(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2016-535902
(P2016-535902A)
(43)公表日　平成28年11月17日(2016.11.17)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/62	(2013.01)	G06F	21/62	３１８	５Ｊ１０４
H04L 9/32	(2006.01)	H04L	9/00	６７３Ａ	
G06F 21/44	(2013.01)	H04L	9/00	６７３Ｂ	
G06F 21/31	(2013.01)	G06F	21/44		
		G06F	21/31		

審査請求 未請求　予備審査請求 未請求　（全 51 頁）

(21)出願番号　特願2016-537389 (P2016-537389)
(86)(22)出願日　平成26年8月29日 (2014.8.29)
(85)翻訳文提出日　平成28年4月18日 (2016.4.18)
(86)国際出願番号　PCT/GB2014/052640
(87)国際公開番号　WO2015/028824
(87)国際公開日　平成27年3月5日 (2015.3.5)
(31)優先権主張番号　1315420.8
(32)優先日　平成25年8月29日 (2013.8.29)
(33)優先権主張国　英国 (GB)

(71)出願人　516060543
リバティ　ヴォールツ　リミテッド
イギリス　エヌ１２　Ｏディーアール　ロンドン　フィンチリー　ウッドベリー　グローブ　２　１階
(74)代理人　110000556
特許業務法人　有古特許事務所
(72)発明者　ジョンストン，　クリストファー　イアン
イギリス　エスダブリュ１９　５イージー　ロンドン　ウィンブルドン　ヴィレッジ　ハイ　ストリート　８７
(72)発明者　ルデュック，　ミシェル
フランス　エフ－１３５３０　トレ　ロティスモン　カバシュード　２７

最終頁に続く

(54)【発明の名称】複数のデバイスからデータにアクセスするためのシステム

(57)【要約】
あるデバイスにおいてデータにアクセスする方法であって、データは、デバイスから遠隔に、または取外し可能なストレージに記憶され、本方法は、下記のステップ、即ち、（ｉ）デバイスから、データへアクセスする要求を送信するステップであって、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、（ｉｉ）少なくとも部分的に識別コードに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、デバイスによるデータへのアクセスを許可または拒絶するステップと、を含む。
【選択図】　図3

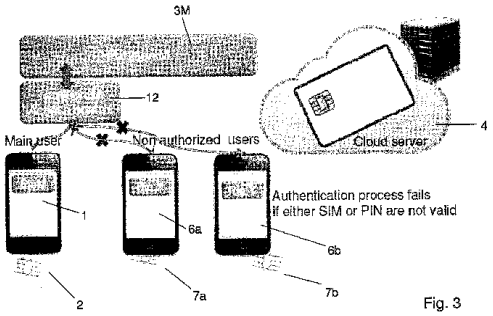


Fig. 3

【特許請求の範囲】
【請求項１】
デバイスにおいてデータにアクセスする方法であって、前記データは、前記デバイスから遠隔に記憶され、または取外し可能なストレージに記憶され、前記方法は、下記のステップ、即ち、
（i）前記デバイスから、前記データへアクセスする要求を送信するステップであって、前記要求は、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、
（ii）少なくとも部分的に前記識別コードに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、
（iii）その結果に応じて、前記デバイスによる前記データへのアクセスを許可または拒絶するステップと、を含む方法。
【請求項２】
前記データは、クラウドに記憶される、請求項1に記載の方法。
【請求項３】
前記要求は、前記デバイスにおいて入力されるパスコードまたはPINを含み、ステップ（ii）は、前記パスコードまたはPINに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含む、請求項1または請求項2に記載の方法。
【請求項４】
前記要求は、前記デバイスのユーザに固有の何かを表すデータを含み、ステップ（ii）は、前記デバイスの前記ユーザに固有の何かを表す前記データに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含み、かつ／または、
前記要求は、ロケーションを含むデータを含み、ステップ（ii）は、前記ロケーションに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含み、かつ／または、
前記要求は、時間を含むデータを含み、ステップ（ii）は、前記時間に基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含み、かつ／または、
前記要求は、前記ユーザがグループの一部であることを示すデータを含み、ステップ（ii）は、前記データへのアクセスが許可されるべきか、拒絶されるべきかを、前記グループの他のメンバが前記データにアクセスしているかどうかに基づいて検証することを含む、請求項1乃至3のいずれかに記載の方法。
【請求項５】
前記デバイスの前記ユーザに固有の何かを表す前記データは、例えば、前記ユーザに関する遺伝学的および／または生体測定的情報を表すデータを含む、請求項4に記載の方法。
【請求項６】
前記セキュアエレメントまたはメモリカードは、前記デバイスに関連づけられるSIM、仮想SIM、SIMソフトウェア、TPM、SE、TEE、マイクロSD、メモリカード、USBキーまたはスマートカードである、請求項1乃至5のいずれかに記載の方法。
【請求項７】
前記データは、前記デバイスに関連づけられるパーティションに記憶され、かつ前記要求は、前記パーティションを指定するデータを含み、かつ好ましくは、前記データは、第三者サービスへの接続を容易にする、請求項1乃至6のいずれかに記載の方法。
【請求項８】
前記パーティションを指定する前記データは、
PINまたはパスコード、および、
前記デバイスの前記ユーザに固有の何かを表すデータ、
のうちの一方または双方を含む、請求項7に記載の方法。

【請求項９】
前記デバイスの前記ユーザに固有の何かを表す前記データは、前記ユーザに関する遺伝学的および／または生体測定的情報を表すデータを含む、請求項8に記載の方法。
【請求項１０】
前記デバイスは、電話、タブレット、ラップトップコンピュータ、デスクトップコンピュータ、テレビ、セット・トップ・ボックス、カメラ、車、ゲーム機、メガネ、腕時計、クロームキャスト、スマートメータまたは他の、リモートデバイスとのデータ送受信が可能な任意のデバイスである、請求項1乃至9のいずれかに記載の方法。
【請求項１１】
前記方法は、ステップ（ｉ）－（ｉｉｉ）に先行して、
セキュアエレメントまたはメモリカードの識別コードを前記データに登録することを含む、請求項1乃至10のいずれかに記載の方法。
【請求項１２】
2つ以上のセキュアエレメントまたはメモリカードの識別コードは、前記データに関連づけられる、請求項11に記載の方法。
【請求項１３】
デバイスからデータへのアクセスを制御する方法であって、前記データは、前記デバイスから遠隔に、または取外し可能なストレージに記憶され、前記方法は、下記のステップ、即ち、
（ｉ）前記デバイスから、前記データへアクセスする要求を受信するステップであって、前記要求は、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、
（ｉｉ）少なくとも部分的に前記識別コードに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、
（ｉｉｉ）その結果に応じて、前記データへの前記デバイスのアクセスを許可または拒絶するステップと、を含む方法。
【請求項１４】
請求項1乃至12のいずれかに記載の方法をさらに含む、請求項13に記載の方法。
【請求項１５】
前記方法は、データ・アクセス・コントローラによって実行される、請求項13または請求項14に記載の方法。
【請求項１６】
前記データ・アクセス・コントローラは、前記デバイスから遠隔に存在する、請求項15に記載の方法。
【請求項１７】
デバイスから遠隔に、または取外し可能なストレージに記憶されるデータへのアクセスを制御するためのデータ・アクセス・コントローラであって、前記データ・アクセス・コントローラは、下記のステップ、即ち、
（ｉ）前記デバイスから前記データへアクセスする要求を受信するステップであって、前記要求は、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、
（ｉｉ）少なくとも部分的に前記識別コードに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、
（ｉｉｉ）その結果に応じて、前記データへの前記デバイスのアクセスを許可または拒絶するステップと、を実行するように構成される、データ・アクセス・コントローラ。
【請求項１８】
前記データ・アクセス・コントローラは、前記データへのアクセスを希望するデバイスから遠隔に存在する、請求項17に記載のデータ・アクセス・コントローラ。
【請求項１９】
デバイスと、前記デバイスから遠隔に、または取外し可能なストレージに記憶されるデ

ータへの前記デバイスからのアクセスを制御するためのデータ・アクセス・コントローラとを備えるシステムであって、前記デバイスは、前記データへのアクセス要求を前記データ・アクセス・コントローラへ送信するように構成され、前記要求は、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含み、かつ前記データ・アクセス・コントローラは、少なくとも部分的に前記識別コードに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証し、かつその結果に応じて、前記データへの前記デバイスのアクセスを許可または拒絶するように構成される、システム。

【請求項２０】

デバイスから遠隔に、または取外し可能なストレージに記憶されるデータへのアクセスを制御するためのコンピュータプログラムであって、前記プログラムは、プロセッサによって実行されると、下記のステップ、即ち、

（ｉ）前記デバイスから、前記データへアクセスする要求を受信するステップであって、前記要求は、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、

（ｉｉ）少なくとも部分的に前記識別コードに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、

（ｉｉｉ）その結果に応じて、前記データへの前記デバイスのアクセスを許可または拒絶するステップと、を実行するように構成される、コンピュータプログラム。

【請求項２１】

デバイスがアクセスコントローラを介してデータにアクセスし得るように、前記デバイスを前記アクセスコントローラに登録する方法であって、前記データは、デバイスから遠隔に、または取外し可能なストレージに記憶され、前記方法は、

データへアクセスするためにデバイスを登録する要求を送信することであって、前記要求は、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むことと、

前記データへのアクセスが許可されるべきかどうかをチェックすることと、

アクセスが許可されるべきものであれば、前記識別コードを前記アクセスされるべきデータに対して登録すること、を含む方法。

【請求項２２】

前記要求は、2または3ファクタ認証コードを含む、請求項21に記載の方法。

【請求項２３】

前記2または3ファクタ認証コードは、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コード、およびPINまたはパスコードおよびユーザに固有の何かを表すデータのうちの一方または双方に基づくものである、請求項22に記載の方法。

【請求項２４】

前記要求は、eメールまたはSMSの形式である、請求項21乃至23のいずれかに記載の方法。

【請求項２５】

前記要求に関連する情報を管理者デバイスへ送信することをさらに含み、前記管理者デバイスは、好ましくは、前記データへのアクセスが認可されるべきか否かを決定する、請求項21乃至24のいずれかに記載の方法。

【請求項２６】

デバイスがアクセスコントローラを介してデータにアクセスし得るように、前記デバイスを前記アクセスコントローラに登録する方法であって、前記データは、前記デバイスから遠隔に、または取外し可能なストレージに記憶され、前記方法は、

データへアクセスするためにデバイスを登録する要求を受信することであって、前記要求は、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むことと、

前記データへのアクセスが許可されるべきかどうかをチェックすることと、

アクセスが許可されるべきものであれば、前記識別コードを前記アクセスされるべきデータに対して登録すること、を含む方法。

【請求項２７】

データへのアクセスに対するデバイスの登録を制御するためのデータ・アクセス・コントローラであって、前記コントローラは、下記のステップ、即ち、

データへアクセスするためにデバイスを登録する要求を受信するステップであって、前記要求は、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、

前記データへのアクセスが許可されるべきかどうかをチェックするステップと、

アクセスが許可されるべきものであれば、前記識別コードを前記アクセスされるべきデータに対して登録するステップと、を実行するように構成される、データ・アクセス・コントローラ。

【請求項２８】

デバイスと、データへのアクセスに対するデバイスの登録を制御するためのデータ・アクセス・コントローラとを備えるシステムであって、前記コントローラは、下記のステップ、即ち、

前記デバイスから、データへアクセスするために前記デバイスを登録する要求を受信するステップであって、前記要求は、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、

前記データへのアクセスが許可されるべきかどうかをチェックするステップと、

アクセスが許可されるべきものであれば、前記識別コードを前記アクセスされるべきデータに対して登録するステップと、を実行するように構成される、システム。

【請求項２９】

データへのアクセスに対するデバイスの登録を制御するためのコンピュータプログラムであって、前記プログラムは、プロセッサによって実行されると、下記のステップ、即ち、

前記デバイスから、データへアクセスするために前記デバイスを登録する要求を受信するステップであって、前記要求は、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、

前記データへのアクセスが許可されるべきかどうかをチェックするステップと、

アクセスが許可されるべきものであれば、前記識別コードを前記アクセスされるべきデータに対して登録するステップと、を実行するように構成される、コンピュータプログラム。

