

明 細 書

発明の名称：

個人データアプリケーションおよび個人データアプリケーション制御方法 技術分野

[0001] 本発明は、コンピュータシステムで稼働するアプリケーションに関する。
特に、正常に開いて使用を開始し、正常にデータを編集し、正常に使用を終了して閉じることを確保せしめたアプリケーションに関する。

また、本発明は、アプリケーションのコンピュータシステムの適用例として、利用者個人の行政上の記録情報または資格情報の内容を示す行政関連ファイルがある。例えば、電子カルテファイル、電子保険証ファイル、電子運転免許証ファイル、電子住民票ファイル、電子印鑑登録証ファイルなどがあり得る。

背景技術

[0002] 従来の紙ベースの利用者個人の行政上の記録情報または資格情報の内容を示す行政関連の公的物、例えば、保険証、運転免許証、住民票、印鑑登録証などは利用者個人が保持しており、必要に応じて行政機関関係者や医療関係者に対して提示し、行政上の取り扱いや民間サービスの取り扱いに利用していた。

[0003] 近年は、クラウドシステムが普及しつつある。クラウドシステム上に様々なデータが管理保管されるようになってきている。やがて近いうちに利用者個人の行政上の記録情報または資格情報の内容を示す行政関連の証書類も電子ファイル化され、行政関連の証書類のデータを記録した個人データアプリケーションファイルとしてクラウドシステム上に管理保管されることが想定される。

[0004] それら行政関連の証書類データなどの個人データアプリケーションファイルをクラウドシステム上に管理保管する際に問題となるのは、セキュリティと利用時の運用方法である。

セキュリティに関しては、一般のクラウドシステムが提供するセキュリティに加え、個人情報保護や改ざんを防止するため、さらに個人データアプリケーションファイルの閲覧、データ編集などに伴うセキュリティ付与も考慮する必要がある。

[0005] コンピュータシステムにおいて、様々なアプリケーションが稼働しており、様々なセキュリティ対策が行われている。セキュリティ対策の意味合いは広いが、例えば、アプリケーションで利用するアプリケーションファイルにアクセスする正当権限者のみがアプリケーションファイルが利用できるように、アプリケーションファイルにアクセスして開く際にパスワードの入力を求める対策は広く採用されている。セキュリティレベルによるが、単純にキーボードからパスワードを入力させるものや、パスワードとともに携帯しているICカードからID情報を入力させるものや、パスワードと指紋や静脈パターンなどの生体情報を入力させるものなどがある。また、一人の操作だけでは不十分とし、複数の権限者のパスワードやID情報等が揃ってようやくアプリケーションファイルを開くことができるものもある。このように、アプリケーションファイルを開いて操作可能状態とするためには高度なセキュリティが設定されているアプリケーションはある。

[0006] アプリケーションが立ち上がってアプリケーションファイルが操作可能状態となれば、利用者はアプリケーションを使用してアプリケーションファイルを編集することができるが、アプリケーションの操作中、さらに、特別な機能を使用したりする際には、別途、個別にパスワードやID情報などが求められる場合もあり得る。

[0007] このように、アプリケーションファイルを開いたり、特別な機能を使用したりする場合には、セキュリティが設定されていることがあり得る。しかし、逆に、アプリケーションの利用が終了してアプリケーションファイルを閉じる際や、特別な機能の使用を終了する際には、終了すること自体には特段何らのパスワードやID情報の入力等を求められることはなく、セキュリティ設定がされているものはない。ほとんどのものは“終了”や“閉じる”と

いうコマンドの入力やボタン押下で単純に終了できる。

[0008] 図17は、一般的なアプリケーションを立ち上げてアプリケーションファイルを開き、その後、終了して閉じる操作を簡単に説明する図である。一例であり、アプリケーションファイルを開いたり閉じたりする典型的な操作である。

図17(a)に示すように、アプリケーション10は、コンピュータシステム上にインストールされており、利用者がアプリケーション10を使用しようとする際には、コンピュータシステムのモニタ上に表示されているアプリケーション10のアイコンをマウスなどのポインティングデバイスなどで選択し、ダブルクリックなどの操作で起動をかければアプリケーション10が起動する。

[0009] また、アプリケーション10で編集可能な各々のアプリケーションファイル20a, 20b, 20cなどもコンピュータシステム上にインストールされており、各々のアイコンがコンピュータシステムのモニタ上に表示されている。利用者が編集しようとするアプリケーションファイル20のアイコンをマウスなどのポインティングデバイスなどで選択し、ダブルクリックなどの操作で起動をかければ、アプリケーション10が立ち上がるとともにアプリケーションファイル20が読み込まれてアプリケーション10を用いて編集可能な状態となり、データの内容がモニタ上に表示される。

[0010] ここで、セキュリティが設定されているアプリケーションファイル20であれば、図17(b)の上段に示すように、使用権限を確認すべくパスワードの入力カラムがポップアップされる。このように、アプリケーションファイル20の編集などアプリケーション10の使用を開始する前にはパスワードの入力が求められる運用がある。なお、アプリケーション10によってはパスワードに加えてICカードからのID情報の入力や生体情報の入力を求めるものもある。

図17(b)の上段に示すように、キーボードや他の入力デバイスなどを介して、アプリケーションファイル20を正常に開いて使用可能とするため

に求められたパスワードやコード情報などを入力し、その認証に成功して設定されたセキュリティレベルを満たした場合には、アプリケーションファイル20がオープンして使用可能となる。

- [0011] 次に、図17(b)の下段に示すように、アプリケーションファイル20の所望の編集が終了すれば、モニタ上に表示されているアプリケーション10の入力画面の“終了”や“閉じる”という操作メニューやボタンをマウスなどのポインティングデバイスなどで選択してクリックなどの操作で指定すれば、アプリケーション10が単純に終了し、アプリケーションファイル20が閉じられる。

ほとんどのアプリケーション10では、アプリケーションファイル20を閉じる際には特別なパスワードやID情報の入力等を求められることはなく、ほとんどのアプリケーション10は単純に終了してアプリケーションファイル20を閉じることができる。

- [0012] つまり、アプリケーションファイル20のアクセスに際しては、使用しようとする者が正当な使用権限がある者か否かを確認するため、様々なセキュリティレベルに基づく情報の入力を求めるが、使用開始時に一度、使用権限の認証が成功すれば、その後はその使用権限者がその権限のもと正しく使用されることが前提であり、終了もその権限のもと正しく終了することが前提となっており、アプリケーションファイル20の編集終了後に閉じる際にはパスワードの入力など特段のセキュリティ設定を行っていない。もっとも操作エラーなどで操作不能に陥ったり、システムエラーが発生したりなどの不具合によって正常ではない形で強制終了したりすることはあり得るが、操作エラーやシステムエラーなどがなく、操作自体が正常であれば、アプリケーション10は単純に終了してアプリケーションファイル20を閉じることができる。

- [0013] 近年、スタンドアロン型で稼働するコンピュータシステムのみならず、ネットワークなどで接続され、複数のコンピュータシステムが連動して業務を実行するものが増えてきている。しかし、アプリケーション10を立ち上げ

てアプリケーションファイル20を開き、その後、終了して閉じるというアプリケーション10の利用のルーチンは、ネットワーク環境でも同様であり、ネットワークにログインする際にはパスワードやIDコードの入力などセキュリティが求められ、ネットワークを介してアプリケーションファイル20にアクセスする際にもパスワードやIDコードの入力などセキュリティが求められるが、アプリケーションファイル20を閉じる際には、何ら特段のパスワードやID情報の入力が必要ではなく、単に終了して閉じることができる。

[0014] ここで、利用者個人の行政関連の証書類も電子ファイル化した個人データアプリケーションファイルについても上記と同様に考えることができる。

図17で説明したアプリケーションの操作と合わせて考えると、一般には、行政関連の証書類に関する個人データアプリケーションファイルに対してパスワードが設定されており、個人データアプリケーションを使用して利用者の利用者個人の行政サービスアプリケーションファイルを閲覧し、データ編集するためにファイルをオープンする際には、要求されるパスワードを入力してファイルをオープンし、個人データアプリケーションファイルを自由に編集することが想定されるが、個人データアプリケーションに対する編集操作が終了すれば、単純に閉じるボタンの押下などで単純に閉じる操作が想定される。

[0015] 特許文献1：特開2006-277193号公報

発明の開示

発明が解決しようとする課題

[0016] 行政関連の証書類は、いわば身分証のように利用者の行政上の立場や財産や資格などを示すものであり、その真正性が担保され、悪意者による改ざん不能であることが好ましい。その行政関連の証書類を電子データ化した個人データアプリケーションファイルのセキュリティは各段に高く設定される必要がある。

上記技術に見たように、一般のアプリケーションファイルを開く際には様

々な高いセキュリティが設定されている例は存在する。しかし、データ編集が完了し、アプリケーションファイルを閉じる際には、特段のセキュリティが設定されている例はない。

[0017] 行政関連の証書類を電子データ化した個人データアプリケーションファイルを想定しても同様であり、個人データアプリケーションファイルを開いた使用者が認証をパスした正当権限を持つ者であれば、個人データアプリケーションファイルの編集作業が一通り完了すれば、そのまま個人データアプリケーションファイルを閉じる操作を行って個人データアプリケーションを終了させ、特段のパスワードの入力などのセキュリティ対策を講じられていない。

