためのものであり、本発明を限定するものではない。本発明は、その趣旨並びに特許請求の範囲を逸脱することなく、変更、改良され得ると共に、本発明にはその等価物が含まれる。

【符号の説明】

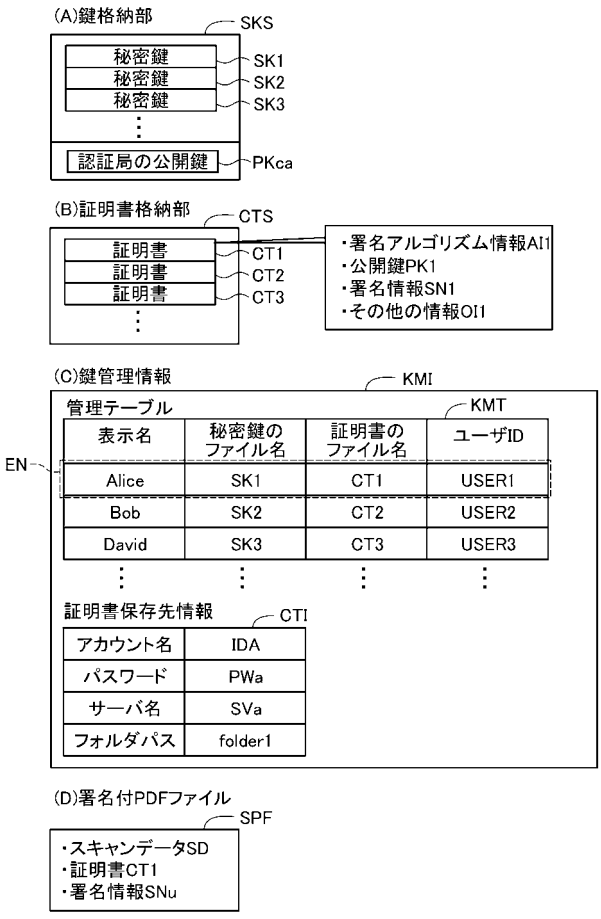
【００８９】

１１０…ＣＰＵ、１２０…揮発性記憶装置、１３０…不揮発性記憶装置、１４０…表示部、１５０…操作部、１６０…印刷実行部、１７０…読取実行部、１９０…インタフェース、２００…計算機、２１０…ＣＰＵ、２２０…揮発性記憶装置、２３０…不揮発性記憶装置、２４０…表示部、２５０…操作部、２９０…インタフェース、１０００…システム、ＮＴ…ローカルエリアネットワーク、ＰＧ１…コンピュータプログラム、ＰＧ２…コンピュータプログラム、ＫＭＩ…鍵管理情報、ＳＤＳ…スキャンデータ格納部、ＣＴＩ…証明書保存先情報、ＳＫＳ…鍵格納部、ＫＭＴ…管理テーブル、ＣＴＳ…証明書格納部