【請求項３０】

デバイスにおいてデータにアクセスする方法であって、前記データは、前記デバイスから遠隔に、または取外し可能なストレージに記憶され、前記方法は、

前記デバイスにおいて、前記データにアクセスする勧誘を受信することであって、前記勧誘は、パスワード、コードまたはPINを含むことと、

前記デバイスから、前記データにアクセスする要求を送信することであって、前記要求は、前記パスワード、コードまたはPINを含むことと、

少なくとも部分的に前記パスワード、コードまたはPINに基づいて、前記データへのアクセスが許可されるべきか拒絶されるべきかを検証することと、

その結果に応じて、前記データへの前記デバイスのアクセスを許可または拒絶すること、を含む方法。

【請求項３１】

前記パスワード、コードまたはPINは、乱数発生器によって発生される、請求項30に記載の方法。

【請求項３２】

前記パスワード、コードまたはPINは、ワンタイムパスワードである、請求項30または請求項31に記載の方法。

【請求項３３】
前記パスワード、コードまたはPINは、指定される時間期間でのみ有効である、請求項30、請求項31または請求項32に記載の方法。
【請求項３４】
前記パスワード、コードまたはPINは、前記データへのアクセスを制御するデバイスによって発生される、請求項30乃至33のいずれかに記載の方法。
【請求項３５】
前記方法は、第1のデバイスによって、第2のデバイスがデータにアクセスすることを許可する方法であり、前記データは、前記第1および第2のデバイスから遠隔に記憶され、前記勧誘は、前記第1のデバイスから前記第2のデバイスへ送信され、前記データにアクセスする前記要求は、前記第2のデバイスから送信され、かつ前記データへのアクセスは、前記第2のデバイスに対して許可または拒絶される、請求項30乃至34のいずれかに記載の方法。
【請求項３６】
前記パスワード、コードまたはPINは、前記第1のデバイスにおいて発生される、請求項35に記載の方法。
【請求項３７】
前記パスワード、コードまたはPINは、前記第1および第2のデバイスの双方から遠隔で発生される、請求項35に記載の方法。
【請求項３８】
前記方法は、さらに、前記発生されるパスワード、コードまたはPINを前記アクセスされるべきデータに登録することを含む、請求項36または請求項37に記載の方法。
【請求項３９】
前記発生されるパスワード、コードまたはPINを前記アクセスされるべきデータに登録する前記ステップは、前記第1のデバイスが、前記発生されるパスワード、コードまたはPINを登録する前に、さらなるデバイスを前記データへアクセスするよう勧誘することを許可されているか検証することを含む、請求項36に従属する場合の請求項38に記載の方法。
【請求項４０】
前記方法は、さらに、前記第1のデバイスから、前記パスワード、コードまたはPINの生成を求める要求を送信することを含み、前記生成されるべきパスワード、コードまたはPINは、前記第1のデバイスがさらなるデバイスをる前記データへアクセスするよう勧誘することを許可されているという検証がなされた後にのみ生成される、請求項37に従属する場合の請求項38に記載の方法。
【請求項４１】
前記第1のデバイスがさらなるデバイスを前記データへアクセスすよう勧誘することを許可されていることの前記検証ステップは、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードのような前記デバイスに関連づけられる識別コードを検証することを含む、請求項40に記載の方法。
【請求項４２】
前記第1のデバイスがさらなるデバイスを前記データへアクセスするよう勧誘することを許可されていることの前記検証ステップは、さらに、前記第1のデバイスから送信される、パーティションを指定するデータを検証することを含む、請求項41に記載の方法。
【請求項４３】
前記パーティションを指定する前記データは、
PINまたはパスコード、および、
前記デバイスの前記ユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等のデータ、
のうちの一方または双方を含む、請求項42に記載の方法。
【請求項４４】
デバイスにおける、データへのアクセスを許可する方法であって、前記データは、前記

デバイスから遠隔に、または取外し可能なストレージに記憶され、前記方法は、
前記デバイスへ、前記データにアクセスする勧誘を送信することであって、前記勧誘は、パスワード、コードまたはPINを含むことと、
前記デバイスから、前記データにアクセスする要求を送信することであって、前記要求は、前記パスワード、コードまたはPINを含むことと、
少なくとも部分的に前記パスワード、コードまたはPINに基づいて、前記データへのアクセスが許可されるべきか拒絶されるべきかを検証することと、
その結果に応じて、前記データへの前記デバイスのアクセスを許可または拒絶すること、を含む方法。

【請求項４５】
第1のデバイスと、第2のデバイスと、データ・アクセス・コントローラとを備えるシステムであって、前記第1のデバイスは、前記第2のデバイスがデータへアクセスするよう勧誘するように構成され、前記データは、前記第2のデバイスから遠隔に、または取外し可能なストレージに記憶され、
前記第1のデバイスは、前記第2のデバイスへ、前記データへのアクセスの勧誘を送信するように構成され、前記勧誘は、パスワード、コードまたはPINを含み、
前記第2のデバイスは、前記データにアクセスする要求を送信するように構成され、前記要求は、前記パスワード、コードまたはPINを含み、かつ、
前記データ・アクセス・コントローラは、少なくとも部分的に前記パスワード、コードまたはPINに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証し、かつその結果に応じて、前記第2のデバイスによる前記データへのアクセスを許可または拒絶するように構成される、システム。

【請求項４６】
デバイスにおいてデータにアクセスする方法であって、前記データは、前記デバイスから遠隔に、または取外し可能なストレージに記憶され、前記方法は、下記のステップ、即ち、
（i）前記デバイスから、前記データにアクセスする要求を送信するステップであって、前記要求は、前記要求に関連するデータを含むステップと、
（ii）少なくとも部分的に前記データに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、
（iii）その結果に応じて、かつ前記データにアクセスする少なくとも1つのさらなるデバイスが存在する場合にのみ、前記デバイスによる前記データへのアクセスを許可するステップと、を含む方法。

【請求項４７】
請求項1乃至28のいずれかに記載の特徴をさらに含む、請求項46に記載の方法。

【請求項４８】
前記さらなるデバイスは、前記データに登録される管理者デバイスである、請求項46または請求項47に記載の方法。

【請求項４９】
ステップ（iii）に先行して、少なくとも1つのさらなるデバイスが前記データにアクセスしているかどうかをチェックすることをさらに含む、請求項46乃至48のいずれかに記載の方法。

【請求項５０】
デバイスにおいてデータへのアクセスを制御する方法であって、前記データは、前記デバイスから遠隔に、または取外し可能なストレージに記憶され、前記方法は、下記のステップ、即ち、
（i）前記デバイスから、前記データへアクセスする要求を受信するステップであって、前記要求は、前記要求に関連するデータを含むステップと、
（ii）少なくとも部分的に前記データに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、

（iii）その結果に応じて、かつ前記データにアクセスする少なくとも1つのさらなるデバイスが存在する場合にのみ、前記デバイスによる前記データへのアクセスを許可するステップと、を含む方法。

【請求項５１】

デバイスにおいてデータへのアクセスを制御するためのデータ・アクセス・コントローラであって、前記データは、前記デバイスから遠隔に、または取外し可能なストレージに記憶され、前記データ・アクセス・コントローラは、下記のステップ、即ち、

（i）前記デバイスから、前記データへアクセスする要求を受信するステップであって、前記要求は、前記要求に関連するデータを含むステップと、

（ii）少なくとも部分的に前記データに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、

（iii）その結果に応じて、かつ前記データにアクセスする少なくとも1つのさらなるデバイスが存在する場合にのみ、前記デバイスによる前記データへのアクセスを許可するステップと、を実行するように構成される、データ・アクセス・コントローラ。

【請求項５２】

前記データ・アクセス・コントローラは、ステップ（iii）の実行に先行して、少なくとも1つのさらなるデバイスが前記データにアクセスしているかどうかをチェックするように構成される、請求項51に記載のデータ・アクセス・コントローラ。

【請求項５３】

デバイスと、デバイスにおいてデータへのアクセスを制御するためのデータ・アクセス・コントローラとを備えるシステムであって、前記データは、前記デバイスから遠隔に、または取外し可能なストレージに記憶され、前記データ・アクセス・コントローラは、下記のステップ、即ち、

（i）前記デバイスから、前記データへアクセスする要求を受信するステップであって、前記要求は、前記要求に関連するデータを含むステップと、

（ii）少なくとも部分的に前記データに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、

（iii）その結果に応じて、かつ前記データにアクセスする少なくとも1つのさらなるデバイスが存在する場合にのみ、前記デバイスによる前記データへのアクセスを許可するステップと、を実行するように構成される、システム。

【請求項５４】

前記デバイスは、前記データにアクセスする要求を前記データ・アクセス・コントローラへ送信するように構成される、請求項53に記載のシステム。

【請求項５５】

前記データ・アクセス・コントローラは、ステップ（iii）の実行に先行して、少なくとも1つのさらなるデバイスが前記データにアクセスしているかどうかをチェックするように構成される、請求項53または請求項54に記載のシステム。

【請求項５６】

デバイスから遠隔に、または取外し可能なストレージに記憶されるデータへのアクセスを制御するためのコンピュータプログラムであって、前記プログラムは、プロセッサによって実行されると、下記のステップ、即ち、

（i）前記デバイスから、前記データへアクセスする要求を受信するステップであって、前記要求は、前記要求に関連するデータを含むステップと、

（ii）少なくとも部分的に前記データに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、

（iii）その結果に応じて、かつ前記データにアクセスする少なくとも1つのさらなるデバイスが存在する場合にのみ、前記デバイスによる前記データへのアクセスを許可するステップと、を実行するように構成される、コンピュータプログラム。

【請求項５７】

前記プログラムは、さらに、ステップ（iii）の実行に先行して、少なくとも1つのさら

なるデバイスが前記データにアクセスしているかどうかをチェックするように構成される、請求項56に記載のプログラム。

【請求項５８】

デバイスにおいてデータにアクセスする方法であって、前記データは、前記デバイスから遠隔に、または取外し可能なストレージに、または前記デバイス自体に記憶され、前記方法は、下記のステップ、即ち、

（ｉ）前記データにアクセスする要求を送信するステップであって、前記要求は、前記デバイスに関連づけられる識別コードと、

PINまたはパスコード、および、

前記デバイスのユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等のデータ、

のうちの一方または双方と、を含むステップと、

（ｉｉ）前記識別コードおよびPINまたはパスコードおよび／または前記ユーザに固有の何かを表すデータに基づいて、前記データへのアクセスが許可されるべきか拒絶されるべきかを検証するステップと、

（ｉｉｉ）その結果に応じて、前記デバイスによる前記データへのアクセスを許可または拒絶するステップと、を含む方法。

【請求項５９】

前記データは、パーティションに記憶される、請求項58に記載の方法。

【請求項６０】

前記PINまたはパスコードおよび／または前記デバイスのユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等の前記データは、ユーザがアクセスすることを求めているデータに関連づけられ、かつこのデータを識別することができる、請求項59に記載の方法。

【請求項６１】

デバイスにおいて、データへのアクセスを制御する方法であって、前記データは、前記デバイスから遠隔に、または取外し可能なストレージに、または前記デバイス自体に記憶され、前記方法は、下記のステップ、即ち、

（ｉ）前記データにアクセスする要求を受信するステップであって、前記要求は、前記デバイスに関連づけられる識別コードと、PINまたはパスコード、および前記デバイスのユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等のデータ、のうちの一方または双方と、を含むステップと、

（ｉｉ）前記識別コードおよび前記PINまたはパスコードおよび／または前記ユーザに固有の何かを表すデータに基づいて、前記データへのアクセスが許可されるべきか拒絶されるべきかを検証するステップと、

（ｉｉｉ）その結果に応じて、前記デバイスによる前記データへのアクセスを許可または拒絶するステップと、を含む方法。

【請求項６２】

デバイスにおいて、データへのアクセスを制御するためのデータ・アクセス・コントローラであって、前記データは、前記デバイスから遠隔に、取外し可能なストレージに、または前記デバイス自体に記憶され、前記データ・アクセス・コントローラは、下記のステップ、即ち、

（ｉ）前記データにアクセスする要求を受信するステップであって、前記要求は、前記デバイスに関連づけられる識別コードと、PINまたはパスコード、および前記デバイスのユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等のデータ、のうちの一方または双方と、を含むステップと、

（ｉｉ）前記識別コードおよび前記PINまたはパスコードおよび／または前記ユーザに固有の何かを表すデータに基づいて、前記データへのアクセスが許可されるべきか拒絶されるべきかを検証するステップと、

（ｉｉｉ）その結果に応じて、前記デバイスによる前記データへのアクセスを許可または

拒絶するステップと、を実行するように構成される、データ・アクセス・コントローラ。
【請求項６３】
デバイスにおいて、データへのアクセスを制御するためのコンピュータプログラムであって、前記データは、前記デバイスから遠隔に、取外し可能なストレージに、または前記デバイス自体に記憶され、前記プログラムは、プロセッサによって実行されると、下記のステップ、即ち、
（ｉ）前記データにアクセスする要求を受信するステップであって、前記要求は、前記デバイスに関連づけられる識別コードと、PINまたはパスコード、および前記デバイスのユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等のデータ、のうちの一方または双方と、を含むステップと、
（ｉｉ）前記識別コードおよび前記PINまたはパスコードおよび／または前記ユーザに固有の何かを表すデータに基づいて、前記データへのアクセスが許可されるべきか拒絶されるべきかを検証するステップと、
（ｉｉｉ）その結果に応じて、前記デバイスによる前記データへのアクセスを許可または拒絶するステップと、を実行するように構成される、コンピュータプログラム。
【請求項６４】
デバイスからクラウドベースまたはウェブベースの第三者サービスにアクセスする方法であって、前記方法は、下記のステップ、即ち、
（ｉ）前記デバイスから、前記デバイスに関連づけられるクラウドベースのパーティションへ要求を送信するステップであって、前記パーティションは、前記第三者サービスへの接続を容易にするためのデータを含み、前記要求は、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、
（ｉｉ）少なくとも部分的に前記識別コードに基づいて、前記パーティションへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、
（ｉｉｉ）その結果に応じて、前記デバイスによる前記パーティションへのアクセスを許可または拒絶するステップと、前記パーティションへのアクセスが許可された後に、
（ｉｖ）前記第三者サービスへ資格認証情報を送信するステップと、を含む方法。
【請求項６５】
前記要求は、前記デバイスにおいて入力されるパスコードまたはPINを含み、ステップ（ｉｉ）は、前記パスコードまたはPINに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含む、請求項64に記載の方法。
【請求項６６】
前記要求は、前記デバイスのユーザに固有の何かを表すデータを含み、ステップ（ｉｉ）は、前記デバイスのユーザに固有の何かを表すデータに基づいて、前記データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含み、
好ましくは、前記デバイスのユーザに固有の何かを表すデータは、前記ユーザに関する遺伝学的および／または生体測定的情報を表すデータを含む、請求項64または請求項65に記載の方法。
【請求項６７】
前記資格認証情報を送信する前記ステップは、
前記デバイスの前記セキュアエレメントまたはメモリカードと前記パーティションに関連づけられるセキュアエレメントとの間で相互的な認証プロセスを実行するステップと、
前記デバイスの前記セキュアエレメントまたはメモリカードと前記パーティションに関連づけられるセキュアエレメントとの間にセキュアなチャネルを生成するステップと、を含む、請求項64乃至66のいずれかに記載の方法。
【請求項６８】
前記資格認証情報を送信する前記ステップは、前記資格認証情報を、前記デバイスの前記セキュアエレメントまたはメモリカードから前記セキュアなチャネルを介して前記パーティションへ送信するステップを含み、