[0018] しかし、個人データアプリケーションファイルに対して、行政関係者や医療関係者などが編集を終了して個人データアプリケーションファイルを閉じる際に、入力内容や操作内容を反映した個人データアプリケーションファイルの作成データをそのまま確定させて良いかどうかを確認したいという要求がある場合があり得る。

個人データアプリケーションファイルの編集集中に入力した入力内容や操作内容が、編集者の誤解や過失による誤った内容であったり、編集者の不正により故意に事実とは異なる内容であったりするケースもあり得る。このように事実とは異なる誤った内容によりそのまま個人データアプリケーションファイルのデータの編集結果として格納され、個人データとして確定されてしまうことは問題である。

[0019] そこで、本発明では、個人データアプリケーションファイルを開く際のみならず、個人データアプリケーションファイルを終了して閉じる際にも、入力内容や操作内容が正しいことを確認せしめるセキュリティ設定を施し、誤解や過失による誤りに基づく過誤入力や、事実とは異なる不正入力などを効果的に低減せしめた個人データアプリケーションを提供すること、およびその個人データアプリケーションファイルの制御方法を提供することを目的とする。

課題を解決するための手段

[0020] 上記目的を達成するため、本発明の個人データアプリケーションは、個人データを取り扱う個人データアプリケーションであって、前記個人データアプリケーションで利用される各々の個人データアプリケーションファイルであって、前記個人データアプリケーションで前記個人データアプリケーションファイルを開くための“オープン暗証コード”と、前記個人データアプリケーションで開いた前記個人データアプリケーションファイルを正常終了して閉じるための“クローズ暗証コード”が設定された個人データアプリケーションファイルと、“オープン暗証コード”の入力を受けて前記個人データアプリケーションファイルを開く個人データアプリケーションファイル開錠機能と、開かれた前記個人データアプリケーションファイルに対して、他のコンピュータリソースを経由した他者によるデータ編集を受け付ける個人データアプリケーションファイル編集機能と、“クローズ暗証コード”の入力を受けて、前記個人データアプリケーションファイルに対する前記個人データアプリケーションファイル編集機能によるデータ編集内容を確定し、正常終了して閉じる個人データアプリケーションファイル閉錠機能を備えたことを特徴とするものである。

[0021] 個人データアプリケーションファイルを開くための“オープン暗証コード”と“クローズ暗証コード”を備えることにより、個人データアプリケーションファイル開錠機能を実行する際に“オープン暗証コード”が求められるだけでなく、個人データアプリケーションファイル閉錠機能を実行する際に“クローズ暗証コード”が求められ、個人データアプリケーションファイル編集機能の実行の際の他者によるデータ編集を確認することができ、利用者が内容を確認したもののみが確定して正常終了することができる。

上記の“オープン暗証コード”、“クローズ暗証コード”として、様々なものが設定できる。

例えば、数字からなるPINコード、さらに文字情報も加えたパスワード、バーコードなどの1次元コード、QRコードなどの二次元コード、さらに

指紋パターンや静脈パターンや虹彩パターンや声紋パターンや顔画像など利用者の生体情報などがある。利用者により入力された暗証コードと利用者端末 200A の端末 ID 番号とを組み合わせるなど一定のアルゴリズムで計算したコードを暗証コードとして送信するものでも良い。

[0022] 次に、上記構成において、個人データアプリケーションファイル編集機能を利用者以外の第三者が使用する場合、さらにセキュリティを高めるため、個人データアプリケーションファイルに、他者による他のコンピュータリソースを経由した個人データアプリケーションファイルへのデータ編集を許可するための“編集開始暗証コード”を設定する。そして、個人データアプリケーションファイル編集機能が、他者に対して個人データアプリケーションファイルへのデータ編集の開始にあたり“編集開始暗証コード”の入力を求めるものとする。

[0023] さらに、上記構成において、さらにセキュリティを高めるため、個人データアプリケーションファイルに、上記した“編集開始暗証コード”に加え、他のコンピュータリソースを経由した前記個人データアプリケーションファイルの編集を終了するための“編集終了暗証コード”を設定する構成もあり得る。そして、個人データアプリケーションファイル編集機能が、他者に対して個人データアプリケーションファイルへのデータ編集の開始にあたり“編集開始暗証コード”の入力を求めるとともに、データ編集の終了にあたり“編集終了暗証コード”の入力を求めるものとすることも可能である。

上記の“編集開始暗証コード”、“編集終了暗証コード”として、様々なものが設定できる。例えば、数字からなる PIN コード、さらに文字情報も加えたパスワード、バーコードなどの 1 次元コード、QR コードなどの二次元コード、さらに指紋パターンや静脈パターンや虹彩パターンや声紋パターンや顔画像など編集者の生体情報などがある。また、編集者が保持携帯するカードに格納された ID 情報でも良い。

[0024] 次に、システム構成として、上記した個人データアプリケーションファイルはネットワーク上のサーバーに格納されて管理されているものでも良く、

個人データアプリケーションが個人データの所有者である個人が保持するスマートフォンにインストールされているかＡＳＰにより利用可能な形態となっている構成がある。他者による他のコンピュータリソースはサーバーにアクセス可能なものとする構成がある。

また、他のシステム構成として、上記した個人データアプリケーションファイルはネットワーク上のクラウドシステムに格納されて管理されているもので良く、個人データアプリケーションが個人データの所有者である個人が保持するスマートフォンにインストールされているかＡＳＰにより利用可能な形態となっている構成がある。他者による他のコンピュータリソースはクラウドシステムにアクセス可能なものとする構成がある。

[0025] 次に、個人データアプリケーションで利用される各々の個人データアプリケーションファイルが個人単位に個人フォルダにまとめられた構成とすることができる。

このように個人フォルダを用いる場合、個人データアプリケーションで利用される各々の個人フォルダに、個人データアプリケーションで個人フォルダを開くための“個人フォルダオープン暗証コード”と、個人データアプリケーションで開いた個人フォルダを閉じるための“個人フォルダクローズ暗証コード”が設定することができる。

[0026] 本発明の個人データアプリケーションは、様々なアプリケーションに適用することができる。

例えば、クラウド電子身分証、資格証に適用することができる。

個人データアプリケーションファイルが、利用者個人の行政上の記録情報または資格情報の内容を示す行政関連電子ファイルであり、個人データアプリケーションが、利用者個人の行政サービスアプリケーションであり、他者が行政関連電子ファイルのデータを編集する行政関係者であり、他のコンピュータリソースが、行政関係者が用いる行政関連電子ファイル管理システムとして適用することができる。

[0027] また、クラウド電子カルテに適用することができる。

個人データアプリケーションファイルが、患者個人の電子カルテファイルであり、個人データアプリケーションが、患者個人の電子カルテサービスアプリケーションであり、他者が医療関係者であり、他のコンピュータリソースが、医療関係者が用いる医療機関利用システムとして適用することができる。

[0028] また、クラウド電子お薬手帳に適用することができる。

個人データアプリケーションファイルが、患者個人の電子お薬手帳ファイルであり、個人データアプリケーションが、患者個人の電子お薬手帳ファイルサービスアプリケーションであり、他者が薬剤師であり、他のコンピュータリソースが、薬剤師が用いる調剤薬局利用システムとして適用できる。

[0029] また、クラウド電子保険証に適用することができる。

個人データアプリケーションファイルが、被保険者個人の電子保険証ファイルであり、個人データアプリケーションが、被保険者個人の電子保険証サービスアプリケーションであり、他者が医療関係者であり、他のコンピュータリソースが、医療関係者が用いる医療機関利用システムとして適用することができる。

[0030] また、クラウド電子運転免許証に適用することができる。

個人データアプリケーションファイルが、運転者個人の電子運転免許証ファイルであり、個人データアプリケーションが、運転者個人の運転免許証サービスアプリケーションであり、他者が電子運転免許証のデータを編集する行政関係者であり、他のコンピュータリソースが、行政関係者が用いる電子運転免許証管理システムとして適用することができる。

また、電子パスポートに適用することができる。

個人データアプリケーションファイルが、個人の電子パスポートファイルであり、個人データアプリケーションが、個人の出入国管理サービスアプリケーションであり、他者が電子パスポートのデータを編集する出入国管理を行う行政関係者であり、他のコンピュータリソースが、出入国管理の行政関係者が用いる電子パスポート管理システムとして適用することができる。

[0031] 次に、本発明にかかる個人データアプリケーションファイルのオープンクローズ制御方法は、個人データを取り扱う個人データアプリケーションの制御方法であって、前記個人データアプリケーションで利用される各々の個人データアプリケーションファイルに対して、前記個人データアプリケーションで前記個人データアプリケーションファイルを開くためのオープン暗証コードと、前記個人データアプリケーションで開いた前記個人データアプリケーションファイルを正常終了して閉じるためのクローズ暗証コードを設定し、前記オープン暗証コードの入力を受けて前記個人データアプリケーションファイルを開く個人データアプリケーションファイル開錠処理と、開かれた前記個人データアプリケーションファイルに対して、他のコンピュータリソースを経由した他者によるデータ編集を受け付ける個人データアプリケーションファイル編集処理と、前記クローズ暗証コードの入力を受けて、前記個人データアプリケーションファイルに対する前記個人データアプリケーションファイル編集処理によるデータ編集内容を確定し、正常終了して閉じる個人データアプリケーションファイル閉錠処理を行うことを特徴とする個人データアプリケーションファイルの制御方法である。