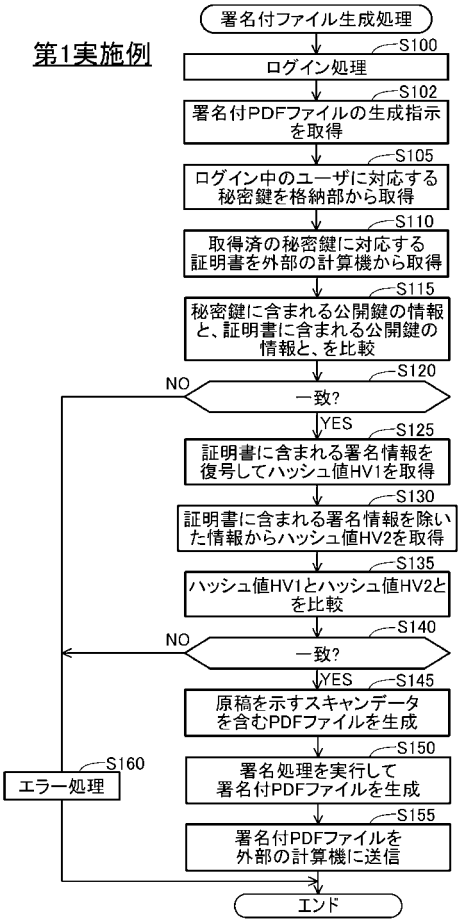
【図１】



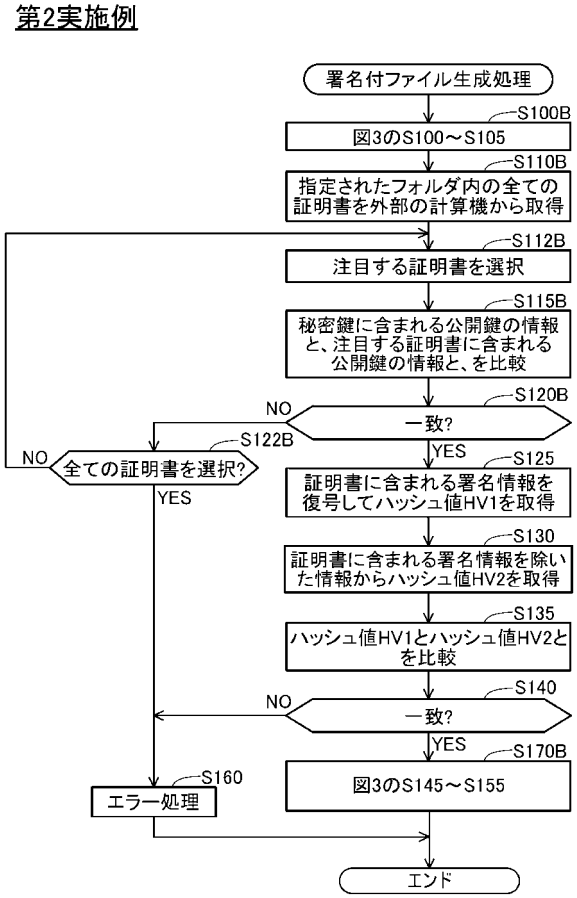
【図２】



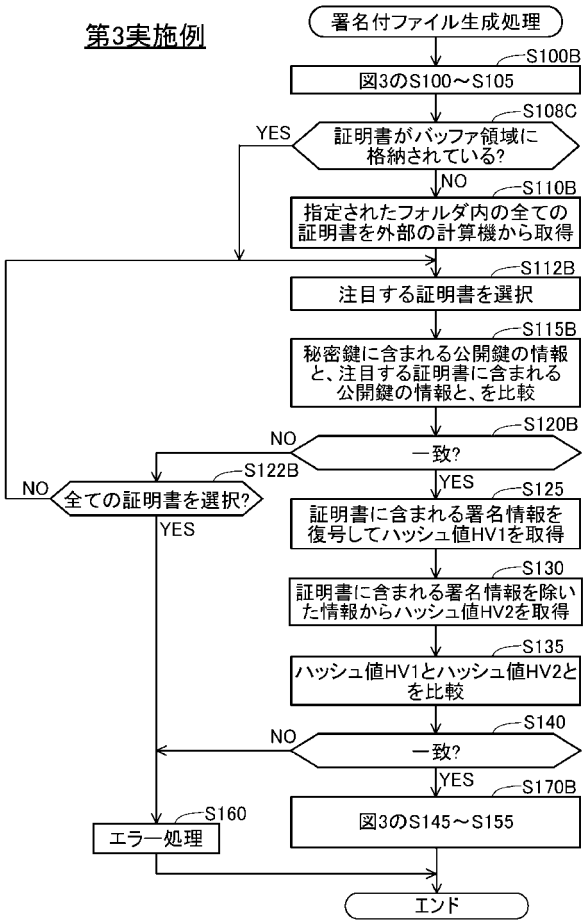
【図３】


第1実施例
署名付ファイル生成処理
S100
ログイン処理
S102
署名付PDFファイルの生成指示を取得
S105
ログイン中のユーザに対応する秘密鍵を格納部から取得
S110
取得済の秘密鍵に対応する証明書を外部の計算機から取得
S115
秘密鍵に含まれる公開鍵の情報と、証明書に含まれる公開鍵の情報と、を比較
S120
一致?
NO
YES
S125
証明書に含まれる署名情報を復号してハッシュ値HV1を取得
S130
証明書に含まれる署名情報を除いた情報からハッシュ値HV2を取得
S135
ハッシュ値HV1とハッシュ値HV2とを比較
S140
一致?
NO
YES
S145
原稿を示すスキャンデータを含むPDFファイルを生成
S150
署名処理を実行して署名付PDFファイルを生成
S155
署名付PDFファイルを外部の計算機に送信
S160
エラー処理
エンド