好ましくは、前記資格認証情報は、前記セキュアなチャネルを介する送信に先行して暗号化される、請求項67に記載の方法。

【請求項６９】

前記資格認証情報を送信する前記ステップは、

前記デバイスの前記セキュアエレメントまたはメモリカードと前記第三者サービスに関連づけられるセキュアエレメントとの間の相互的な認証プロセスを実行するステップと、

前記デバイスの前記セキュアエレメントまたはメモリカードと前記第三者サービスに関連づけられるセキュアエレメントとの間にセキュアなチャネルを生成するステップと、

前記資格認証情報を暗号化するステップと、

前記暗号化された資格認証情報を、前記デバイスの前記セキュアエレメントまたはメモリカードから前記セキュアなチャネルを介して前記第三者サービスに関連づけられる前記セキュアエレメントへ送信するステップと、を含む、請求項67または請求項68に記載の方法。

【請求項７０】

前記第三者サービスは、第三者サービスにアクセスするための特定のPINコードを要求し、かつ前記PINコードは、前記セキュアエレメントまたはメモリカードと前記第三者サービスに関連づけられる前記セキュアエレメントとの間に生成される前記セキュアなチャネルを介して送信される、請求項69に記載の方法。

【請求項７１】

第三者サービスにアクセスするための資格認証情報、および／または前記第三者サービスにより要求されるフォーム記入用データは、前記認証プロセスが成功裡に完了した後に自動的に提供される、請求項64乃至70のいずれかに記載の方法。

【請求項７２】

アプリケーションは、前記認証プロセスが成功裡に完了した後に前記第三者サービスにおいて自動的に開始される、請求項64乃至71のいずれかに記載のデータアクセス方法。

【請求項７３】

前記セキュアエレメントまたはメモリカードは、前記デバイスに関連づけられるSIM、仮想SIM、SIMソフトウェア、TPM、SE、TEE、マイクロSD、メモリカード、USBキーまたはスマートカードである、請求項64乃至72のいずれかに記載の方法。

【請求項７４】

前記資格認証情報は、前記パーティションに安全に記憶される、請求項64乃至73のいずれかに記載の方法。

【請求項７５】

前記資格認証情報は、前記デバイスの前記セキュアエレメントまたはメモリカードに安全に記憶され、かつ好ましくは、前記資格認証情報は、前記セキュアエレメントまたはメモリカードから前記パーティションへ供給される、請求項64乃至73のいずれかに記載の方法。

【請求項７６】

ユーザ・エンロールメント・プロセスを含み、これにより、前記ユーザは、前記第三者サービスの使用をエンロールし、前記ユーザ・エンロールメント・プロセスは、

前記第三者サービスにアクセスするための資格認証情報および／またはフォーム記入用データを収集するステップと、

前記資格認証情報および／またはフォーム記入用データを安全に記憶するステップと、を含む、請求項64乃至75のいずれかに記載の方法。

【請求項７７】

ユーザ・エンロールメント・プロセスを含み、これにより、前記ユーザは、前記第三者サービスの使用をエンロールし、前記ユーザ・エンロールメント・プロセスは、

前記相互的な認証プロセスを初期化するステップと、

前記第三者サービスを選択するステップと、を含む、請求項64乃至75のいずれかに記載の方法。

【請求項７８】

前記資格認証情報は、前記パーティションへのアクセスが許可された後に、前記パーティションによって自動的に生成される、請求項77に記載の方法。

【請求項７９】

前記自動的に生成される資格認証情報は、周期的に、または要求に応じて新しくされる、請求項78に記載の方法。

【請求項８０】

前記自動的に生成される資格認証情報は、他の手段によってサービスにアクセスする場合に使用される資格認証情報とは異なる、請求項78または請求項79に記載の方法。

【請求項８１】

前記自動的に生成される資格認証情報の精巧化および複雑さは、ユーザのセキュリティポリシに従って、または第三者サービスのセキュリティポリシに従って適合化される、請求項78、請求項79または請求項80に記載の方法。

【請求項８２】

前記セキュアエレメントまたはメモリカードには、複数のアプレットが記憶され、かつ各アプレットは、所定のアプレットに関連するサービスにアクセスするための前記資格認証情報を生成する前に、別個の認証プロセスを実行する、請求項64乃至81のいずれかに記載の方法。

【請求項８３】

前記資格認証情報は、ユーザIDおよび／またはパスワードを含む、請求項64乃至82のいずれかに記載の方法。

【請求項８４】

前記デバイスは、新しい資格認証情報を生成するため、または前記第三者サービスにアクセスするための資格認証情報を更新するために使用されるマスタデバイスである、請求項64乃至83のいずれかに記載の方法。

【請求項８５】

前記デバイスは、マスタデバイスとして作動し、さらなるデバイスも前記第三者サービスへアクセスできるようにし、アクセスコードが発生されて前記デバイス上に表示され、あるいはSMSまたはeメールによってユーザへ送信され、かつ前記ユーザにより、前記さらなるデバイスを用いて前記第三者サービスに関連づけられるウェブサイトへ入力され、

好ましくは、前記アクセスコードは、前記デバイス上で実行されるアプリケーションによって生成され、かつ／または前記アクセスコードには時間的制約がある、請求項64乃至84のいずれかに記載の方法。

【請求項８６】

さらなるデバイスを前記パーティションへ接続して、好ましくは前記パーティションのコンテンツおよび／または前記接続されるデバイスの資格認証情報を同期するステップを含む、請求項64乃至85のいずれかに記載の方法。

【請求項８７】

前記パーティションを識別しかつ／またはこれにアクセスするために要求される情報は、NFCタグまたは信号放出デバイスから読み取られ、好ましくは、前記信号放出デバイスは、Bluetooth、BLE、wifi、zigbee、NFC、GPSまたはISO14443デバイスであり、または、他の任意形式の非接触通信を利用する、請求項64乃至86のいずれかに記載の方法。

【請求項８８】

前記パーティションは、電話またはメッセージングサービスのための一意の識別子を記憶する、請求項64乃至87のいずれかに記載の方法。

【請求項８９】

前記電話またはメッセージングサービスは、モバイルフォン電話サービス、VOIPサービスまたはインスタント・メッセージング・サービスである、請求項88に記載の方法。

【請求項９０】
前記一意の識別子は、電話またはメッセージングサービス識別子へリンクされ、好ましくは、前記電話またはメッセージングサービス識別子は、ユーザ名および関連のパスワードまたは国内または国際電話番号である、請求項88または請求項89に記載の方法。
【請求項９１】
前記一意の識別子と前記電話またはメッセージングサービス識別子との間のマッピングは、前記デバイスの前記セキュアエレメントまたはメモリカードに記憶されても、前記パーティションに記憶されても、移動ネットワークのオペレータによって記憶されてもよい、請求項90に記載の方法。
【請求項９２】
特定のサービスに関連づけられる一意の識別子は、ユーザのロケーションに依存して起動される、請求項88乃至91のいずれかに記載の方法。
【請求項９３】
（iv）前記デバイスと前記リモートストレージまたは取外し可能なストレージとの間で相互的な認証プロセスを実行するステップと、
（v）前記デバイスと前記リモートストレージまたは取外し可能なストレージとの間にセキュアなチャネルを生成するステップと、
（vi）前記２つのデバイス間でデータを送信するステップと、をさらに含む、請求項1乃至12のいずれかに記載の方法。
【請求項９４】
前記認証は、2つ以上のファクタを含み、前記ファクタは、下記のリスト、即ち、
前記デバイスに関連づけられるスマートオブジェクト（メモリカードまたはセキュアエレメント）の識別コード、
パスコードまたはPIN、
遺伝学的または生体測定的識別データ、
ロケーション、
時刻、または、
別のメンバ（例えば、管理者）、または前記ユーザが属するグループが前記データにアクセスしているかどうか、
から選択される、請求項93に記載の方法。
【請求項９５】
前記認証は、2つのファクタを含み、前記ファクタは、
前記デバイスに関連づけられるスマートオブジェクト（メモリカードまたはセキュアエレメント）の識別コード、および、
パスコードまたはPIN、
である、請求項93に記載の方法。
【請求項９６】
デバイスによるクラウドベースまたはウェブベースの第三者サービスへのアクセスを制御する方法であって、前記方法は、下記のステップ、即ち、
（i）前記デバイスから前記デバイスに関連づけられるクラウドベースのパーティションへの要求を受信するステップであって、前記パーティションは、前記第三者サービスへの接続を容易にするためのデータを含み、前記要求は、前記デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、
（ii）少なくとも部分的に前記識別コードに基づいて、前記パーティションへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、
（iii）その結果に応じて、前記デバイスによる前記パーティションへのアクセスを許可または拒絶するステップと、前記パーティションへのアクセスが許可された場合に、
（iv）前記第三者サービスへ資格認証情報を送信するステップと、を含む方法。
【請求項９７】
請求項64乃至95のいずれかの特徴をさらに含む、請求項96に記載の方法。

【請求項９８】
デバイスによるクラウドベースまたはウェブベースの第三者サービスへのアクセスを制御するためのコンピュータプログラムであって、前記プログラムは、プロセッサによって実行されると、請求項96または請求項97に記載の方法を実行するように構成される、コンピュータプログラム。
【請求項９９】
デバイスからパーティションにアクセスする方法であって、
a. 前記パーティションと前記デバイスとの間で相互的な認証を実行するステップと、
b. 前記パーティションと前記デバイスとの間にセキュアなチャネルを生成するステップと、を含み、
前記認証は、2つ以上のファクタを含み、前記ファクタは、下記のリスト、即ち、
前記デバイスに関連づけられるスマートオブジェクト（メモリカードまたはセキュアエレメント）の識別コード、
パスコードまたはPIN、
遺伝学的または生体測定的識別データ、
ロケーション、
時刻、または、
別のメンバ（例えば、管理者）、またはユーザが属するグループがデータにアクセスしているかどうか、
から選択される方法。
【請求項１００】
アクセスすることは、前記パーティションを共有するステップ、生成するステップ、編集するステップまたは削除するステップを含む、請求項99に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、データアクセスの分野に関する。より具体的には、本発明は、複数のデバイスからデータにアクセスするためのシステムに関する。
【背景技術】
【０００２】
ユーザにクラウドベースのデータストレージを提供することは、技術上知られている。このクラウドベースのストレージは、複数のデバイスからアクセスされる場合がある。
【０００３】
例えば、Dropbox（商標）は、ユーザに、そのデータのためのクラウドベースのリモートストレージを提供するシステムである。データは、例えば携帯電話によって撮られる写真を含む場合がある。データが、携帯電話から例えばリモートストレージへアップロードされていれば、これは、インターネットへ接続されている、ラップトップまたはデスクトップコンピュータ等の他のデバイスからアクセスされる場合がある。記憶されたデータは、256-ビットAES暗号化で暗号化されていて、ユーザは、そのデータへのアクセスが認可される前に、ユーザの登録されたeメールアドレスおよびパスワードをウェブサイトを介して入力しなければならない。
【０００４】
しかしながら、このシステムに関わる1つの問題点は、ユーザのeメールアドレスおよびパスワードが第三者によって発見されれば、この第三者も記憶されたデータへ任意のデバイスからアクセスし得ることにある。したがって、1つ以上のデバイスからアクセスされ得る、より安全なリモート・ストレージ・システムが必要とされている。
【発明の概要】
【０００５】
本発明の第1の態様によれば、あるデバイスにおいてデータにアクセスする方法が提供されており、データは、デバイスから遠隔に、または取外し可能なストレージに記憶され

、本方法は、下記のステップ、即ち、（ｉ）デバイスから、データへアクセスする要求を送信するステップであって、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、（ｉｉ）少なくとも部分的に識別コードに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、デバイスによるデータへのアクセスを許可または拒絶するステップと、を含む。

【０００６】

したがって、データへのアクセスは、デバイスに関連づけられる正しい識別コードが提供される場合にのみ許可される。よって、無認可のデバイスは正しい識別コードを提供することができないという理由で、無認可デバイスによるデータへのアクセスを防止することができる。

【０００７】

先に述べたように、要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含む。しかしながら、識別コードは、要求に、変更された形式で、例えば、暗号化された形式で、かつ／または1つ以上のさらなるコード、データまたは情報と組み合わせて含まれてもよい。

【０００８】

アクセスされるべきデータには、メモリに記憶されることが可能なあらゆる形式のデータが含まれる。例えば、これには、1つ以上のデータファイル、データベース、アプリケーション、ソフトウェアおよび／またはサービスが含まれてもよい。サービスの幾つかの例については、後に論じる。

【０００９】

好ましくは、識別コードは、セキュアなチャネルを介して送信される。あるいは、または追加的に、識別コードは、暗号化されてもよい。これは、プロセスをより安全なものにすることができ、かつ識別コードが第三者によって傍受されかつ／または発見されることを防止する手助けをすることができる。

【００１０】

さらなる（追加的または代替的な）可能性は、デバイス側で、セキュアエレメントまたはメモリカードの識別コードおよびデバイスからの1つ以上の他のエレメントまたはコードに基づいてコードを生成することであると思われる。生成されるこのコードは、次に、特定のセッションのために送信される可能性もあり、かつその特定のセッションに関してのみ有効であってもよい。したがって、これは、傍受されたとしても、第三者にとって無用のものであると思われる。