図面の簡単な説明

[0032] [図1]実施例1にかかる個人データアプリケーション110-1、210-1、個人データアプリケーションファイル310-1の構成を簡単に示した図である。

[図2]実施例1にかかる本発明の個人データアプリケーション110-1、210-1、個人データアプリケーション310-1の操作の概略を説明する図（その1）である。

[図3]実施例1にかかる本発明の個人データアプリケーション110-1、210-1、個人データアプリケーション310-1の操作の概略を説明する図（その2）である。

[図4]実施例2にかかる個人データアプリケーション110-2、210-2、個人データアプリケーションファイル310-2の構成を簡単に示した図

である。

[図5]実施例2にかかる本発明の個人データアプリケーション110-2、210-2、個人データアプリケーション310-2の操作の概略を説明する図（その1）である。

[図6]実施例2にかかる本発明の個人データアプリケーション110-2、210-2、個人データアプリケーション310-2の操作の概略を説明する図（その2）である。

[図7]実施例2にかかる本発明の個人データアプリケーション110-2、210-2、個人データアプリケーション310-2の操作の概略を説明する図（その3）である。

[図8]実施例3にかかる個人データアプリケーション110-3、210-3、個人データアプリケーションファイル310-3、個人フォルダ320-3の構成を簡単に示した図である。

[図9]実施例3にかかる本発明の個人データアプリケーション110-3、210-3、個人データアプリケーション310-3の操作の概略を説明する図（その1）である。

[図10]実施例3にかかる本発明の個人データアプリケーション110-3、210-3、個人データアプリケーション310-3の操作の概略を説明する図（その2）である。

[図11]実施例3にかかる本発明の個人データアプリケーション110-3、210-3、個人データアプリケーション310-3の操作の概略を説明する図（その3）である。

[図12]実施例3にかかる本発明の個人データアプリケーション110-3、210-3、個人データアプリケーション310-3の操作の概略を説明する図（その4）である。

[図13]サーバー300内の個人フォルダ320-3、個人データアプリケーションファイル310-3の例を模式的に示した図である。

[図14]実施例4の個人データアプリケーション110、210、個人データ

アプリケーションファイル310の構成を簡単に示した図である。

[図15]実施例4にかかる運用例を簡単に示す図（その1）である。

[図16]実施例4にかかる運用例を簡単に示す図（その2）である。

[図17]一般的なアプリケーションを立ち上げてアプリケーションファイルを開き、その後、終了して閉じる操作を簡単に説明する図である。

発明を実施するための最良の形態

[0033] 以下、本発明を実施するための最良の形態について実施例により具体的に説明する。なお、本発明はこれらの実施例に限定されるものではない。

以下、実施例1、実施例2、実施例3、実施例4として、本発明の個人データアプリケーションおよびその操作の概略を説明する。なお、具体的な個人データアプリケーション例として、クラウド電子カルテを例に説明する。

実施例1は、個人データアプリケーションファイルにオープン暗証コードとクローズ暗証コードが設定されており、個人データアプリケーションが、アプリケーションファイル開錠機能と、アプリケーションファイル編集機能と、アプリケーションファイル閉錠機能を備えている例である。

実施例2は、個人データアプリケーションファイルに、オープン暗証コードとクローズ暗証コードに加え、編集開始暗証コードと編集終了暗証コードが設定されており、個人データアプリケーションが、アプリケーションファイル開錠機能と、アプリケーションファイル編集機能と、アプリケーションファイル閉錠機能に加え、アプリケーションファイル編集機能に関する編集開始暗証コードの入力機能および編集終了暗証コードの入力機能を備えている例である。

実施例3は、個人データアプリケーションファイルが個人単位に個人フォルダにまとめられており、個人フォルダについて個人フォルダオープン暗証コードと、個人フォルダクローズ暗証コードが設定されており、個人データアプリケーションファイルにオープン暗証コード、クローズ暗証コード、編集開始暗証コード、編集終了暗証コードが設定されており、個人データアプリケーションが、個人フォルダ開錠機能、アプリケーションファイル開錠機

能、編集開始暗証コードの入力機能、アプリケーションファイル編集機能、編集終了暗証コードの入力機能、アプリケーションファイル閉錠機能、個人フォルダ閉錠機能を備えている例である。

実施例4は、本発明の個人データアプリケーションを搭載した本発明の業務システム例としてクラウド電子保険証、クラウド電子カルテ、クラウド電子運転免許証を取り扱うサービス提供支援システムを説明するものである。

実施例 1

[0034] 実施例1にかかる本発明の個人データアプリケーションについて説明する。

図1は、実施例1にかかる個人データアプリケーション110-1、210-1、個人データアプリケーションファイル310-1の構成を簡単に示した図である。

ネットワーク上には、サーバー300があり、個人データアプリケーションファイル310-1が記憶装置に格納されており、個人データアプリケーション110-1、個人データアプリケーション210-1からアクセス可能になっている。クラウドシステムとして利用される場合もあり得る。

個人データアプリケーションファイル310-1は、当該個人データアプリケーション110-1で取り扱われ、編集・操作され得るデータのまとまりであるデータセットである。

この実施例1では、個人データアプリケーションファイル310-1は電子カルテファイルであり、利用者個人の診察記録、治療記録、レセプトに関する諸データなど医療機関において取り扱われる一般的なカルテに必要な情報が格納されたファイルである。例えば、クラウドシステム上に格納され管理されているものとする。

サーバー300に格納されている個人データアプリケーションファイル310の規模であるが、本発明では限定されない。運用によって多様な規模があり得る。例えば、個人データアプリケーションファイル310が1つのクリニックだけで利用されるものであれば、そのクリニックを利用する患者の

規模となる。例えば、国民皆保険に加入する被保険者のカルテが電子カルテファイルとして共通仕様に制定された場合、国民皆保険に加入する被保険者の総数に相当する規模となる。このように膨大な電子カルテファイルを取り扱う場合、サーバー300が大規模なシステムとなることが想定できる。

[0035] 実施例1では、個人データアプリケーションファイル310-1には、個人データアプリケーションファイル本体311と、オープン暗証コード312とクローズ暗証コード313が設定されている。

“オープン暗証コード”は個人データアプリケーション110-1により個人データアプリケーションファイル310-1を開くための暗証コードである。

“クローズ暗証コード”は個人データアプリケーション110-1で開いている個人データアプリケーションファイル310-1を正常終了して閉じるための暗証コードである。

なお、オープン暗証コード312、クローズ暗証コード313は、例えば、数字からなるPINコード、さらに文字情報も加えたパスワード、バーコードなどの1次元コード、QRコードなどの二次元コード、さらに指紋パターンや静脈パターンや虹彩パターンや声紋パターンや顔画像など利用者の生体情報などがある。利用者により入力された暗証コードと利用者端末200Aの端末ID番号とを組み合わせるなど一定のアルゴリズムで計算したコードを暗証コードとして送信するものでも良い。

[0036] 次に、利用者が保持する利用者端末100は、スマートフォンなど利用者が使用可能なコンピュータリソースであれば良いが、この例ではスマートフォンとなっている。利用者端末100には、個人データアプリケーション110-1がダウンロードされているか、またはASPで利用可能となっている。

図1ではスマートフォン上にダウンロードされたアプリケーションとして描いているが、ASPで利用可能な場合、アプリケーション本体はネットワーク上に存在している。

本発明の個人データアプリケーション 110-1 はソフトウェアであれば良く、特に用途が限定されるわけではない。

この実施例 1 では、個人データアプリケーション 110-1 は、電子カルテファイルを閲覧したり操作したりする電子カルテアプリケーションを例として説明する。

[0037] 実施例 1 では、当該個人データアプリケーション 110-1 は、アプリケーション本体機能 111、入力手段 112、アプリケーションファイル開錠機能 114 と、アプリケーションファイル閉錠機能 115、アプリケーションファイルアクセス情報通知手段 113 を備えている例となっている。

[0038] アプリケーション本体機能 111 は、個人データアプリケーション 110-1 によって多種多様であり、個人データ管理に必要な処理を実行するための諸機能が装備されているものとする。なお、データ入力機能、データ出力機能、データ格納機能などの汎用的な機能も含まれているものとする。

この実施例 1 では、電子カルテを取り扱う上で必要とされるアプリケーションの諸機能が装備されているものとする。

[0039] 入力手段 112 は、システムが装備しているデータ入力デバイスである。

入力手段 112 は、キーボード、タッチパネルなどの一般的な入力デバイスのほか、IC カードリーダー、生体情報読み取りデバイスなど、多様な入力デバイスが利用可能である。システムの運用に応じて、装備する入力デバイスを取り付ければ良い。

[0040] アプリケーションファイルアクセス情報通知手段 113 は、他者が個人データアプリケーションファイル 310-1 にアクセスできるよう、利用者が、他者のコンピュータリソースに対して個人データアプリケーションファイル 310-1 が格納されているネットワーク上のサーバーのアドレス情報を通知する手段である。

ここでは、利用者が、医師のコンピュータシステムに対して利用者の電子カルテファイル 310-1 が格納されているネットワーク上のアドレス情報について通知する。

[0041] アプリケーションファイル開錠機能 114 は、“オープン暗証コード”の入力を受けて“オープン暗証コード”の認証を確認し、認証が成立すれば個人データアプリケーションファイル 310 を開く機能である。