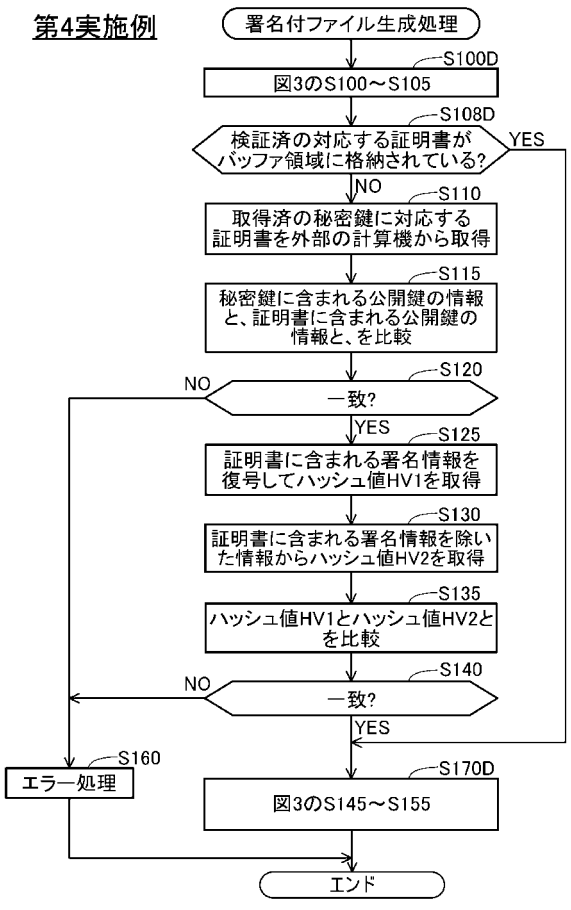
【図４】


第2実施例
署名付ファイル生成処理
S100B
図3のS100～S105
S110B
指定されたフォルダ内の全ての証明書を外部の計算機から取得
S112B
注目する証明書を選択
S115B
秘密鍵に含まれる公開鍵の情報と、注目する証明書に含まれる公開鍵の情報と、を比較
S120B
一致?
NO
YES
S122B
全ての証明書を選択?
NO
YES
S125
証明書に含まれる署名情報を復号してハッシュ値HV1を取得
S130
証明書に含まれる署名情報を除いた情報からハッシュ値HV2を取得
S135
ハッシュ値HV1とハッシュ値HV2とを比較
S140
一致?
NO
YES
S160
エラー処理
S170B
図3のS145～S155
エンド

【図５】


第3実施例
署名付ファイル生成処理
S100B
図3のS100～S105
S108C
証明書がバッファ領域に格納されている?
YES
NO
S110B
指定されたフォルダ内の全ての証明書を外部の計算機から取得
S112B
注目する証明書を選択
S115B
秘密鍵に含まれる公開鍵の情報と、注目する証明書に含まれる公開鍵の情報と、を比較
S120B
一致?
NO
YES
S122B
全ての証明書を選択?
NO
YES
S125
証明書に含まれる署名情報を復号してハッシュ値HV1を取得
S130
証明書に含まれる署名情報を除いた情報からハッシュ値HV2を取得
S135
ハッシュ値HV1とハッシュ値HV2とを比較
S140
一致?
NO
YES
S160
エラー処理
S170B
図3のS145～S155
エンド

【図６】


第4実施例
署名付ファイル生成処理
S100D
図3のS100～S105
S108D
検証済の対応する証明書がバッファ領域に格納されている?
YES
NO
S110
取得済の秘密鍵に対応する証明書を外部の計算機から取得
S115
秘密鍵に含まれる公開鍵の情報と、証明書に含まれる公開鍵の情報と、を比較
S120
一致?
NO
YES
S125
証明書に含まれる署名情報を復号してハッシュ値HV1を取得
S130
証明書に含まれる署名情報を除いた情報からハッシュ値HV2を取得
S135
ハッシュ値HV1とハッシュ値HV2とを比較
S140
一致?
NO
YES
S160
エラー処理
S170D
図3のS145～S155
エンド