【００１１】

データは、リムーバブル・ストレージ・デバイス、クラウドまたは他の形式のリモート・データ・ストレージに記憶されてもよい。例えば、データは、USBキー、ラップトップ、コンピュータサーバ（個人または法人）、コンピュータネットワーク（個人または法人）、タブレットまたは電話に記憶される可能性もある。

【００１２】

要求は、デバイス側で入力されるパスコードまたはPINも含んでもよく、ステップ（ｉｉ）は、パスコードまたはPINに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含んでもよい。このように、データにアクセスするためには、2ファクタ認証が要求されてもよい。

【００１３】

パスコードまたはPINは、（まず）デバイスに関連づけられるセキュアエレメントまたはメモリカード（例えば、SIMまたは仮想SIM）によって検証されてもよい。

【００１４】

あるいは（または追加的に）、パスコードまたはPINは、デバイスから遠隔的に、例えば、データへのアクセスを制御するように構成されるアクセスコントローラにおいて、検証されてもよい。

【００１５】
パスコードまたはPINがセキュアエレメントまたはメモリカードによって検証される場合、この検証の結果は、好ましくは、例えばアクセスコントローラへ、安全かつ保護された方式で、例えばセキュアなチャネルを介して転送される。例えば、結果は、証明、暗号化コード、セッションコードまたは暗号化されたセッションコードの形式で転送される可能性もある。好ましくは、検証の結果は、検証が成功裡に行われた場合、即ち、正しいパスコードまたはPINが入力された場合、にのみ転送される。
【００１６】
パスコードまたはPINが、デバイスから遠隔的に、例えばアクセスコントローラにおいて検証される場合、パスコードまたはPINは、例えばアクセスコントローラへ、安全かつ／または保護された方式で転送されることが好ましい。例えば、パスコードまたはPINは、セキュアなチャネルを介して、かつ／または転送前にパスコードまたはPINを暗号化することによって、転送される可能性もある。
【００１７】
あるいは、または追加的に、要求は、デバイスのユーザに固有の何かを表すデータを含んでもよく、よってステップ（ii）は、デバイスのユーザに固有の何かを表すデータに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含んでもよい。このように、データへアクセスするためには、2ファクタまたは3ファクタ認証が要求されてもよく、かつ認証されたユーザのみが、データへのアクセスを認可されてもよい。
【００１８】
デバイスのユーザに固有の何かを表すデータは、ユーザに関する遺伝学的および／または生体測定的情報を表すデータ、例えば指紋または虹彩データ等、を含んでもよい。
【００１９】
認証形式としては、PINおよび／またはデバイスのユーザに固有の何かを表すデータを用いる認証（識別コードを用いる2ファクタまたは3ファクタ認証）の代わりに、またはこれに追加して、次のようなものが可能である。
【００２０】
要求は、ロケーション（即ち、ユーザがデータにアクセスしようとしている起点場所）を含むデータを含んでもよく、ステップ（ii）は、ロケーションに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含んでもよい。
【００２１】
要求は、時間（即ち、ユーザがデータにアクセスしようとしている時刻）を含むデータを含んでもよく、よってステップ（ii）は、時間に基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含んでもよい。
【００２２】
要求は、ユーザがグループの一部であることを指すデータを含んでもよく、ステップ（ii）は、データへのアクセスが許可されるべきか、拒絶されるべきかを、グループの別のメンバ（例えば、管理者）がデータにアクセスしているかどうかに基づいて検証することも含んでもよい。
【００２３】
セキュアエレメントまたはメモリカードは、例えば、「スマートオブジェクト」、または、それ自体も理想的には安全かつ改竄防止的である一意の識別コードを有する安全かつ改竄防止的なハードウェアデバイスである。セキュアエレメントまたはメモリカードは、例えば、SIM、仮想SIM、SIMソフトウェア、TPM（トラステッド・プラットフォーム・モジュール）、SE（セキュアエレメント）、TEE（トラステッドエグゼキューション環境）、マイクロSD、メモリカード、USBキーまたはスマートカードである可能性もある。
【００２４】
先に述べたように、セキュアエレメントの一般的な一例は、SIMカードである。SIMカードは、全てのGSM移動体デバイス、およびスマートフォンに備えられている。しかしなが

ら、SIMカードは、電話網によって備えられ、よって、（アプレットのSIMへのダウンロード、またはSIMの修正が容易ではない、という意味で）容易にはアクセスできない。さらに、デバイスのオペレーティングシステムは、SIMとインタフェースするためのソフトウェアツールキットを有していない場合がある。前述の欠点を克服するために、デバイス上へアプリケーションとしてロードされることが可能な仮想SIM（ソフトウェアSIM）をダウンロードすることが可能である。仮想SIMは、物理SIMのように動作するが、これは、仮想SIMがアプレットを受信して処理することができ、かつアプレット、資格認証情報、キーおよびアルゴリズム、他を安全に記憶できることを意味する。

【００２５】

セキュアエレメントまたはメモリカードは、あらゆるローカル、リモートまたは取外し可能形式のメモリであってもよい。

【００２６】

セキュアエレメントまたはメモリカードの識別コードは、好ましくは、例えばセキュアエレメントまたはメモリカード内のセーフボックスにおいて良好に保護されかつ記憶される。

【００２７】

本発明の好適な実施形態において、セキュアエレメントまたはメモリカードは、セキュアなチャネルを生成するために、かつ／または識別コードおよび／またはPINまたはパスコードを暗号化するために使用される。

【００２８】

データは、デバイスに関連づけられるパーティション、例えばメモリのパーティション、に記憶されてもよく、かつ要求は、パーティションを指定する、例えばアクセスされるべきパーティションを指定するデータを含んでもよい。

【００２９】

セキュアなチャネルは、セキュアエレメントまたはメモリカードとパーティションとの間に生成されてもよく、よって次に、データ、ファイル、資格認証情報またはデータをファイルする他の形式をデバイスとパーティションとの間で転送するために使用されることが可能である。

【００３０】

したがって、本方法は、（ｉｖ）デバイスとリモートストレージまたは取外し可能なストレージとの間で相互的な認証プロセスを実行するステップと、（ｖ）デバイスとリモートストレージまたは取外し可能なストレージとの間にセキュアなチャネルを生成するステップと、を含んでもよい。

【００３１】

認証は、2つ以上のファクタを含んでもよく、これらのファクタは、下記のリストから選択される。

【００３２】

デバイスに関連づけられるスマートオブジェクト（メモリカードまたはセキュアエレメント）の識別コード、
パスコードまたはPIN、
遺伝学的または生体測定的識別データ、
ロケーション、
時刻、または、
別のメンバ（例えば、管理者）、またはユーザが属するグループがデータにアクセスしているかどうか。

【００３３】

デバイスは、パーティションを識別してアクセスするために、NFC（近距離無線通信）タグ、生体センサ／リーダまたは信号放出デバイスからコードを読み取ってもよい。NFCタグ、生体センサ／リーダまたは信号放出デバイスは、デバイスへ、（そうでなければユーザによって入力される必要があると思われる）パーティションを選択しかつ最終的にこ

れを開くために必要な情報を提供してもよい。

【００３４】

信号放出デバイスは、Bluetooth（登録商標）、BLE（低電力ブルートゥース（登録商標））、wifi、zigbee、NFC、GPSまたはISO14443デバイスであっても、他の任意の形式の非接触通信を利用するデバイスであってもよい。

【００３５】

パーティションは、第三者のウェブベースまたはクラウドベースのサービス（銀行が提供するインターネットバンキング、または物流会社が提供する荷物追跡）への接続を容易にするためのデータを記憶してもよい。

【００３６】

パーティションを指定するデータは、PINまたはパスコード、およびデバイスのユーザに固有の何かを表すデータ、のうちの一方または双方を含む可能性もある。デバイスのユーザに固有の何かを表すデータは、例えば、ユーザに関する遺伝学的および／または生体測定的情報を表すデータを含む可能性もある。

【００３７】

デバイスは、電話（移動体または固定式）、スマートフォン、タブレット、ラップトップコンピュータ、デスクトップコンピュータ、テレビ、セット・トップ・ボックス、カメラ、車、ゲーム機、メガネ、腕時計、クロームキャスト、（例えば、建物における電気、ガスまたは水道消費量を測定するための）スマートメータ、宝石類、乗車カード、バンクカード、ATM機、衣料品、スポーツ用品、Eリーダ、双眼鏡、MP3プレーヤ、手持ち式ゲーム機、飛行機、列車、自転車、ボートまたはバス等の乗り物、EPO、台所用品、鏡、ハンドバッグ、財布、帽子、乳母車、Hi-fiまたは他のミュージックプレーヤまたはラジオ、またはリモートデバイスまたは取外し可能デバイスとのデータ送受信が可能な、またはリモートデバイスまたは取外し可能デバイスとのデータ送受信が可能な関連手段を有する、他の任意のデバイスであってもよく、または、デバイスにはこれらが含まれてもよい。

【００３８】

デバイス、または好ましくはセキュアエレメントまたはメモリカードには、好ましくは、データにアクセスするためのデータ・アクセス・ソフトウェア・コードがインストールされている。好ましくは、データ・アクセス・ソフトウェア・コードをインストールするために、デバイスは、例えば、少なくともセキュアエレメントまたはメモリカードの識別コードに関連する情報を提示することによって、システムに登録しなければならない。

【００３９】

本方法は、好ましくは、ステップ（ｉ）－（ｉｉｉ）に先行して、セキュアエレメントまたはメモリカードの識別コード、またはこれに基づくコードまたは証明をデータに登録することを含む。

【００４０】

2つ以上のセキュアエレメントまたはメモリカードの識別コードは、データに関連づけられてもよい。したがって、2つ以上のデバイスがデータに登録されかつデータへ安全にアクセスする可能性はある。

【００４１】

マスタデバイスは、例えばさらなるデバイスに関連づけられる識別コードを登録してもよく、またはこうした識別コードの登録を要求してもよい。

【００４２】

先に論じたように、識別コードは、好ましくは、デバイスのスマートオブジェクトに関連づけられる識別コードである。スマートオブジェクトは、例えば、デバイスに関連づけられるSIM、仮想SIM、SIMソフトウェア、TPM（トラステッド・プラットフォーム・モジュール）、SE（セキュアエレメント）、TEE（トラステッドエグゼキューション環境）、マイクロSD、メモリカード、USBまたはスマートカードであってもよい。異なるデバイスの識別コードを提供するために、異なるスマートオブジェクトが使用される可能性もある。スマートオブジェクトは、あらゆるローカル、リモートまたは取外し可能形式のメモリで

あってもよい。

【００４３】

事例によっては、デバイスは、少なくとも1つのさらなるデバイスが同じくデータにアクセスしている場合にのみ、データへのアクセスを許容されてもよい。事例によっては、前記少なくとも1つのさらなるデバイスは、管理者デバイス等の指定された特定のデバイスでなければならない場合がある。

【００４４】

さらなる態様によれば、デバイスからデータへのアクセスを制御する方法が提供されており、前記データは、デバイスから遠隔に、または取外し可能なストレージに記憶され、本方法は、下記のステップ、即ち、（ｉ）デバイスから、データへアクセスする要求を受信するステップであって、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、（ｉｉ）少なくとも部分的に識別コードに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、データへのデバイスのアクセスを許可または拒絶するステップと、を含む。

【００４５】

本態様は、先に述べた第1の態様の何れかの追加的または任意選択の特徴を含んでもよい。

【００４６】

好ましくは、本態様による方法は、データ・アクセス・コントローラによって実行される。データ・アクセス・コントローラは、データへのアクセスを希望するデバイスから遠隔に存在してもよい。例えば、データ・アクセス・コントローラは、クラウド内に存在してもよい。

【００４７】

さらなる態様によれば、デバイスから遠隔に、または取外し可能なストレージに記憶されるデータへのアクセスを制御するためのデータ・アクセス・コントローラが提供されており、前記データ・アクセス・コントローラは、下記のステップ、即ち、（ｉ）デバイスから、データへアクセスする要求を受信するステップであって、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、（ｉｉ）少なくとも部分的に識別コードに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、データへのデバイスのアクセスを許可または拒絶するステップと、を実行するように構成される。

【００４８】

データ・アクセス・コントローラは、データへのアクセスを希望するデバイスから遠隔に存在してもよい。例えば、データ・アクセス・コントローラは、クラウド内に存在してもよい。

【００４９】

アクセスされるべきデータは、クラウドベースまたはウェブベースの第三者サービスへのアクセスを容易にするためのデータであってもよい。本発明の下記の態様は全て（その好適な、または任意選択の特徴と共に）、同じくこの任意選択の特徴を含んでもよい。

【００５０】

データにアクセスする要求は、クラウドベースのパーティションによって受信されてもよい。適用可能であれば、本発明の下記の態様は（その好適な、または任意選択の特徴と共に）、同じくこの任意選択の特徴を含んでもよい。

【００５１】

さらなる態様によれば、デバイスと、デバイスから遠隔に、または取外し可能なストレージに記憶されるデータへのデバイスからのアクセスを制御するためのデータ・アクセス・コントローラとを備えるシステムが提供されており、前記デバイスは、データへのアクセス要求をデータ・アクセス・コントローラへ送信するように構成され、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含み、か

つ前記データ・アクセス・コントローラは、少なくとも部分的に識別コードに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証し、かつその結果に応じて、データへのデバイスのアクセスを許可または拒絶するように構成される。

【００５２】

さらなる態様によれば、デバイスから遠隔に、または取外し可能なストレージに記憶されるデータへのアクセスを制御するためのコンピュータプログラムが提供されており、前記プログラムは、プロセッサによって実行されると、下記のステップ、即ち、（ｉ）デバイスから、データへアクセスする要求を受信するステップであって、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、（ｉｉ）少なくとも部分的に識別コードに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、データへのデバイスのアクセスを許可または拒絶するステップと、を実行するように構成される。