[0042] アプリケーションファイル閉錠機能 115 は、“クローズ暗証コード”の入力を受けて“クローズ暗証コード”の認証を確認し、認証が成立すれば、開いている状態の個人データアプリケーションファイル 310-1 を正常終了して閉じる機能である。

[0043] 次に、他者が利用するコンピュータリソース 200 には、個人データアプリケーション 210-1 がダウンロードされているか、または A S P で利用可能となっている。図 1 ではスマートフォン上にダウンロードされたアプリケーションとして描いているが、A S P で利用可能な場合、アプリケーション本体はネットワーク上に存在している。

この例では、コンピュータリソース 200 の個人データアプリケーション 210-1 は、アプリケーション管理機能 211、入力手段 212、アプリケーションファイル編集機能 214、アプリケーションファイルアクセス情報受信手段 213 を備えた構成となっている。

[0044] アプリケーション管理機能 211 は、個人データアプリケーション 210-1 によって多種多様であり、個人データ管理に必要な処理を実行するための諸機能が装備されているものとする。この実施例 1 では、電子カルテを取り扱う上で必要とされるアプリケーションの諸機能が装備されているものとする。

[0045] 入力手段 212 は、他者利用のコンピュータシステム 200 が装備しているデータ入力デバイスである。

入力手段 212 は、キーボード、タッチパネルなどの一般的な入力デバイスのほか、I C カードリーダー、生体情報読み取りデバイスなど、多様な入力デバイスが利用可能である。システムの運用に応じて、装備する入力デバイスを取り付ければ良い。

[0046] アプリケーションファイルアクセス情報受信手段 213 は、アプリケーシ

ョンファイルアクセス情報通知手段 113 から通知されたサーバーのアドレス情報を受信する手段である。この受け取ったサーバーのアドレス情報を用いて、個人データアプリケーションファイル 310-1 にアクセスする。

ここでは、医師のコンピュータシステムが、サーバーのアドレス情報を基に利用者の電子カルテファイル 310-1 が格納されているクラウドシステムにアクセスできるようになる。

[0047] アプリケーションファイル編集機能 214 は、オープン状態にある個人データアプリケーションファイル 310-1 に対してデータ入力、データ変更などの編集を行う機能である。具体的な機能は個人データアプリケーションファイル 310-1 の内容によって異なる。

この実施例 1 では、電子カルテの閲覧機能、入力機能、編集機能などが装備されているものとする。

[0048] 図 2 から図 3 は、実施例 1 にかかる本発明の個人データアプリケーション 110-1、210-1、個人データアプリケーション 310-1 の操作の概略を説明する図である。特に、個人データアプリケーションファイル 310-1 を開く際と、個人データアプリケーションファイル 310-1 を閉じる際に設定されているセキュリティの処理について説明している。

この例では、個人データアプリケーション 110-1 は、スマートフォンに搭載された例となっており、スマートフォンのタッチパネルを介した入力が可能となっている。

[0049] 近年のグラフィックユーザーインターフェイスでは、各種アプリケーションファイルがアイコンで表示されており、従来の一般のアプリケーションファイルでは、当該アイコンを指定すると当該アプリケーションファイルを取り扱うアプリケーションが立ち上がり、その後当該アプリケーションによりアプリケーションファイルが開かれて編集可能な状態になる。

本実施例 1 においても、スマートフォンに格納された個人データアプリケーション 110-1 で取り扱い可能な個人データアプリケーションファイル 310-1 のアイコンが多数表示されてアイコン操作が可能なケースを例に

とり説明する。

[0050] 以下、操作と処理の流れを説明する。

以下、番号は図1～図3の図中に表示した番号となっている。

(1)－1、(1)－2、(1)－3、(1)－4、(1)－5

利用者が、個人データアプリケーション110－1を選択起動する。

この例では、患者がスマートフォンを操作してタッチパネル上に表示されている電子カルテサービスアプリのアイコンをタップする。

また、利用者が、表示されたアイコンから目的の個人データアプリケーションファイル310－1を選択する。

個人データアプリケーションファイル310－1を選択起動する方法は限定されないが、ここでは一例として、患者がスマートフォンを操作してタッチパネル上に表示されている自分自身の電子カルテファイルのアイコンをダブルタップすることにより、個人データアプリケーションファイル310－1が選択的に起動される。

[0051] 一方、他者は、コンピュータシステムにおいて個人データアプリケーション210－1を選択起動する。

この例では、医師がコンピュータシステムのディスプレイ上に表示されている電子カルテサービスアプリのアイコンをクリックする。

さらに、医師が診察に訪れている患者の診察ファイルをクリックし、患者の診察ファイルを開いておく。

[0052] (2)－1、(2)－2

利用者が、表示された入力カラムを介してオープン暗証コードを入力する。

アプリケーションファイル開錠機能114によって、個人データアプリケーションファイル310－1を開くための“オープン暗証コード”の入力カラムが表示され、“オープン暗証コード”の入力が要求される。

この例では、患者がスマートフォンを操作してタッチパネル上に表示されているオープン暗証コードの入力カラムにオープン暗証コードを入力する。

“オープン暗証コード”の入力方法は限定されないが、この例では入力カラムに対して、表示画面に表示された入力キーをタップすることにより入力してゆく。

“オープン暗証コード”が入力され、アプリケーションファイル開錠機能 114 によって認証が成立すれば、個人データアプリケーション 110-1 が立ち上がり、個人データアプリケーションファイル 310-1 が開いて当該個人データアプリケーション 110-1 により編集・操作が可能な状態となる。

[0053] (3) - 1、(3) - 2

アプリケーションファイルアクセス情報通知手段 113 は、アプリケーションファイルアクセス情報受信手段 213 に対して、ネットワーク上のサーバーのアドレス情報を通知する。

この例では、利用者のスマートフォンに表示されている医療機関の選択画面において電子カルテファイルへのアクセスを許可する医療機関の選択を行う。

アプリケーションファイルアクセス情報受信手段 213 は、サーバーのアドレス情報を受信する。

この例では、アプリケーションファイルアクセス情報受信手段 213 は、サーバーのアドレス情報を受信すると、該当する患者の電子カルテファイルの準備ができた旨の表示がなされる。

[0054] (4) - 1、(4) - 2

アプリケーションファイル編集機能 214 は、この受け取ったサーバーのアドレス情報を用いて、個人データアプリケーションファイル 310-1 にアクセスする。

個人データアプリケーションファイル 310-1 はオープンされ、編集可能となっており、他者によってアプリケーションファイル編集機能 214 を用いてデータ編集が可能となる。

ここでは、医師のコンピュータシステムが、サーバーのアドレス情報を基

に利用者の電子カルテファイル 310-1 が格納されているクラウドシステムにアクセスできるようになり、過去の治療履歴の閲覧、今回の診察内容の書き込みなどの編集が可能となる。

ここでは、医師が、患者の電子カルテファイル 310-1 に対して、アプリケーションファイル編集機能 214 により操作・編集を行い、患者の電子カルテファイル 310-1 への編集・入力が完了する。

たとえば、入力終了のボタンを押下する。

[0055] (5)-1、(5)-2、(5)-3

他者によるデータ編集・入力が完了したことを受け、利用者が個人データアプリケーションファイル 310-1 を閉じる操作を行う。

ここでは、利用者がアプリケーション 110-1 上の操作ボタンの 1 つである“閉じる”操作ボタンをタップしてアプリケーションファイル 110 を閉じる操作を指定する。

利用者のスマートフォンのタッチパネルには、アプリケーションファイル閉錠機能 115 により、アプリケーションファイル 310-1 を正常終了するためのクローズ暗証コードの入力カラムが表示され、クローズ暗証コードの入力が要求される。

クローズ暗証コードの入力方法は限定されないが、この例では入力カラムに対して、表示画面に表示された入力キーをタップすることにより入力してゆく。

クローズ暗証コードが入力され、アプリケーションファイル閉錠機能 115 による認証が成立すれば、アプリケーションファイル 110-1 が正常終了して閉じる。アプリケーションファイル 110 の編集内容が確定することとなる。

利用者のスマートフォン上、他者のコンピューターリソース上、個人データアプリケーションの終了画面が表示される。

[0056] アプリケーションファイル開錠機能 114、アプリケーションファイル閉錠機能 115 を装備することにより、アプリケーションファイルは通常時は

アクセス、編集ができない状態となっており、利用者の意思に基づいて編集可能となり、また、他者のアプリケーションファイル編集機能214で編集された個人データアプリケーションファイル310-2の編集内容を利用者本人が確認してから確定することができるため、セキュリティが高まる。

この例では、個人データアプリケーション110-1が電子カルテアプリケーションであり、個人データアプリケーションファイル310-1が電子カルテファイルであり、想定できる利用者が患者本人（子供の場合は保護者）であり、電子カルテファイルを編集する者が医師などの医療関係者であるので、アプリケーションファイル閉錠機能115が装備されていれば、利用者がインフォームドコンセントを受けて、その内容（編集内容）を確認した上で、クラウドシステム上にある電子カルテファイルへの編集を確定して終了することができる。

実施例 2

[0057] 実施例2にかかる本発明の個人データアプリケーション110-2について説明する。

実施例1と同様、ネットワーク上には、サーバー300があり、個人データアプリケーションファイル310-2が記憶装置に格納されており、個人データアプリケーション110-2、個人データアプリケーション210-2からアクセス可能になっている。クラウドシステムとして利用される場合もあり得る。

実施例2においても、個人データアプリケーションファイル310-2は電子カルテファイルの例として説明する。

図4は実施例2にかかる個人データアプリケーション110-2、210-2、個人データアプリケーションファイル310-2の構成を簡単に示した図である。

[0058] 実施例2にかかる個人データアプリケーション110-2で利用される各々の個人データアプリケーションファイル310-2に対して、個人データアプリケーション110-2により個人データアプリケーションファイル3

10-2を開くための“オープン暗証コード”と、個人データアプリケーション110-2で開いている個人データアプリケーションファイル310-2を正常終了して閉じるための“クローズ暗証コード”に加え、他者のコンピュータリソースを経由した当該個人データアプリケーションファイル310-2へのデータ編集を許可するための“編集開始暗証コード”と、他のコンピュータリソースを経由した個人データアプリケーションファイル310-2の編集を終了するための“編集終了暗証コード”が設定されたものとなっている。

なお、オープン暗証コード312、クローズ暗証コード313、編集開始暗証コード314、編集終了暗証コード315は、例えば、数字からなるPINコード、さらに文字情報も加えたパスワード、バーコードなどの1次元コード、QRコードなどの二次元コード、さらに指紋パターンや静脈パターンや虹彩パターンや声紋パターンや顔画像など編集者の生体情報などがある。また、編集者が保持携帯するカードに格納されたID情報でも良い。

[0059] 次に、利用者が保持するスマートフォンなどの利用者端末100には、個人データアプリケーション110-2がダウンロードされているか、またはASPで利用可能となっている。図4ではスマートフォン上にダウンロードされたアプリケーションとして描いているが、ASPで利用可能な場合、アプリケーション本体はネットワーク上に存在している。

利用者が保持するスマートフォンなどの利用者端末100、個人データアプリケーション110-2の構成および処理動作は実施例1と同様で良く、ここでの詳しい説明は省略する。

[0060] 次に、他者が利用するコンピュータリソース200を説明する。

他者が利用するコンピュータリソース200には、個人データアプリケーション210-1がダウンロードされているか、またはASPで利用可能となっている。図4ではスマートフォン上にダウンロードされたアプリケーションとして描いているが、ASPで利用可能な場合、アプリケーション本体はネットワーク上に存在している。

実施例２の構成例では、個人データアプリケーション２１０－２は、アプリケーション管理機能２１１、入力手段２１２、アプリケーションファイルアクセス情報受信手段２１３、アプリケーションファイル編集機能２１４に加え、編集開始暗証コード認証機能２１５、編集開始暗証コード認証機能２１６を備えた構成となっている。

ここで、アプリケーション管理機能２１１、入力手段２１２、アプリケーションファイルアクセス情報受信手段２１３、アプリケーションファイル編集機能２１４は、実施例１と同様で良く、ここでの説明は省略する。

[0061] 編集開始暗証コード認証機能２１５は、アプリケーションファイル編集機能２１４が、利用者の個人データアプリケーションファイル３１０－２へのデータ編集を行う他者に対して、個人データアプリケーションファイル３１０－２へのデータ編集の開始にあたり“編集開始暗証コード”の入力を求め、認証を行う機能である。

[0062] 編集開始暗証コード認証機能２１６は、データ編集の正常終了にあたり“編集終了暗証コード”の入力を求め、認証を行う機能である。

つまり、個人データアプリケーションファイル３１０－２へのデータ編集を完了するには、データ編集前に、利用者自身による“オープン暗証コード”の入力と、編集する他者による“編集開始暗証コード”の入力を要求し、データ編集後の正常終了に際して、利用者自身による“クローズ暗証コード”の入力と、編集する他者による“編集終了暗証コード”の入力を要求する流れとなっている。

[0063] 図５から図７は、実施例２にかかる本発明の個人データアプリケーション１１０－２、２１０－２、個人データアプリケーション３１０－２の操作の概略を説明する図である。特に、個人データアプリケーションファイル３１０－２を開く際と、個人データアプリケーションファイル３１０－２を閉じる際、および、他者が編集を開始する際と編集を終了する際に設定されているセキュリティの処理について説明している。

この例では、個人データアプリケーション１１０－２は、スマートフォン

に搭載された例となっており、スマートフォンのタッチパネルを介した入力が可能となっている。

[0064] 以下、操作と処理の流れを説明する。

以下、番号は図4～図7の図中に表示した番号となっている。

(11) - 1、(11) - 2、(11) - 3、(11) - 4、(11) - 5

利用者による個人データアプリケーション110-2の選択起動、個人データアプリケーションファイル310-2の選択、他者によるコンピュータシステムにおける個人データアプリケーション210-2の選択起動などの流れは実施例1と同様で良く、ここでの詳しい説明は省略する。

[0065] (12) - 1、(12) - 2

利用者によるオープン暗証コードの入力、入力されたオープン暗証コードを用いたアプリケーションファイル開錠機能114による認証成立による、個人データアプリケーション110-2の立ち上げ、個人データアプリケーションファイル310-2の開錠の各処理についても実施例1と同様で良く、ここでの詳しい説明は省略する。

[0066] (13) - 1、(13) - 2

アプリケーションファイルアクセス情報通知手段113による、アプリケーションファイルアクセス情報受信手段213に対するネットワーク上のサーバーのアドレス情報の通知、アプリケーションファイルアクセス情報受信手段213によるサーバーのアドレス情報の受信、該当する患者の電子カルテファイルの準備ができた旨の表示の各処理についても実施例1と同様で良く、ここでの詳しい説明は省略する。

[0067] (14) - 1、(14) - 2

アプリケーションファイル編集機能214は、この受け取ったサーバーのアドレス情報を用いて、個人データアプリケーションファイル310-2にアクセスする。該当する個人データアプリケーションファイルの編集開始を意味するボタンを押下する。ここではたとえば“電子カルテが準備できまし

た” というボタンを押下する。

本実施例2では、個人データアプリケーションファイル310-2はオープンされているが、編集に際しては、編集開始暗証コードの認証処理が必要となっている。

[0068] 利用者のコンピュータリソース200のディスプレイに表示される編集開始暗証コードの入力カラムに対して編集開始暗証コードを入力する。

編集開始暗証コードの入力方法は限定されないが、この例では入力カラムに対して、表示画面に表示された入力キーをタップすることにより入力してゆく。

編集開始暗証コードが入力され、編集開始暗証コード認証機能215による認証が成立すれば、他者によってアプリケーションファイル編集機能214を用いてアプリケーションファイル110-2へのデータ編集が可能となる。

ここでは、医師のコンピュータシステムが、サーバー300のアドレス情報を基に利用者の電子カルテファイル310-2が格納されているクラウドシステムにアクセスできるようになり、過去の治療履歴の閲覧、今回の診察内容の書き込みなどの編集が可能となる。

[0069] (15) 個人データアプリケーションファイルの編集

他者が個人データアプリケーションファイルの編集を行う。

ここでは、医師が、患者の電子カルテファイル310-2に対して、アプリケーションファイル編集機能214により操作・編集を行い、患者の電子カルテファイル310-2への編集・入力が完了する。

たとえば、入力終了のボタンを押下する。

[0070] (16)-1、(16)-2、(16)-3

本実施例2では、他者による個人データアプリケーションファイル310-2への編集の終了の際にも編集終了暗証コードの認証処理が必要となっている。編集が同一人により開始されて終了されたことを確認するためである。

この例では、医師による患者へのインフォームドコンセントを行い、その後、編集終了ボタンを押下することにより、利用者のコンピュータリソース 200 のディスプレイに表示され、当該編集終了暗証コードの入力カラムに対して編集終了暗証コードを入力する。

編集終了暗証コードの入力方法は限定されないが、この例では入力カラムに対して、表示画面に表示された入力キーをタップすることにより入力してゆく。

編集終了暗証コードが入力され、編集終了暗証コード認証機能 216 による認証が成立すれば、他者によってアプリケーションファイル編集機能 214 を用いてアプリケーションファイル 110-2 へのデータ編集が終了する。

[0071] (17)-1、(17)-2、(17)-3

他者によるデータ編集・入力が完了したことを受け、利用者が個人データアプリケーションファイル 310-2 を閉じる操作を行う。

利用者による個人データアプリケーションファイル 310-2 の正常終了処理、アプリケーションファイル閉錠機能 115 によるクローズ暗証コードの認証処理、アプリケーションファイル 110-2 の正常終了処理は実施例 1 と同様で良く、ここでの説明は省略する。

[0072] このように、編集開始暗証コード認証機能 215、編集終了暗証コード認証機能 216 を備えることにより、編集した他者が正当な編集権限を持つ他者であることが認証でき、成り済まし防止などのセキュリティが高まる。

また、アプリケーションファイル開錠機能 114、アプリケーションファイル閉錠機能 115 を装備することにより、アプリケーションファイルは通常時はアクセス、編集ができない状態となっており、利用者の意思に基づいて編集可能となり、また、他者のアプリケーションファイル編集機能 214 で編集された個人データアプリケーションファイル 310-2 の編集内容を利用者本人が確認してから確定することができるため、セキュリティが高まる。