【００５３】

さらなる態様によれば、デバイスがアクセスコントローラを介してデータにアクセスし得るように、デバイスをアクセスコントローラに登録する方法が提供されており、前記データは、デバイスから遠隔に、または取外し可能なストレージに記憶され、本方法は、データへアクセスするためにデバイスを登録する要求を送信することであって、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むことと、データへのアクセスが許可されるべきかどうかをチェックすることと、アクセスが許可されるべきものであれば、識別コードをアクセスされるべきデータに対して登録すること、を含む。

【００５４】

要求は、好ましくは、例えば、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コード、およびPINまたはパスコードおよびユーザに固有の何かを表すデータのうちの一方または双方を基礎とする2または3ファクタコードを含む。これは、どのデバイスがパーティションへのアクセスを要求しているかの監査可能な追跡を可能にする。

【００５５】

要求は、eメールまたはSMSの形式であってもよい。

【００５６】

本方法は、好ましくは、要求に関連する情報を管理者デバイスへ送信することをさらに含み、管理者デバイスは、好ましくは、データへのアクセスが認可されるべきか否かを決定する。要求に関連する情報は、例えば、アクセスコントローラまたは登録を求めているデバイスから送信されてもよい。管理者デバイスは、アクセスを要求するデバイスに対する、読取り専用、またはデータを編集し／削除し／追加コンテンツを加える能力等のアクセス許可を設定するために使用されてもよい。

【００５７】

例えば、子供のデバイス（例えば、電話またはタブレット）のセキュアエレメントまたはメモリカードが、両親のデータにアクセスできるように登録される事例において、両親のデバイス（例えば、電話またはタブレット）のセキュアエレメントまたはメモリカードは、子供によるデータへのアクセスを監視しかつ制御できるように、そのデータの管理者として登録されることも可能である。データ自体は、実際には、両親の管理者デバイスに記憶されることも可能である。したがって、あるデバイス（または複数のデバイス）は（各々）、例えば限定的な、または指定された読取り／書込み許可によって、1つ以上のさらなるデバイスがそのデバイスに記憶されるデータにアクセスすることを許可してもよい。

【００５８】

好ましくは、管理者がデバイスによるデータへのアクセスを許可すると決定すれば、管理者からアクセスコントローラへ、この旨を示す信号が送信される。

【００５９】

さらなる態様によれば、デバイスがアクセスコントローラを介してデータにアクセスし得るように、デバイスをアクセスコントローラに登録する方法が提供されており、前記データは、デバイスから遠隔に、または取外し可能なストレージに記憶され、本方法は、データへアクセスするためにデバイスを登録する要求を受信することであって、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むことと、データへのアクセスが許可されるべきかどうかをチェックすることと、アクセスが許可されるべきものであれば、識別コードをアクセスされるべきデータに対して登録すること、を含む。

【００６０】

さらなる態様によれば、データへのアクセスに対するデバイスの登録を制御するためのデータ・アクセス・コントローラが提供されており、前記コントローラは、下記のステップ、即ち、データへアクセスするためにデバイスを登録する要求を受信するステップであって、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、データへのアクセスが許可されるべきかどうかをチェックするステップと、アクセスが許可されるべきものであれば、識別コードをアクセスされるべきデータに対して登録するステップと、を実行するように構成される。

【００６１】

さらなる態様によれば、デバイスと、データへのアクセスに対するデバイスの登録を制御するためのデータ・アクセス・コントローラとを備えるシステムが提供されており、前記コントローラは、下記のステップ、即ち、デバイスから、データへアクセスするためにデバイスを登録する要求を受信するステップであって、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、データへのアクセスが許可されるべきかどうかをチェックするステップと、アクセスが許可されるべきものであれば、識別コードをアクセスされるべきデータに対して登録するステップと、を実行するように構成される。

【００６２】

システムは、好ましくは、管理者デバイスをさらに備える。

【００６３】

データ・アクセス・コントローラは、好ましくは、デバイスが登録されるべくデータへのアクセスが許可されるべきかどうかをチェックするために、管理者デバイスへ信号を送信するように構成される。

【００６４】

管理者デバイスは、好ましくは、デバイスが登録されるべくデータへのアクセスが許可されるべきかどうかを確認する信号、かつ／またはアクセスを要求するデバイスに対する、読取り専用、またはデータを編集し／削除し／追加コンテンツを加える能力等のアクセス許可を設定する信号を送信するように構成される。

【００６５】

さらなる態様によれば、データへのアクセスに対するデバイスの登録を制御するためのコンピュータプログラムが提供されており、前記プログラムは、プロセッサによって実行されると、下記のステップ、即ち、デバイスから、データへアクセスするデバイスを登録する要求を受信するステップであって、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、データへのアクセスが許可されるべきかどうかをチェックするステップと、アクセスが許可されるべきものであれば、識別コードをアクセスされるべきデータに対して登録するステップと、を実行するように構成される。

【００６６】

さらなる態様によれば、デバイスにおいてデータにアクセスする方法が提供されており、前記データは、デバイスから遠隔に、または取外し可能なストレージに記憶され、本方法は、デバイスにおいて、データにアクセスする勧誘を受信することであって、前記勧誘は、パスワード、コードまたはPINを含むことと、デバイスから、データにアクセスする

要求を送信することであって、前記要求は、パスワード、コードまたはPINを含むことと、少なくとも部分的にパスワード、コードまたはPINに基づいて、データへのアクセスが許可されるべきか拒絶されるべきかを検証することと、その結果に応じて、データへのデバイスのアクセスを許可または拒絶すること、を含む。

【００６７】

したがって、ユーザは、さらなるデバイスもデータにアクセスし得るように、さらなるデバイス（ユーザ固有の、または別のユーザのデバイス）へ勧誘を送信することが可能である。これらのデバイス（または、これらに関連づけられる識別コード）は、必ずしも、アクセスを認可されるべくデータに登録される必要はない。

【００６８】

この態様によれば、デバイスに対して、アクセスは、時間を無制限に、または予め決められた時間内で認可されてもよい。何れの場合も、アクセスは、アクセスが認可された後の何れかの時点で、例えば別のユーザによって止められてもよい。

【００６９】

パスワード、コードまたはPINは、例えば乱数発生器によって発生されてもよい。

【００７０】

パスワード、コードまたはPINは、好ましくは、ワンタイムパスワードである。これは、さらなるユーザにアクセスを認可する安全な方法を提供することができる。

【００７１】

好ましくは、パスワード、コードまたはPINは、指定される時間期間でのみ有効である。したがって、これが指定された期間内に使用されなければ、このパスワード、コードまたはPINに基づくアクセスは認可されない。この期間は、例えば、1、2、3、4、5、6、7、8、9、10、15、20、25、30、45、60、90または120分までであってもよい。期間は、好ましくは、24時間以内である。一方で、実施形態によっては、パスワード、コードまたはPINは、特定の有効時間を持たなくてもよい。

【００７２】

好ましくは、パスワード、コードまたはPINは、少なくとも、セキュアなチャネルを介してデバイスへ、かつ／またはデバイスから送信される（好ましくは、デバイスとの間で送受信される）。

【００７３】

実施形態によっては、パスワード、コードまたはPINは、データへのアクセスを制御する、マスタデバイス等のデバイスによって発生される。あるいは、マスタデバイスは、この機能を非マスタデバイスへ付与してもよい。

【００７４】

本方法は、第1のデバイスによって、第2のデバイスがデータにアクセスすることを許可する方法であってもよく、前記データは、第1および第2のデバイスから遠隔に記憶され、勧誘は、第1のデバイスから第2のデバイスへ送信され、データにアクセスする要求は、第2のデバイスから送信され、かつデータへのアクセスは、第2のデバイスに対して許可または拒絶される。

【００７５】

この場合、パスワード、コードまたはPINは、第1のデバイスにおいて発生されてもよい。

【００７６】

あるいは、パスワード、コードまたはPINは、第1および第2のデバイスの双方から遠隔で、例えばデータへのアクセスを制御するプロセッサにおいて発生されてもよい。

【００７７】

何れの場合も、本方法は、好ましくは、発生されるパスワード、コードまたはPINをアクセスされるべきデータに登録することをさらに含む。

【００７８】

発生されるパスワード、コードまたはPINをアクセスされるべきデータに登録するステ

ップは、第1のデバイスが、発生されるパスワード、コードまたはPINを登録する前に、さらなるデバイスをデータへアクセスすよう勧誘することを許可されているか検証することを含んでもよい。

【００７９】

本方法は、さらに、第1のデバイスから、パスワード、コードまたはPINの発生を求める要求を送信することを含んでもよく、前記発生されるべきパスワード、コードまたはPINは、第1のデバイスがさらなるデバイスをデータへアクセスするよう勧誘することを許可されているという検証がなされた後にのみ発生される。

【００８０】

したがって、何れの場合も、認証されたデバイスのみが、さらなるデバイスをデータへアクセスするよう勧誘してもよい。

【００８１】

第1のデバイスがさらなるデバイスをデータへアクセスするよう勧誘することを許可されていることの検証ステップは、好ましくは、先に述べたような、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コード等の、デバイスに関連づけられる識別コードを検証することを含む。

【００８２】

第1のデバイスがさらなるデバイスをデータへアクセスするよう勧誘することを許可されていることの検証ステップは、さらに、第1のデバイスから送信される、パーティションを指定するデータを検証することを含んでもよい。

【００８３】

パーティションを指定するデータは、好ましくは、PINまたはパスコード、および、デバイスのユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等のデータ、のうちの一方または双方を含む。

【００８４】

さらなる態様によれば、デバイスにおける、データへのアクセスを許可する方法が提示されており、前記データは、デバイスから遠隔に、または取外し可能なストレージに記憶され、本方法は、デバイスへ、データにアクセスする勧誘を送信することであって、前記勧誘は、パスワード、コードまたはPINを含むことと、デバイスから、データにアクセスする要求を送信することであって、前記要求は、パスワード、コードまたはPINを含むことと、少なくとも部分的にパスワード、コードまたはPINに基づいて、データへのアクセスが許可されるべきか拒絶されるべきかを検証することと、その結果に応じて、データへのデバイスのアクセスを許可または拒絶すること、を含む。

【００８５】

勧誘は、管理者デバイスから、好ましくはアクセスコントローラを介して送信されてもよい。勧誘は、eメールまたはSMSメッセージ等のメッセージ形式であってもよく、かつ／または、勧誘は、データ・アクセス・アプリケーション内のメッセージングシステムを介して送信されかつ閲覧可能であることも可能である。勧誘されたユーザは、このアプリケーションを開く、またはこれにログインすると、所定のデータへのアクセスに対する勧誘が受信されていることを視認し得る。ユーザは、次に、データにアクセスしてもよい。

【００８６】

勧誘は、OTP（ワンタイムパスワード）、例えばデータにウェブブラウザ経由で（例えば、データ・アクセス・アプリケーション経由ではなく）アクセスするためにユーザがウェブブラウザに入力し得るOTP、を含んでもよい。

【００８７】

さらなる態様によれば、第1のデバイスと、第2のデバイスと、データ・アクセス・コントローラとを備えるシステムが提供されており、前記第1のデバイスは、第2のデバイスにおけるデータへのアクセスを許可するように構成され、前記データは、第2のデバイスから遠隔に、または取外し可能なストレージに記憶され、前記第1のデバイスは、第2のデバイスへ、データへのアクセスの勧誘を送信するように構成され、前記勧誘は、パスワード

、コードまたはPINを含み、前記第2のデバイスは、データにアクセスする要求を送信するように構成され、前記要求は、パスワード、コードまたはPINを含み、かつ前記データ・アクセス・コントローラは、少なくとも部分的にパスワード、コードまたはPINに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証し、かつその結果に応じて、第2のデバイスによるデータへのアクセスを許可または拒絶するように構成される。

【００８８】

さらなる態様によれば、デバイスにおいてデータにアクセスする方法が提供されており、前記データは、デバイスから遠隔に、または取外し可能なストレージに記憶され、本方法は、下記のステップ、即ち、（ｉ）デバイスから、データにアクセスする要求を送信するステップであって、前記要求は、要求に関連するデータを含むステップと、（ｉｉ）少なくとも部分的にデータに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、かつデータにアクセスする少なくとも1つのさらなるデバイスが存在する場合にのみ、デバイスによるデータへのアクセスを許可するステップと、を含む。

【００８９】

このような方法は、金融取引、メッセージングおよび／または（例えば、機密）データのビューイング等の所定のアクションが、さらなるデバイスが存在する場合にのみ実行され得るセキュアな環境を提供することができる。さらなるデバイス（例えば、管理者デバイス）は、次に、デバイスにより実行されるあらゆるアクションを監視することも可能である。よって、適切であれば、データへのさらなるアクセスの阻止または防止等の迅速な措置を講じることも可能である。

【００９０】

本方法は、好ましくは、ステップ（ｉｉｉ）に先行して、少なくとも1つのさらなるデバイスがデータにアクセスしているかどうかをチェックすることを含む。少なくとも1つのさらなるデバイスは、例えば、「マスタ」デバイス等の特定の指定されたデバイスであってもよい。

【００９１】

さらなる態様によれば、デバイスにおいてデータへのアクセスを制御する方法が提供されており、前記データは、デバイスから遠隔に、または取外し可能なストレージに記憶され、本方法は、下記のステップ、即ち、（ｉ）デバイスから、データへアクセスする要求を受信するステップであって、前記要求は、要求に関連するデータを含むステップと、（ｉｉ）少なくとも部分的にデータに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、かつデータにアクセスする少なくとも1つのさらなるデバイスが存在する場合にのみ、デバイスによるデータへのアクセスを許可するステップと、を含む。