実施例 3

[0073] 実施例3にかかる本発明の個人データアプリケーション110-3、210-3、個人データアプリケーションファイル310-3、個人フォルダ320-3について説明する。

図8は実施例3にかかる個人データアプリケーション110-3、210-3、個人データアプリケーションファイル310-3、個人フォルダ320-3の構成を簡単に示した図である。

実施例3は、個人データアプリケーションファイル310-3が個人単位に個人フォルダ320-3にまとめられており、個人フォルダ320-3は1つまたは複数個設けられており、それぞれの個人フォルダ320-3の中には、個人データアプリケーションファイル310-3が格納されている。

[0074] 図13は、サーバー300内の個人フォルダ320-3、個人データアプリケーションファイル310-3の例を模式的に示した図である。個人データアプリケーション110-3、210-3の構成は図示を省略している。

図13に示す例では、個人フォルダ320-3として個人フォルダ1と個人フォルダ2があり、個人フォルダ1には、個人データアプリケーションファイル310-3として、電子カルテファイル、電子保険証ファイル、電子お薬手帳ファイルが格納されている例となっている。個人フォルダ2には、個人データアプリケーションファイル310-3として、電子住民票ファイル、電子資格証ファイル、電子運転免許証ファイル、電子パスポートなどが格納されている例となっている。

[0075] 実施例3の例では、図8に示すように、個人フォルダ320-3には、個人フォルダオープン暗証コード321と、個人フォルダクローズ暗証コード322が設定されている。

また、個人データアプリケーションファイル310-3にはオープン暗証コード312、クローズ暗証コード313、編集開始暗証コード314、編集終了暗証コード315が設定されている。

また、個人データアプリケーション110-3には、個人フォルダ開錠機

能 1 1 6、アプリケーションファイル開錠機能 1 1 4、アプリケーションファイル閉錠機能 1 1 5、個人フォルダ閉錠機能 1 1 7 を備えている例である。

[0076] 個人フォルダ開錠機能 1 1 6 は、“個人フォルダオープン暗証コード”の入力を受けて“個人フォルダオープン暗証コード”の認証を確認し、認証が成立すれば個人フォルダ 3 2 0-3 を開く機能である。

個人フォルダ閉錠機能 1 1 7 は、“個人フォルダクローズ暗証コード”の入力を受けて“個人フォルダクローズ暗証コード”の認証を確認し、認証が成立すれば、開いている状態の個人フォルダ 3 2 0-3 を正常終了して閉じる機能である。

他の構成要素は実施例 1、実施例 2 と同様であり、ここでの詳しい説明は省略する。

[0077] また、個人データアプリケーション 2 1 0-3 には、編集開始暗証コード認証機能 2 1 5、アプリケーションファイル編集機能 2 1 4、編集終了暗証コード認証機能 2 1 6 を備えている例である。

これら構成要素は実施例 2 と同様であり、ここでの詳しい説明は省略する。

[0078] 以下、操作と処理の流れを説明する。

以下、番号は図 8～図 1 3 の図中に表示した番号となっている。

(2 1) - 1、(2 1) - 2、(2 1) - 3、(2 1) - 4、(2 1) - 5

利用者が、個人データアプリケーション 1 1 0-1 を選択起動する。

この例では、患者がスマートフォンを操作してタッチパネル上に表示されている電子カルテサービスアプリのアイコンをタップする。

次に、利用者が、表示されたアイコンから目的の個人フォルダ 3 2 0-3 を選択起動する。

個人フォルダ 3 2 0-3 を選択起動する方法は限定されないが、ここでは一例として、患者がスマートフォンを操作してタッチパネル上に表示されて

いる個人フォルダ320-3から、使用しようとする電子カルテファイルが格納されている個人フォルダ320-3のアイコンをダブルタップすることにより、個人フォルダ320-3が選択的に起動される。

一方、他者は、コンピュータシステムにおいて個人データアプリケーション210-1を選択起動する。

この例では、医師がコンピュータシステムのディスプレイ上に表示されている電子カルテサービスアプリのアイコンをクリックする。

さらに、医師が診察に訪れている患者の診察ファイルをクリックし、患者の診察ファイルを開いておく。

[0079] (22)

実施例3の構成例では、個人フォルダ開錠機能116によって、個人フォルダ320-3を開くための“個人フォルダオープン暗証コード”の入力カラムが表示され、“個人フォルダオープン暗証コード”の入力が要求される。

この例では、患者がスマートフォンを操作してタッチパネル上に表示されている個人フォルダオープン暗証コードの入力カラムに個人フォルダオープン暗証コードを入力する。

“個人フォルダオープン暗証コード”の入力方法は限定されないが、この例では入力カラムに対して、表示画面に表示された入力キーをタップすることにより入力してゆく。

“個人フォルダオープン暗証コード”が入力され、個人フォルダ開錠機能116によって認証が成立すれば、個人フォルダ320-3が立ち上がり、個人フォルダ320-1が開いてその中に格納されている個人データアプリケーションファイル310-3が表示される。

[0080] (23)

利用者による個人データアプリケーション110-3を選択起動については実施例1、2と同様で良く、ここでの詳しい説明は省略する。

この例では、患者がスマートフォンを操作してタッチパネル上に表示され

ている電子カルテサービスアプリのアイコンをタップする。

医師は診察に訪れている患者の診察ファイルをクリックし、患者の診察ファイルを開いておく。

[0081] (24) - 1、(24) - 2

利用者によるオープン暗証コードの入力、入力されたオープン暗証コードを用いたアプリケーションファイル開錠機能114による認証成立による、個人データアプリケーション110-2の立ち上げ、個人データアプリケーションファイル310-2の開錠の各処理についても実施例1、2と同様で良く、ここでの詳しい説明は省略する。

[0082] (25) - 1、(25) - 2

アプリケーションファイルアクセス情報通知手段113による、アプリケーションファイルアクセス情報受信手段213に対するネットワーク上のサーバーのアドレス情報の通知、アプリケーションファイルアクセス情報受信手段213によるサーバーのアドレス情報の受信、該当する患者の電子カルテファイルの準備ができた旨の表示の各処理についても実施例1、2と同様で良く、ここでの詳しい説明は省略する。

[0083] (26) - 1、(26) - 2

アプリケーションファイル編集機能214による個人データアプリケーションファイル310-2へのアクセス、編集開始暗証コードの入力カラムに対する編集開始暗証コードの入力、編集開始暗証コードの認証処理についても実施例1、2と同様で良く、ここでの詳しい説明は省略する。

[0084] (27)

他者によるアプリケーションファイル編集機能214を用いたアプリケーションファイル110-2へのデータ編集が可能となる。

ここでは、医師のコンピュータシステムが、サーバー300のアドレス情報を基に利用者の電子カルテファイル310-2が格納されているクラウドシステムにアクセスできるようになり、過去の治療履歴の閲覧、今回の診察内容の書き込みなどの編集が可能となる。

ここでは、医師が、患者の電子カルテファイル 310-2 に対して、アプリケーションファイル編集機能 214 により操作・編集を行い、患者の電子カルテファイル 310-2 への編集・入力完了する。

[0085] (28)-1、(28)-2

医師による患者へのインフォームドコンセント

本実施例 3 では、他者による個人データアプリケーションファイル 310-2 への編集の終了の際にも編集終了暗証コードの認証処理が必要となっている。編集が同一人により開始されて終了されたことを確認するためである。

この例では、医師による患者へのインフォームドコンセント、編集終了暗証コードの入力カラムに対する編集終了暗証コードの入力、編集終了暗証コード認証機能 216 による認証処理については実施例 2 と同様であり、ここでの詳しい説明は省略する。

[0086] (29)

他者によるデータ編集・入力完了したことを受け、利用者が個人データアプリケーションファイル 310-3 を閉じる操作を行う。

利用者による個人データアプリケーションファイル 310-3 の正常終了処理、アプリケーションファイル閉錠機能 115 によるクローズ暗証コードの認証処理、アプリケーションファイル 110-3 の正常終了処理は実施例 1 と同様で良く、ここでの説明は省略する。

[0087] (30)

実施例 3 の構成例では、個人フォルダ閉錠機能 117 によって、個人フォルダ 320-3 を閉じるための“個人フォルダクローズ暗証コード”の入力カラムが表示され、“個人フォルダクローズ暗証コード”の入力が要求される。

この例では、患者がスマートフォンを操作してタッチパネル上に表示されている個人フォルダクローズ暗証コードの入力カラムに個人フォルダクローズ暗証コードを入力する。

“個人フォルダクローズ暗証コード”の入力方法は限定されないが、この

例では入力カラムに対して、表示画面に表示された入力キーをタップすることにより入力してゆく。

“個人フォルダクローズ暗証コード”が入力され、個人フォルダ閉錠機能 1 1 7 によって認証が成立すれば、個人フォルダ 3 2 0 - 3 が正常終了して閉じられる。

- [0088] このように、個人フォルダ開錠機能 1 1 6 および個人フォルダ閉錠機能 1 1 7 を備えることにより、個人フォルダは通常時はアクセスできない状態となっており、利用者の意思に基づいて個人フォルダを開いたり閉じたりすることができる。また、他者のアプリケーションファイル編集機能 2 1 4 で編集された個人データアプリケーションファイル 3 1 0 - 3 の編集内容を利用者本人が確認してから確定することができるため、セキュリティが高まる。