【００９２】

さらなる態様によれば、デバイスにおいてデータへのアクセスを制御するためのデータ・アクセス・コントローラが提供されており、前記データは、デバイスから遠隔に、または取外し可能なストレージに記憶され、本データ・アクセス・コントローラは、下記のステップ、即ち、（ｉ）デバイスから、データへアクセスする要求を受信するステップであって、前記要求は、要求に関連するデータを含むステップと、（ｉｉ）少なくとも部分的にデータに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、かつデータにアクセスする少なくとも1つのさらなるデバイスが存在する場合にのみ、デバイスによるデータへのアクセスを許可するステップと、を実行するように構成される。

【００９３】

データ・アクセス・コントローラは、好ましくは、ステップ（ｉｉｉ）の実行に先行して、少なくとも1つのさらなるデバイスがデータにアクセスしているかどうかをチェックするようにも構成される。

【００９４】
さらなる態様によれば、デバイスと、デバイスにおいてデータへのアクセスを制御するためのデータ・アクセス・コントローラとを備えるシステムが提供されており、前記データは、デバイスから遠隔に、または取外し可能なストレージに記憶され、前記データ・アクセス・コントローラは、下記のステップ、即ち、（ｉ）デバイスから、データへアクセスする要求を受信するステップであって、前記要求は、要求に関連するデータを含むステップと、（ｉｉ）少なくとも部分的にデータに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、かつデータにアクセスする少なくとも1つのさらなるデバイスが存在する場合にのみ、デバイスによるデータへのアクセスを許可するステップと、を実行するように構成される。
【００９５】
好ましくは、デバイスは、データにアクセスする要求をデータ・アクセス・コントローラへ送信するように構成される。
【００９６】
データ・アクセス・コントローラは、好ましくは、ステップ（ｉｉｉ）の実行に先行して、少なくとも1つのさらなるデバイスがデータにアクセスしているかどうかをチェックするようにも構成される。
【００９７】
さらなる態様によれば、デバイスから遠隔に、または取外し可能なストレージに記憶されるデータへのアクセスを制御するためのコンピュータプログラムが提供されており、前記プログラムは、プロセッサによって実行されると、下記のステップ、即ち、（ｉ）デバイスから、データへアクセスする要求を受信するステップであって、前記要求は、要求に関連するデータを含むステップと、（ｉｉ）少なくとも部分的にデータに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、かつデータにアクセスする少なくとも1つのさらなるデバイスが存在する場合にのみ、デバイスによるデータへのアクセスを許可するステップと、を実行するように構成される。
【００９８】
プログラムは、好ましくは、ステップ（ｉｉｉ）の実行に先行して、少なくとも1つのさらなるデバイスがデータにアクセスしているかどうかをチェックするようにも構成される。
【００９９】
本発明のさらなる態様は、デバイスにおいてデータにアクセスする方法に関し、前記データは、デバイスから遠隔に、取外し可能なストレージに、またはデバイス自体に記憶され、本方法は、下記のステップ、即ち、（ｉ）データにアクセスする要求を送信するステップであって、前記要求は、デバイスに関連づけられる識別コードと、PINまたはパスコード、およびデバイスのユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等のデータ、のうちの一方または双方と、を含むステップと、（ｉｉ）識別コードおよびPINまたはパスコードおよび／またはユーザに固有の何かを表すデータに基づいて、データへのアクセスが許可されるべきか拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、デバイスによるデータへのアクセスを許可または拒絶するステップと、を含む。
【０１００】
データは、好ましくは、パーティションに記憶される。この場合、PINまたはパスコードおよび／またはデバイスのユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等のデータは、ユーザがアクセスすることを求めているパーティションに関連づけられる。例えば、PINまたはパスコードおよび／またはデバイスのユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等のデータは、データ、またはデータが記憶されるパーティションを識別してもよい。
【０１０１】
遺伝学的および／または生体測定的情報の場合、1つの選択肢は、どの指紋が入力され

て送信されるかに依存して、対応するデータまたはパーティションがアクセスされるように、異なる指の指紋が異なるデータまたはパーティションに関連づけられることである可能性もある。

【０１０２】

本発明のさらなる態様は、デバイスにおいて、データへのアクセスを制御する方法に関し、前記データは、デバイスから遠隔に、取外し可能なストレージに、またはデバイス自体に記憶され、本方法は、下記のステップ、即ち、（ｉ）データにアクセスする要求を受信するステップであって、前記要求は、デバイスに関連づけられる識別コードと、PINまたはパスコード、およびデバイスのユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等のデータ、のうちの一方または双方と、を含むステップと、（ｉｉ）識別コードおよびPINまたはパスコードおよび／またはユーザに固有の何かを表すデータに基づいて、データへのアクセスが許可されるべきか拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、デバイスによるデータへのアクセスを許可または拒絶するステップと、を含む。

【０１０３】

本発明のさらなる態様は、デバイスにおいて、データへのアクセスを制御するためのデータ・アクセス・コントローラに関し、前記データは、デバイスから遠隔に、取外し可能なストレージに、またはデバイス自体に記憶され、前記データ・アクセス・コントローラは、下記のステップ、即ち、（ｉ）データにアクセスする要求を受信するステップであって、前記要求は、デバイスに関連づけられる識別コードと、PINまたはパスコード、およびデバイスのユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等のデータ、のうちの一方または双方と、を含むステップと、（ｉｉ）識別コードおよびPINまたはパスコードおよび／またはユーザに固有の何かを表すデータに基づいて、データへのアクセスが許可されるべきか拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、デバイスによるデータへのアクセスを許可または拒絶するステップと、を実行するように構成される。

【０１０４】

本発明のさらなる態様は、デバイスにおいて、データへのアクセスを制御するためのコンピュータプログラムに関し、前記データは、デバイスから遠隔に、取外し可能なストレージに、またはデバイス自体に記憶され、前記プログラムは、プロセッサによって実行されると、下記のステップ、即ち、（ｉ）データにアクセスする要求を受信するステップであって、前記要求は、デバイスに関連づけられる識別コードと、PINまたはパスコード、およびデバイスのユーザに固有の何かを表す、遺伝学的および／または生体測定的情報等のデータ、のうちの一方または双方と、を含むステップと、（ｉｉ）識別コードおよびPINまたはパスコードおよび／またはユーザに固有の何かを表すデータに基づいて、データへのアクセスが許可されるべきか拒絶されるべきかを検証するステップと、（ｉｉｉ）その結果に応じて、デバイスによるデータへのアクセスを許可または拒絶するステップと、を実行するように構成される。

【０１０５】

本発明の態様は、本発明のあらゆる他の態様の、好適な、または任意選択の特徴を含むあらゆる特徴を含んでもよい。

【０１０６】

何れの態様においても、データは、好ましくは暗号化される。好ましくは、データは、データにアクセスするデバイスによって復号される。この場合、デバイスは、好ましくは、データを復号するためのキーを有する。キーは、好ましくは、セキュアエレメントまたはメモリカードに記憶されるが、遠隔に記憶されてもよい。好ましくは、キー自体も暗号化される。キーは、好ましくは、デバイスへセキュアな方法で、例えばTSM（トラステッド・サービス・マネージャ）によって転送される。

【０１０７】

上記から、本発明の実施形態は、

複数のデバイスがパーティションアクセスを有することができ、

ユーザは、制御および監査追跡を保全しながら、他のユーザ（デバイス）とセキュアに共有することができ、

トランザクションをセキュアに実行することができる、方法およびシステムを提供し得る、という認識を得ることができる。

【０１０８】

同じリモートパーティションへは、複数のデバイスがアクセスしてもよい。

【０１０９】

データまたは（1つ以上の）パーティションにアクセスすると、デバイスは、下記のサービス、即ち、メッセージング、メディア、テレビ、映画、ラジオ、雑誌、ソーシャルメディア、電子商取引、スマートデバイス（例えば、ユーティリティおよびホームコントロール）、企業向けサービス、絵画、写真および映像シェア、政府サービス、金融サービス、医療サービス、旅行業務、音楽およびゲームのうちの1つ以上にアクセス可能であってもよい。当然ながら、追加的に、または代替としてアクセスされる可能性もある、言及されていないさらなるサービスも存在し得る。

【０１１０】

デバイスは、パーティションにアクセスするために、2または3ファクタ認証を提供可能であってもよい。デバイスは、認証の1ファクタがスマートオブジェクト（メモリカードまたはセキュアエレメント）の識別コードであり、かつ1つ以上のさらなるファクタがパスコードまたはPIN、または何らかの形式の遺伝学的または生体測定的識別データ、またはロケーション、または時間、または別のメンバ（例えば、管理者）またはユーザの属するグループがデータにアクセスしているかどうか、であることによって守られてもよい。

【０１１１】

次の表は、ユーザが用いてパーティションへのアクセスを希望し得るデバイスの例、およびその可能な対応する「スマートオブジェクト」（即ち、セキュアエレメントまたはメモリカード）を記載している。スマートオブジェクトは、その識別コードがパーティションに関連づけられ、かつパーティションへのアクセスが許可されるために検証されなければならないデバイスのオブジェクトである。

【０１１２】

【表１】

デバイス	スマートオブジェクト
電話	SIM、仮想SIM、SIMソフトウェア、SE、TEE、マイクロSD、メモリカード、NFCスマートオブジェクト（NFCスマートフォン用）
タブレット	SIM、SE、TEE、マイクロSD、メモリカード
ラップトップ	SIM、仮想SIM、SIMソフトウェア、SE、TEE、TPM、マイクロSD、メモリカード、USBキー、スマートカード
デスクトップ	SIM、仮想SIM、SIMソフトウェア、SE、TEE、マイクロSD、メモリカード、USBキー、スマートカード
テレビ	SIM、仮想SIM、SIMソフトウェア、SE、TEE、マイクロSD、メモリカード、USBキー、スマートカード
セット・トップ・ボックス	SIM、仮想SIM、SIMソフトウェア、SE、TEE、マイクロSD、メモリカード、USBキー、スマートカード
カメラ	SIM、仮想SIM、SIMソフトウェア、SE、TEE、マイクロSD、メモリカード、USBキー、スマートカード
車	SIM、仮想SIM、SIMソフトウェア、SE、TEE、マイクロSD、メモリカード、USBキー、スマートカード
ゲーム機	SIM、仮想SIM、SIMソフトウェア、SE、TEE、マイクロSD、メモリカード、USBキー、スマートカード
メガネ	SIM、仮想SIM、SIMソフトウェア、SE、TEE、マイクロSD、メモリカード、USBキー、スマートカード
腕時計	SIM、仮想SIM、SIMソフトウェア、SE、TEE、マイクロSD、メモリカード、USBキー、スマートカード
クロームキャスト	SIM、仮想SIM、SIMソフトウェア、SE、TEE、マイクロSD、メモリカード、USBキー、スマートカード
スマートメータ（ホームユーティリティ）	SIM、仮想SIM、SIMソフトウェア、SE、TEE、マイクロSD、メモリカード、USBキー、スマートカード

【０１１３】
パーティションは、下記のような異なるタイプが設けられてもよい。

【０１１４】
ユーザのみがアクセスを有するクローズドパーティション、
勧誘のみによって他のユーザと共有されることが可能なクローズドパーティション、
監査履歴追跡を有するオープンパーティション、
ユーザの履歴または監査追跡を持たないオープンかつ無記名のパーティション。

【０１１５】
あらゆる種類のパーティションが、タイムスロット等の基準に基づいてオープンまたはクローズドであるようにトグルされてもよい。例えば、パーティションは、予め規定された特定の時間にオープンであり、かつ予め規定された特定の時間にクローズドであるように設定される可能性もある。

【０１１６】
ユーザは、複数のデバイスをパーティションに対して登録してもよく、かつ登録する追加デバイスに対して機能をトグルし、編集しかつアップロードしてもよい。例えば、ユーザは、ユーザのカメラが写真をパーティションにアップロードしかつパーティション内の写真を見る能力を有するが、パーティション内の何れのコンテンツも削除または編集する能力を持たないように希望してもよい。

【０１１７】
ユーザは、1つ以上のデバイスをパーティションの管理者デバイスにするように選んでもよい。これにより、管理者は、パーティションへのアクセスを制御し、かつ管理者がそ

れを必要であると判断すれば、アクセスを停止することができるようになる可能性もある。また、ユーザは、管理者の力量において、ユーザが管理者であるパーティションへのアクセスを認可されている他の全てのユーザのデバイスへのアクセスを有する可能性もある。これにより、ユーザは、リアルタイムで、パーティションへのアクセス許可を編集または取り消すことができるようになる可能性もある。また、これにより、ユーザは、ユーザがデバイスをなくせば、または所有しないようになれば、デバイスへのアクセスを禁止することもできるようになる可能性もある。

【０１１８】

管理者デバイスは、ユーザによってトグルされ得る、かつユーザに、登録されたスマートオブジェクトへ接続されていないマシン上へのログへのアクセスを与え得る、好ましくは時間的制約のあるコードを生成する能力を有してもよい。このコードは、任意の長さである可能性もあり、かつ／またはアクセスコントローラへ接続されるインタフェースに入力される可能性もあり、かつパーティションへのアクセスは、デスクトップまたはラップトップ等の非登録デバイス上で許可される可能性もある。ユーザは、このセッションを任意の時点で管理者デバイスから、例えば、管理者デバイス上の停止ボタンを始動することによって停止する能力を有する可能性もある。生成されるコードは、好ましくは、管理者デバイスによる2または3ファクタ認証の結果である。

【０１１９】

スマートオブジェクトは、添付された同じ、または異なるパスコード／認証子を有し得る複数のパーティションを管理してもよい。パーティション内部において、システムは、ユーザが多くの異なる第三者サービスにサインアップできるように、または自動的にサインアップできるようにしてもよい。パーティション内部において、システムは、ユーザIDおよびユーザが設定するパスワードを、パスワードおよびユーザID双方の英数字列に変えてもよい。これは、第三者サービスプロバイダへ伝えられることも可能である。これらのコードは、サービスの最良実施ガイドラインに基づいて新しくされてもよい。例えば、これらは、ユーザが英国内の医療記録にアクセスしていれば、NHS情報ガバナンスの要件に従って60日毎に新しくされることも可能である。

【０１２０】

かくして、本発明のさらなる態様によれば、デバイスを用いてクラウドベースまたはウェブベースの第三者サービスにアクセスする方法が提供されており、本方法は、下記のステップ、即ち、（i）デバイスから、デバイスに関連づけられるクラウドベースのパーティションへ要求を送信するステップであって、前記パーティションは、第三者サービスへの接続を容易にするためのデータを含み、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、（ii）少なくとも部分的に識別コードに基づいて、パーティションへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、（iii）その結果に応じて、デバイスによるパーティションへのアクセスを許可または拒絶するステップと、パーティションへのアクセスが許可された後に、（iv）第三者サービスへ資格認証情報を送信するステップと、を含む。

【０１２１】

本発明のさらなる態様によれば、デバイスによるクラウドベースまたはウェブベースの第三者サービスへのアクセスを制御する方法が提供されており、本方法は、下記のステップ、即ち、（i）デバイスから、デバイスに関連づけられるクラウドベースのパーティションへの要求を受信するステップであって、前記パーティションは、第三者サービスへの接続を容易にするためのデータを含み、前記要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含むステップと、（ii）少なくとも部分的に識別コードに基づいて、パーティションへのアクセスが許可されるべきか、拒絶されるべきかを検証するステップと、（iii）その結果に応じて、デバイスによるパーティションへのアクセスを許可または拒絶するステップと、パーティションへのアクセスが許可された後に、（iv）第三者サービスへ資格認証情報を送信するステップと、を含む。

【０１２２】

したがって、第三者サービスへのアクセスは、デバイスに関連づけられる正しい識別コードが提供される場合にのみ許可される。したがって、非認証デバイスによる第三者サービスへのアクセスは、これらが正しい識別コードを提供できないことによって防止することが可能である。

【０１２３】

次の好適な特徴は、本発明の前述の2態様にも等しく当てはまる。

【０１２４】

デバイスが特定のパーティションにアクセスできるように、デバイスは、パーティションにアクセスするための適切なソフトウェア（例えば、アプリケーション）をインストールしていてもよい。これは、例えば、デバイスに関連づけられるセキュアエレメントまたはメモリカードに記憶される。

【０１２５】

あるいは、アプリケーションは、単に部分的に、セキュアエレメントまたはメモリカードに記憶されてもよく、例えば、アプリケーションは、標準モバイルアプリケーションで、かつセキュアエレメント内部のアプレットで構成されることも可能である。

【０１２６】

パーティションは、幾つかの異なるウェブサービスに関連づけられてもよい。

【０１２７】

少なくとも部分的に識別コードに基づいて、パーティションへのアクセスが許可されるべきであることが検証されれば、デバイスのセキュアエレメントまたはメモリカードとクラウドパーティションとの間で相互的な認証プロセスが開始されてもよい。このプロセスは、デバイスのセキュアエレメントまたはメモリカードとクラウドパーティションとの間のセキュアなチャネルの生成を可能にする。よって、デバイスのセキュアエレメントまたはメモリカードとクラウドパーティションとの間でデータが転送されてもよい。データは、暗号化されてもよい。

【０１２８】

したがって、資格認証情報を送信するステップ（iv）は、デバイスのセキュアエレメントまたはメモリカードとクラウドパーティションとの間で相互的な認証プロセスを実行するステップと、セキュアエレメントまたはメモリカードとクラウドパーティションとの間にセキュアなチャネルを生成するステップとを含む。ステップ（iv）は、資格認証情報をセキュアなチャネルを介してパーティションへ送信することも含んでもよい。資格認証情報は、暗号化されてもよく、この場合、資格認証情報は、セキュアなチャネルを介する送信に先行して暗号化される。資格認証情報は、次に、パーティションによって第三者サービスへ提供されてもよい。

【０１２９】

あるいは、資格認証情報は、パーティションのセキュアエレメントに記憶されてもよい。この場合、資格認証情報をセキュアエレメントまたはメモリカードからパーティションへ送信する必要はない。代わりに、パーティションへのアクセスがデバイスに認可されている場合には、資格認証情報は、パーティションから直接第三者サービスへ送信されてもよい。

【０１３０】

資格認証情報は、第三者サービスへ暗号化された形式で送信されてもよい。この場合、送信された暗号資格認証情報を翻訳できるように、互換性のあるセキュアエレメントがウェブサービスレベルで実装される。

【０１３１】

セキュアエレメントまたはメモリカードは、例えば、それ自体も理想的にはセキュアかつ改竄防止的な固有の識別コードを有する「スマートオブジェクト」またはセキュアな、または改竄防止的なハードウェアデバイスである。セキュアエレメントまたはメモリカードは、例えば、SIM、仮想SIM、SIMソフトウェア、TPM（トラステッド・プラットフォーム・モジュール）、SE（セキュアエレメント）、TEE（トラステッドエグゼキューション環

境）、マイクロSD、メモリカード、USBキーまたはスマートカードであることも可能である。

【０１３２】

したがって、セキュアエレメントは、データを安全に記憶しかつ／または処理できる様々なタイプのセキュアなチップ、デバイスまたはソフトウェアソリューション（例えば、キー、アルゴリズム、アプレット、資格認証情報）の総称である。

【０１３３】

セキュアエレメントまたはメモリカードは、メモリのあらゆるローカル、リモートまたは取外し可能な形式であってもよい。

【０１３４】

セキュアエレメントまたはメモリカードの識別コードは、好ましくは、良好に保護され、かつ例えば、セキュアエレメントまたはメモリカード内のセーフボックスに記憶される。好ましくは、識別コードは、セキュアなチャネルを介して送信される。あるいは、または追加的に、識別コードは、暗号化されてもよい。これは、プロセスをより安全なものにし、かつ識別コードが第三者によって傍受される、かつ／または発見されることを防止する手助けをする。

【０１３５】

先に述べたように、要求は、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを含む。しかしながら、識別コードは、要求に、変形された形式で、例えば暗号化された形式で、かつ／または1つ以上のさらなるコード、データまたは情報と組み合わせて含まれてもよい。

【０１３６】

要求は、デバイス側で入力されるパスコードまたはPINも含んでもよく、よって、ステップ（ii）は、パスコードまたはPINに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含んでもよい。このように、データにアクセスするためには、2ファクタ認証が要求されてもよい。

【０１３７】

パスコードまたはPINは、（まず）デバイスに関連づけられるセキュアエレメントまたはメモリカード（例えば、SIMまたは仮想SIM）によって検証されてもよい。

【０１３８】

あるいは、または追加的に、要求は、デバイスのユーザに固有の何かを表すデータを含んでもよく、ステップ（ii）は、デバイスのユーザに固有の何かを表すデータに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含んでもよい。このように、データへアクセスするためには、2ファクタまたは3ファクタ認証が要求されてもよく、かつ認証されたユーザのみが、データへのアクセスを認可されてもよい。

【０１３９】

デバイスのユーザに固有の何かを表すデータは、ユーザに関する遺伝学的および／または生体測定的情報を表すデータ、例えば指紋または虹彩データ等、を含んでもよい。

【０１４０】

認証形式としては、PINおよび／またはデバイスのユーザに固有の何かを表すデータを用いる認証（識別コードを用いる2ファクタまたは3ファクタ認証）の代わりに、またはこれに追加して、次のようなものが可能である。

【０１４１】

要求は、ロケーション（即ち、ユーザがデータにアクセスしようとしている起点場所）を含むデータを含んでもよく、ステップ（ii）は、ロケーションに基づいて、データへのアクセスが許可されるべきか、拒絶されるべきかを検証することも含んでもよい。

【０１４２】

要求は、時間（即ち、ユーザがデータにアクセスしようとしている時刻）を含むデータを含んでもよく、ステップ（ii）は、時間に基づいて、データへのアクセスが許可される

べきか、拒絶されるべきかを検証することも含んでもよい。

【０１４３】

要求は、ユーザがグループの一部であることを指すデータを含んでもよく、ステップ（ii）は、データへのアクセスが許可されるべきか、拒絶されるべきかを、グループの別のメンバ（例えば、管理者）がデータにアクセスしているかどうかに基づいて検証することも含んでもよい。

【０１４４】

本発明の好適な実施形態において、セキュアエレメントまたはメモリカードは、相互的な認証プロセスを実行し、かつ／またはセキュアなチャネルを生成しかつ／または識別コードおよび／またはPINまたはパスコードを暗号化するために使用される。

【０１４５】

本方法は、ユーザ・エンロールメント・プロセスを含んでもよく、これにより、ユーザは、第三者サービスの使用をエンロールする。このようなユーザ・エンロールメント・プロセスは、第三者サービスにアクセスするための資格認証情報および／または第三者サービスが要求するフォーム記入用データを収集するステップと、資格認証情報および／またはフォーム記入用データを安全に記憶するステップとを含んでもよい。資格認証情報は、ユーザIDおよび／またはパスワードを含んでもよい。さらに、資格認証情報は、第三者サービスをエンロールするために必要なユーザに関する（例えば、支払い明細を含む）あらゆる情報を含んでもよい。例えば、資格認証情報は、次のような情報、即ち、氏名、姓、肩書、住所、年齢、生年月日、性別、獲得ポイント、ポイントカード番号、支払いカード番号、カードの種類、有効期限、CVVコード、IDカードまたはパスポート番号、のうちの1つ以上を含んでもよい。これらの情報は、フォーム記入用データと称されてもよい。

【０１４６】

資格認証情報は、ユーザ・エンロールメント・プロセスにおいて収集される代わりに、パーティションへのアクセスが許可された後、パーティションによって自動的に生成されてもよい。即ち、エンロールメントプロセスは、デバイスにより、第三者サービスと組み合わせて管理され、ユーザによる能動的な介入はない。このような場合、ユーザ・エンロールメント・プロセスは、相互的な認証プロセスを初期化するステップと、第三者サービスを選択するステップとを含んでもよい。即ち、ユーザは、第三者サービスにアクセスするためにその資格認証情報を提供する必要がなくてもよく、パーティションにアクセスするためには、正しい識別コード（および好ましくは、パスコード／PINも必要とする実施形態ではパスコード／PIN）が提供されることで足りる場合がある。

【０１４７】

資格認証情報および／またはフォーム記入用データは、パーティションに安全に記憶されてもよい。あるいは、資格認証情報および／またはフォーム記入用データは、セキュアエレメントまたはメモリカードに安全に記憶されてもよい。後者の場合、資格認証情報は、必要に応じて、セキュアエレメントまたはメモリカードからパーティションへ供給されてもよい。

【０１４８】

資格認証情報（ユーザIDおよび／またはパスワード等）が自動的に生成される実施形態において、自動的に生成される資格認証情報は、周期的に、または要求に応じて新しくされてもよい。資格認証情報の更新周期は、ユーザのセキュリティポリシに従って、または第三者サービスのセキュリティポリシに従って適合化されてもよい。自動的に発生される資格認証情報は、他の手段によってサービスにアクセスする場合（例えば、ウェブブラウザを用いる、即ち特定のアプリケーションを用いない、PC、タブレットまたはスマートフォン、他からの標準的なウェブアクセス）に使用される資格認証情報とは異なっていてもよい。自動的に発生される資格認証情報の精巧化および／または複雑さは、ユーザのセキュリティポリシに従って、または第三者サービスのセキュリティポリシに従って適合化されてもよい。例えば、最短のパスワード長さは、ユーザのセキュリティポリシに従って、または第三者サービスのセキュリティポリシに従って設定されてもよい。また、ユーザID

および／またはパスワードは、小文字、大文字、句読点または句読記号および数字のうちの2つ以上による混合を含むように要求されてもよい。

【０１４９】

デバイスのセキュアエレメントまたはメモリカードには、単一のアプレットがインストールされてもよく、単一のアプレットは、全ての認証プロセスおよびサービスへのアクセスを駆動するように構成される。しかしながら、幾つかのタイプのサービスは、それらの固有のセキュリティを管理する能力、よって、認証プロセスおよびこれらのサービスへのアクセスを、セキュアエレメントまたはメモリカードにインストールされる他のあらゆるアプレットとは独立して制御する能力、を要求してもよい。銀行サービスは、その一例である。したがって、あるいは、デバイスのセキュアエレメントまたはメモリカードには、複数のアプレットが記憶されてもよい。各アプレットは、所定のアプレットに関連する第三者サービスにアクセスするための資格認証情報を生成する前に、別個の認証プロセスを実行してもよい。

【０１５０】

デバイスのセキュアエレメントまたはメモリカードとパーティションとの間の認証ステップだけでなく、本方法は、デバイスのセキュアエレメントまたはメモリカードと第三者サービスのセキュアエレメントとの間で第2の認証プロセスを実行するステップを含んでもよい。これは、第三者サービスが追加のセキュリティを要求し、よって第三者サービスが認証プロセスに対する制御を要求する、という場合であってもよい。第三者サービスは、例えば、銀行であってもよい。

【０１５１】

したがって、資格認証情報を送信するステップ（iv）は、デバイスのセキュアエレメントまたはメモリカードと第三者サービスのセキュアエレメントとの間で相互的な認証プロセスを実行するステップと、デバイスのセキュアエレメントまたはメモリカードと第三者サービスのセキュアエレメントとの間にセキュアなチャネルを生成するステップと、資格認証情報を暗号化するステップと、暗号化された資格認証情報を、セキュアなチャネルを介して第三者サービスのセキュアエレメントへ送信するステップと、を含む。