実施例 4

- [0089] 実施例 4 にかかる本発明の個人データアプリケーション 1 1 0 - 4、2 1 0、個人データアプリケーションファイル 3 1 0 について説明する。

実施例 4 は、利用者である患者が利用する利用者端末 1 0 0 - 4 が病院などの医療施設の受付などに設置されている受付端末となっている例である。つまり、利用者は自分のスマートフォンなどの個人所有のものではなく、来院した患者が当該 1 台の受付端末を使用するものとなっており、複数の患者が共用する端末となっている例である。

- [0090] 図 1 4 は実施例 4 にかかる個人データアプリケーション 1 1 0、2 1 0、個人データアプリケーションファイル 3 1 0 の構成を簡単に示した図である。

実施例 4 は、病院の総合受付端末 1 0 0 - 4 にインストールされているか A S P により利用可能な形態となっている。病院に来院した患者は総合受付端末 1 0 0 - 4 を介して来院の受付を行う運用となっており、複数の患者がこの総合受付端末 1 0 0 - 4 で利用可能な個人データアプリケーション 1 1 0 を使用する。

- [0091] 図 1 4 に示すように、個人データアプリケーション 1 1 0 は、実施例 1 と

同様、アプリケーション本体機能 1 1 1、入力手段 1 1 2、アプリケーションファイルアクセス情報通知手段 1 1 3、アプリケーションファイル開錠機能 1 1 4、アプリケーションファイル閉錠機能 1 1 5 を備えたものとなっている。

[0092] アプリケーション本体機能 1 1 1 は、電子カルテファイル管理に必要な処理を実行するための諸機能が装備されているが、本実施例 4 では、患者の I D 識別機能を備え、患者の提示した I D 情報に応じてサーバー 3 0 0 に格納されている電子カルテファイル 3 1 0 のうち当該患者の電子カルテファイルを識別してデータ入力機能、データ出力機能、データ格納機能などの機能を提供する。

[0093] 患者の I D 識別機能は、限定されず多様なものがあり得る。

例えば、患者が生体情報を登録していれば、来院した患者が生体情報を入力することにより患者の生体情報を I D 識別情報と取り扱うことが可能である。

例えば、患者が通院カードを有していれば、来院した患者がリーダなどを介して通院カードに書き込まれている I D 識別情報を入力することが可能である。

[0094] 入力手段 1 1 2 は、本実施例 4 では病院の総合受付端末のタッチパネルなどとして提供されている。キーボードやマウスなどの入力手段を排除するものではないが、タッチパネルやボタン押下式の方が共用される環境ではキーボードやマウスの操作が苦手な人でも利便性が高い。

[0095] アプリケーションファイルアクセス情報通知手段 1 1 3、アプリケーションファイル開錠機能 1 1 4、アプリケーションファイル閉錠機能 1 1 5 は、実施例 1 で説明したものと同様で良い。

[0096] 次に、医療関係者などが利用するコンピュータリソース 2 0 0 にインストールまたは A S P で利用可能となっている個人データアプリケーション 2 1 0 は、アプリケーション管理機能 2 1 1、入力手段 2 1 2、アプリケーションファイルアクセス情報受信手段 2 1 3、アプリケーションファイル編集機

能 2 1 4 を備えた構成となっている。これらは実施例 1 と同様で良い。

[0097] 次に、サーバー 3 0 0 に格納されている個人データアプリケーションファイル 3 1 0 を説明する。

実施例 1 から実施例 3 においても、サーバー 3 0 0 には、複数の者の個人データアプリケーションファイル 3 1 0 を格納することが可能である。

サーバー 3 0 0 に格納されている個人データアプリケーションファイル 3 1 0 の規模であるが、本発明では限定されない。運用によって多様な規模があり得る。この実施例 4 の例は、電子カルテファイルを例に説明しており、例えば、個人データアプリケーションファイル 3 1 0 が 1 つのクリニックだけで利用されるものであれば、そのクリニックを利用する患者の規模となる。例えば、国民皆保険に加入する被保険者のカルテが電子カルテファイルとして共通仕様に制定された場合、国民皆保険に加入する被保険者の総数に相当する規模となる。このように膨大な電子カルテファイルを取り扱う場合、サーバー 3 0 0 が大規模なシステムとなることが想定できる。

[0098] ここでは、説明上、サーバー 3 0 0 には、患者 A の電子カルテファイル 3 1 0 - A、患者 B の電子カルテファイル 3 1 0 - B、患者 C の電子カルテファイル 3 1 0 - C、患者 D の電子カルテファイル 3 1 0 - D の 4 者の電子カルテファイル 3 1 0 のみを図示しているが、多数の数に上る場合も同様に考えればよい。

[0099] 図 1 4 に示した電子カルテファイル 3 1 0 には、実施例 1 の個人データアプリケーションファイル 3 1 0 - 1 と同様、個人データアプリケーションファイル本体 3 1 1、オープン暗証コード 3 1 2、クローズ暗証コード 3 1 3 が設けられている。もし、実施例 2 のタイプの電子カルテファイル 3 1 0 - 2 であれば、それらに加え、編集開始暗証コード 3 1 4、編集終了暗証コード 3 1 5 が設けられており、実施例 3 のタイプのものであれば、個人フォルダ 3 2 0 ごとに整理されており、個人フォルダ 3 2 0 に、個人フォルダオープン暗証コード 3 2 1、個人フォルダクローズ暗証コード 3 2 2 を備えたものとなっている。

[0100] 実施例4にかかる利用者端末100が病院などの受付端末100-4となっている例の場合の運用の例を説明する。

例えば、図15に示すように、来院した患者Aは、受付端末100-4を介して受付をして自分のID識別情報を入れて受付をする。この例では、診療科別にボタンが表示されており、自分が受診したいボタンをタッチして受付を続行する。受付端末100-4がサーバー300にアクセスし、当該ID識別情報により特定される患者Aの電子カルテファイル310Aにアクセスする。実施例1に示したように、患者Aはアプリケーションファイル開錠機能114を介して、オープン暗証コードを入力して、自分自身の電子カルテファイル310をオープンにする。ここでは受付端末100-4の入力手段112を介して指定された生体情報を入れる。

[0101] 受付端末100-4はアプリケーションファイルアクセス情報通知手段113を介して、患者Aが受診する担当医師の利用するコンピュータリソース200にアプリケーションファイルアクセス情報を通知する。

この例では、引き続き、患者Bが来院し、患者Aと同様、受付を行う。患者Bの受診したい診療科が異なっても良く、受付の結果、患者BのID識別情報の入力、オープン暗証コードの入力を経て、電子カルテファイル310Bがオープンされ、患者Bが受診する担当医師の利用するコンピュータリソース200にアプリケーションファイルアクセス情報が通知される。

つまり、図15に示すように、同時に複数の電子カルテファイル310が独立して個別にオープン状態となり、個別に別々の医師により独立して個別に編集することができる。

[0102] 次に、例えば、図16に示すように、患者Aの診察が終了し、医師が電子カルテファイル310Aを編集した後、受付端末100-4は、退院の処理のため受付端末100-4に訪れた患者Aに対して、電子カルテファイル310Aの編集の承認を得るべくアプリケーションファイル閉鍵機能215を介してクローズ暗証コードの入力を求め、クローズ暗証コードの入力があった場合に、診察費支払い案内とともに電子カルテファイル310Aをクロー

ズする。ここでは患者Aがふたたび受付端末100-4の入力手段112を介して指定された生体情報を入れる。

[0103] 一方、患者Bはまだ診察が終了しておらず患者Bの電子カルテファイル310Bはオープンしたままとなっている。

[0104] さらに、図16の例では、この状態で、新たに患者Cが来院し、来院した患者Cが、受付端末100-4を介して受付をした例となっている。患者Cが同様に自分のID識別情報を入れて受付をし、当該ID識別情報により特定される患者Cの電子カルテファイル310Cにアクセスされ、アプリケーションファイル開錠機能114を介して、患者Cがオープン暗証コードを入力して、患者Cの電子カルテファイル310Cをオープンされている。

[0105] このように、複数の患者が任意のタイミングで来院、退院しても、共用する受付端末100-4を介して、実施例1、実施例2、実施例3で示した、個人データアプリケーション100を操作し、個人データアプリケーションファイル310を利用できるものとなっている。医師も自分が担当する患者の個人データアプリケーションファイル310を利用できるものとなっている。

産業上利用可能性

[0106] 本発明は、コンピュータシステムで利用される個人データアプリケーションファイルに適用され、例として、利用者個人の行政上の記録情報または資格情報の内容を示す行政関連ファイル、電子カルテファイル、電子保険証ファイル、電子お薬手帳ファイル、電子運転免許証ファイル、電子資格証ファイル、電子住民票ファイル、電子印鑑登録証ファイル、電子パスポートファイルなど多様なものに適用できる。

符号の説明

- [0107] 100 利用者端末
110 個人データアプリケーション
111 アプリケーション本体機能
112 入力手段

- 1 1 3 アプリケーションファイルアクセス情報通知手段
- 1 1 4 アプリケーションファイル開錠機能
- 1 1 5 アプリケーションファイル閉錠機能
- 1 1 6 個人フォルダ開錠機能
- 1 1 7 個人フォルダ閉錠機能
- 2 0 0 コンピュータリソース
- 2 1 0 個人データアプリケーション
- 2 1 1 アプリケーション管理機能
- 2 1 2 入力手段
- 2 1 3 アプリケーションファイルアクセス情報受信手段
- 2 1 4 アプリケーションファイル編集機能
- 2 1 5 編集開始暗証コード認証機能
- 2 1 6 編集開始暗証コード認証機能
- 3 1 0 個人データアプリケーションファイル
- 3 1 1 個人データアプリケーションファイル本体
- 3 1 2 オープン暗証コード
- 3 1 3 クローズ暗証コード
- 3 1 4 編集開始暗証コード
- 3 1 5 編集終了暗証コード
- 3 2 0 個人フォルダ
- 3 2 1 個人フォルダオープン暗証コード
- 3 2 2 個人フォルダクローズ暗証コード

請求の範囲

- [請求項1] 個人データを取り扱う個人データアプリケーションであって、
前記個人データアプリケーションで利用される各々の個人データアプリケーションファイルであって、前記個人データアプリケーションで前記個人データアプリケーションファイルを開くためのオープン暗証コードと、前記個人データアプリケーションで開いた前記個人データアプリケーションファイルを正常終了して閉じるためのクローズ暗証コードが設定された個人データアプリケーションファイルと、
前記オープン暗証コードの入力を受けて前記個人データアプリケーションファイルを開くアプリケーションファイル開錠機能と、
開かれた前記個人データアプリケーションファイルに対して、他のコンピュータリソースを経由した他者によるデータ編集を受け付けるアプリケーションファイル編集機能と、
前記クローズ暗証コードの入力を受けて、前記個人データアプリケーションファイルに対する前記アプリケーションファイル編集機能によるデータ編集内容を確定し、正常終了して閉じるアプリケーションファイル閉錠機能を備えたことを特徴とする個人データアプリケーション。
- [請求項2] 前記個人データアプリケーションファイルに、前記他者による前記他のコンピュータリソースを経由した前記個人データアプリケーションファイルへのデータ編集を許可するための編集開始暗証コードが設定されたものであり、
前記アプリケーションファイル編集機能が、前記他者に対して前記個人データアプリケーションファイルへの前記データ編集の開始にあたり前記編集開始暗証コードの入力を求めることを特徴とする請求項1に記載の個人データアプリケーション。
- [請求項3] 前記個人データアプリケーションファイルに、前記他者による前記他のコンピュータリソースを経由した前記個人データアプリケーション

ンファイルへのデータ編集を許可するための編集開始暗証コードと、前記他のコンピュータリソースを経由した前記個人データアプリケーションファイルの編集を終了するための編集終了暗証コードが設定されたものであり、

前記個人データアプリケーションファイル編集機能が、前記他者に対して前記個人データアプリケーションファイルへの前記データ編集の開始にあたり前記編集開始暗証コードの入力と、前記データ編集の終了にあたり前記編集終了暗証コードの入力を求めることを特徴とする請求項1に記載の個人データアプリケーション。

[請求項4] 前記オープン暗証コードおよび前記クローズ暗証コードが、あらかじめ登録された前記個人データの所有者である個人の生体情報であることを特徴とする請求項1に記載の個人データアプリケーション。

[請求項5] 前記オープン暗証コードおよび前記クローズ暗証コードが、あらかじめ登録された前記個人データの所有者である個人の生体情報であり、
前記編集開始暗証コードが、あらかじめ登録された前記他者の生体情報であることを特徴とする請求項2に記載の個人データアプリケーション。

[請求項6] 前記オープン暗証コードおよび前記クローズ暗証コードが、あらかじめ登録された前記個人データの所有者である個人の生体情報であり、
前記編集開始暗証コードおよび前記編集終了暗証コードが、あらかじめ登録された前記他者の生体情報であることを特徴とする請求項3に記載の個人データアプリケーション。

[請求項7] 前記個人データアプリケーションファイルが、ネットワーク上のサーバーに格納され、管理されており、
前記個人データアプリケーションのうち、前記アプリケーションファイル開錠機能および前記アプリケーションファイル閉錠機能が、前

記個人データの所有者である個人が保持するスマートフォンにインストールされているか A S P により利用可能な形態で前記サーバーにアクセス可能になっており、

前記個人データアプリケーションのうち、前記アプリケーションファイル編集機能が、前記他者による前記他のコンピュータリソースにインストールされているか A S P により利用可能な形態で前記サーバーにアクセス可能なものになっていることを特徴とする請求項 1 から 6 のいずれかに記載の個人データアプリケーション。

[請求項8]

前記個人データアプリケーションファイルが、ネットワーク上のクラウドシステムに格納され、管理されており、

前記個人データアプリケーションのうち、前記アプリケーションファイル開錠機能および前記アプリケーションファイル閉錠機能が、前記個人データの所有者である個人が保持するスマートフォンにインストールされているか A S P により利用可能な形態で前記クラウドシステムにアクセス可能になっており、

前記個人データアプリケーションのうち、前記アプリケーションファイル編集機能が、前記他者による前記他のコンピュータリソースにインストールされているか A S P により利用可能な形態で前記クラウドシステムにアクセス可能なものになっていることを特徴とする請求項 1 から 6 のいずれかに記載の個人データアプリケーション。

[請求項9]

前記個人データアプリケーションで利用される各々の個人データアプリケーションファイルが個人単位に個人フォルダにまとめられており、

前記個人データアプリケーションで利用される各々の個人フォルダに、前記個人データアプリケーションで個人フォルダを開くための個人フォルダオープン暗証コードと、前記個人データアプリケーションで開いた前記個人フォルダを閉じるための個人フォルダクローズ暗証コードが設定されたものであることを特徴とする請求項 1 から 8 のい

ずれかに記載の個人データアプリケーション。

[請求項10] 前記個人データアプリケーションファイルが、利用者個人の行政上の記録情報または資格情報の内容を示す行政関連電子ファイルであり、前記個人データアプリケーションが、前記利用者個人の行政サービスアプリケーションであり、前記他者が前記行政関連電子ファイルのデータを編集する行政関係者であり、前記他のコンピュータリソースが、前記行政関係者が用いる行政関連電子ファイル管理システムであることを特徴とする請求項1から9のいずれかに記載の個人データアプリケーション。

[請求項11] 前記個人データアプリケーションファイルが、患者個人の電子カルテファイルであり、前記個人データアプリケーションが、前記患者個人の電子カルテサービスアプリケーションであり、前記他者が医療関係者であり、前記他のコンピュータリソースが、前記医療関係者が用いる医療機関利用システムであることを特徴とする請求項1から9のいずれかに記載の個人データアプリケーション。

[請求項12] 前記個人データアプリケーションファイルが、患者個人の電子お薬手帳ファイルであり、前記個人データアプリケーションが、前記患者個人の電子お薬手帳ファイルサービスアプリケーションであり、前記他者が薬剤師であり、前記他のコンピュータリソースが、前記薬剤師が用いる調剤薬局利用システムであることを特徴とする請求項1から9のいずれかに記載の個人データアプリケーション。

[請求項13] 前記個人データアプリケーションファイルが、被保険者個人の電子保険証ファイルであり、前記個人データアプリケーションが、前記被保険者個人の電子保険証サービスアプリケーションであり、前記他者が医療関係者であり、前記他のコンピュータリソースが、前記医療関係者が用いる医療機関利用システムであることを特徴とする請求項1から9のいずれかに記載の個人データアプリケーション。

[請求項14] 前記個人データアプリケーションファイルが、運転者個人の電子運

転免許証ファイルであり、前記個人データアプリケーションが、前記運転者個人の運転免許証サービスアプリケーションであり、前記他者が前記電子運転免許証のデータを編集する行政関係者であり、前記他のコンピュータリソースが、前記行政関係者が用いる電子運転免許証管理システムであることを特徴とする請求項 1 から 9 のいずれかに記載の個人データアプリケーション。

[請求項15] 前記個人データアプリケーションファイルが、個人の電子パスポートファイルであり、前記個人データアプリケーションが、前記個人の出入国管理サービスアプリケーションであり、前記他者が前記電子パスポートのデータを編集する出入国管理を行う行政関係者であり、前記他のコンピュータリソースが、前記出入国管理の行政関係者が用いる電子パスポート管理システムであることを特徴とする請求項 1 から 9 のいずれかに記載の個人データアプリケーション。

[請求項16] 個人データを取り扱う個人データアプリケーションの制御方法であって、

前記個人データアプリケーションで利用される各々の個人データアプリケーションファイルに対して、前記個人データアプリケーションで前記個人データアプリケーションファイルを開くためのオープン暗証コードと、前記個人データアプリケーションで開いた前記個人データアプリケーションファイルを正常終了して閉じるためのクローズ暗証コードを設定し、

前記オープン暗証コードの入力を受けて前記個人データアプリケーションファイルを開くアプリケーションファイル開錠処理と、

開かれた前記個人データアプリケーションファイルに対して、他のコンピュータリソースを経由した他者によるデータ編集を受け付けるアプリケーションファイル編集処理と、

前記クローズ暗証コードの入力を受けて、前記個人データアプリケーションファイルに対する前記アプリケーションファイル編集処理に

よるデータ編集内容を確定し、正常終了して閉じるアプリケーション
ファイル閉錠処理を行うことを特徴とする個人データアプリケーション
ファイルの制御方法。