【０１５２】

第三者サービスは、第三者サービスにアクセスするためのパスコード／PINを要求してもよく、パスコード／PINは、好ましくは、セキュアエレメントまたはメモリカードと第三者サービスのセキュアエレメントとの間に生成されるセキュアなチャネルを介して送信される。

【０１５３】

好ましくは、第三者サービスにアクセスするための資格認証情報、および／または第三者サービスにより要求されるフォーム記入用データは、自動的に、セキュアエレメントまたはメモリカードからセキュアなチャネルを介して第三者パーティションへ提供され、かつ次には、成功裡に完了した第2の認証プロセスに続いて、要求があれば、第三者サービスへ提供される。

【０１５４】

第三者サービスは、成功裡に完了した第2の認証プロセスに続いて、自動的に開始されてもよい。

【０１５５】

デバイスは、マスタデバイスとして作動し、さらなるデバイス（例えば、PCまたはタブレット）も第三者サービスへアクセスできるようにしてもよい。このような場合、アクセスコードが発生されてデバイス上に表示されても（あるいは、例えばSMSまたはeメールによってユーザへ送信されても）よく、かつユーザにより、さらなるデバイスを用いて、第三者サービスに関連づけられるウェブサイトへ入力されてもよい。アクセスコードは、好ましくは、デバイス上で実行されるアプリケーションによって発生されてもよい。

【０１５６】

あるいは、マスタデバイスは、（別のデバイスのためにアクセスコードを発生させる）

この同じ機能を、非マスタデバイスへ付与してもよい。

【０１５７】

アクセスコードは、時間的制約のあるものであってもよく、即ち、所定の時間期間に渡ってのみ有効であってもよい。期間は、例えば、1、5、10、15、20、25、30、45、60、90または120分までであってもよい。

【０１５８】

マスタデバイスは、新しい資格認証情報を生成するため、または第三者サービスにアクセスするための資格認証情報を更新するために使用されてもよい。さらなるデバイスがパーティションに（かつ必然的に、このパーティションに関連づけられるウェブサービスにも）接続されると、資格認証情報は、これらの接続されたデバイス（即ち、デバイスおよびさらなるデバイス）間で同期されてもよい。あるいは、または追加的に、パーティションのコンテンツは、接続されたデバイス間で同期されてもよい。例えば、デバイスから新しい資格認証情報、新しいサービスまたは新しいコンテンツが利用可能になれば、さらなるデバイスは、接続されかつ成功裡に認証プロセスを通れば、これらを瞬時に利用できるようになる。

【０１５９】

デバイスは、パーティションにアクセスしかつパーティションから第三者サービスを開始するために、NFC（近距離無線通信）タグからコードを読み取ってもよい。NFCタグは、デバイスへ、パーティションを選択し（そうでなければ、ユーザはこれを入力する必要がある）かつ最終的にこれを開くために必要な情報を提供してもよい。

【０１６０】

あるいは、デバイスは、パーティションにアクセスしかつパーティションから第三者サービスを開始するために、生体センサ／リーダからコードを読み取ってもよい。生体センサ／リーダは、デバイスへ、パーティションを選択し（そうでなければ、ユーザはこれを入力する必要がある）かつ最終的にこれを開くために必要な情報を提供してもよい。

【０１６１】

別の実施形態において、デバイスは、パーティションを選択し（そうでなければ、ユーザはこれを入力する必要がある）かつ最終的にこれを開くために必要な情報をデバイスへ提供し得る信号放出デバイスから、コードを受信してもよい。信号放出デバイスは、Bluetooth（登録商標）、BLE（低電力ブルートゥース（登録商標））、wifi、zigbee、NFC、GPSまたはISO14443デバイスであってもよく、または、他の任意形式の非接触通信を利用するデバイスであってもよい。

【０１６２】

各パーティションは、電話またはメッセージングサービスのための一意の識別子を記憶してもよい。電話またはメッセージングサービスは、例えば、モバイルフォン電話サービス、VOIPサービスまたはインスタント・メッセージング・サービスであってもよい。一意の識別子は、ユーザ名およびパスワードまたは電話番号（国内または国際）等の電話またはメッセージングサービス識別子へリンクされてもよい。

【０１６３】

パーティションは、各々が一意の識別子を有して複数で存在してもよい。一例として、一名のユーザは、各々が異なる電話番号にリンクされる、各々が一意の識別子に関連づけられる10個のパーティションを有してもよい。

【０１６４】

デバイスのセキュアエレメントまたはメモリカードには、一意の識別子と電話またはメッセージングサービス識別子との間のマッピングが記憶されてもよい。あるいは、マッピングは、クラウド内に記憶されてもよい。あるいは、移動ネットワークのオペレータが、電話またはメッセージングサービス識別子への一意の識別子のマッピングを促進してもよい。

【０１６５】

識別子がパーティションに記憶されることから、ユーザがデバイスからパーティション

にアクセスすることができる限り、ユーザは、（どのデバイスを用いてパーティションにアクセスしているかに関わらず）電話またはメッセージングサービスにアクセスすることができる。したがって、ユーザは、使用するデバイスに関わらず、その電話またはメッセージングサービスに関連づけられるあらゆる音声、テキストまたはデータメッセージを送信または受信する能力を有することになる。

【０１６６】

特定の電話またはメッセージングサービス識別子および関連の電話またはメッセージングサービスは、ユーザのロケーションに依存して起動されてもよい。これは、ユーザのロケーションが2または3ファクタ認証プロセスの一部である場合であってもよい。例えば、パーティションへホームwi-fiネットワークを介して接続する場合、デバイス上で家庭の電話番号が起動されてもよい。同様に、接続が他国のGPSまたは4G基地局を介して行われれば、その領域内の現地の電話番号がデバイス上で起動されてもよい。例えば、ユーザがフランスへ旅行すれば、ユーザが使用するために、フランスの電話番号が発生されてもよい。フランスを出国する際に、ユーザには、その番号を保持するか、別のユーザが使用できるように手放すかの選択が与えられてもよい。

【０１６７】

可能な別のアプリケーションは、従業員が雇用者から業務用に携帯電話を与えられる、という場合である。従業員は、個人的な電話および業務用の電話の双方を携帯することを望まないことがある。代わりに、従業員は、その個人的な電話番号にリンクされる一意の識別子を有する（業務用電話に関連づけられる）パーティションを生成してもよい。したがって、従業員は、業務用携帯電話を用いて、雇用者の電話契約を用いることなく電話呼の送受信を行ってもよい。

【０１６８】

また、本発明は、デバイスによるクラウドベースまたはウェブベースの第三者サービスへのアクセスを制御するためのコンピュータプログラムにも拡大され、前記プログラムは、これまでに述べた態様における方法（および／または、これまでに述べたような方法の好適な特徴）を実行するように構成される。

【０１６９】

本発明のあらゆる態様は、好適または任意選択の特徴を含む、本発明のあらゆる他の態様のあらゆる特徴を含んでもよい。

【０１７０】

したがって、本発明は、これまでに述べた本発明の全ての態様（およびその好適な特徴）において規定されているデータ・アクセス・コントローラ、デバイスをデータ・アクセス・コントローラに登録する方法、デバイスとアクセスコントローラとを備えるシステム、デバイスの登録を制御するためのコンピュータプログラム、デバイスにおいてデータへアクセスする方法、デバイスにおけるデータへのアクセスを許可する方法、第1のデバイスと第2のデバイスとデータ・アクセス・コントローラとを備えるシステム、にも拡大され、アクセスされるべきデータは、クラウドベースまたはウェブベースの第三者サービスであり、かつ／またはデータにアクセスする要求は、クラウドベースのパーティションによって送信されかつ／または受信される。

【０１７１】

クラウドベースまたはウェブベースの第三者サービスへのアクセスに関連する後者の2態様の好適な特徴は、これまでに述べた本発明の全ての態様（およびその好適な特徴）において規定されているデータ・アクセス・コントローラ、デバイスとアクセスコントローラとを備えるシステム、デバイスの登録を制御するためのコンピュータプログラム、デバイスにおいてデータへアクセスする方法、デバイスにおけるデータへのアクセスを許可する方法、第1のデバイスと第2のデバイスとデータ・アクセス・コントローラとを備えるシステムと組み合わせて解釈されてもよい。

【０１７２】

パーティションには、複数のスマートオブジェクト・ロックがかかってもよい。例えば

、パーティションは、2つ以上の異なるユーザがパーティションにログインされる場合にのみ開かれてもよい。これは、企業ランドスケープにおける文書の共有または秘密会議の実施に関して言えば、特に適切である。パーティションを開くための複数のスマートオブジェクトの使用は、第三者ベンダとのトランザクション、またはそれほど改まったものではない、セキュアな環境を必要とするピアツーピア・トランザクション等のトランザクション、といったサービスを許可する場合に第三者の同一性を保護するためにも使用される可能性がある。

【０１７３】

これまでに述べた態様の多くは、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードを基礎とする、データへのアクセスが許可されるべきか拒絶されるべきかの検証（または同様のステップ）を参照する。

【０１７４】

これらの態様は、パーティションにアクセスするために、2（以上の）ファクタ認証を提供することができてもよい（但し、アクセスには、パーティションの生成、編集または削除が含まれる）。認証の1つのファクタは、デバイスに関連づけられるスマートオブジェクト（メモリカードまたはセキュアエレメント）の識別コードであってもよく、かつさらなる1つ以上のファクタは、パスコードまたはPIN、または何らかの形式の遺伝学的または生体測定的識別データ、またはロケーション、または時間、または別のメンバ（例えば、管理者）またはユーザの属するグループがデータにアクセスしているかどうか、であってもよい。

【０１７５】

これまでに論じたものに対応する態様では、ファクタの1つが、デバイスに関連づけられるメモリカードまたはセキュアエレメントの識別コードである必要はない。

【０１７６】

したがって、本発明のさらなる態様では、パーティションとデバイスとの間で相互的な認証を実行するステップと、パーティションとデバイスとの間にセキュアなチャネルを生成するステップとを含む、デバイスからパーティションにアクセスする方法が提供されており、前記認証は、2つ以上のファクタを含み、前記ファクタは、次のリスト、即ち、デバイスに関連づけられるスマートオブジェクト（メモリカードまたはセキュアエレメント）の識別コード、パスコードまたはPIN、何らかの形式の遺伝学的または生体測定的識別データ、ロケーション、時間、または別のメンバ（例えば、管理者）またはユーザの属するグループがデータにアクセスしているかどうか、から選択される。好ましくは、「アクセスする」という用語は、パーティションを生成、編集または削除することを含む。

【０１７７】

このリストに含まれるファクタについては、これまでの説明において、本発明の先の態様を参照して詳しく論じている。

【図面の簡単な説明】

【０１７８】

以下、図面を参照して、本発明の好適な実施形態を単なる例示として説明する。

【図１】図1は、携帯電話とその対応するクラウドベースのリモートストレージとを備えるシステムを示す概略図である。

【図２】図2は、携帯電話およびタブレットデバイスとその対応するクラウドベースのリモートストレージとを備えるシステムを示す概略図である。

【図３】図3は、携帯電話から、遠隔に記憶されているデータへの、認証された、および認証されていないアクセス試行を示す概略図である。

【図４】図4は、携帯電話から、遠隔に記憶されているデータへの、認証された、勧誘された、および認証されていないアクセス試行を示す概略図である。

【図５】図5は、アクセス監視を有する携帯電話から、遠隔に記憶されているデータへの、認証された、勧誘された、および認証されていないアクセス試行を示す概略図である。

【図６】図6は、アクセス監視のない携帯電話から、遠隔に記憶されているデータへの、

認証された、勧誘された、および認証されていないアクセス試行を示す概略図である。
【図７】図7は、パーティションにアクセスできるようにデバイスを登録するためのプロセスを示すフロー図である。
【図８】図8は、認証プロセスを示すフロー図である。
【図９】図9は、アクセスコード暗号化プロセスを示すフロー図である。
【図１０】図10は、モバイルデバイスと、クラウドと、第三者ウェブサービスとを備えるシステムを示す概略図である。
【図１１】図11は、高いセキュリティを要求する、モバイルデバイスと、クラウドと、第三者ウェブサービスとを備えるシステムを示す概略図である。
【発明を実施するための形態】
【０１７９】
図1に示されているように、携帯電話1は、SIM2を備え、かつクラウドサーバ4内のデータストレージ・パーティション3a、3b、3cへのアクセスを有する。SIM2は、リモート・データ・パーティションにアクセスするためのソフトウェアを含む。
【０１８０】
携帯電話1がパーティション3a、3bまたは3cにアクセスできるのは、パーティション3a、3bまたは3cの正しいパスコードまたはPINを入力した時に限られる。各パーティションは、ユーザにより設定される固有のパスコードまたはPINを有する。
【０１８１】
パーティション3a、3bまたは3c内のデータへのアクセスが認可されるためには、正しいパスコードまたはPINに加えて、正しいSIM2からの識別コードも提供されなければならない。
【０１８２】
ユーザは、特定のパーティション3a、3bまたは3cへのアクセスを希望する場合、そのパーティション3a、3bまたは3cのパスコードまたはPINを、携帯電話1のキーパッドでのタイピングまたはタッチ感応画面によって入力する。入力されたパスコードまたはPINは、次にSIM2へ送られ、ここで、パスコードまたはPINをSIM識別コードと組み合わせる暗号化アルゴリズムに送られてハッシュが生成される。
【０１８３】
ハッシュは、次に、クラウドサーバ4におけるプロセッサへ送られ、ここで復号されて、パスコードまたはPINが抽出され、かつユーザがどのパーティション3a、3bまたは3cへのアクセスを求めているかが識別される。次に、このハッシュがクラウドサーバ4におけるメモリにそのパーティション3a、3bまたは3cに関して既に記憶されているハッシュに一致すれば、要求されているパーティション3a、3bまたは3cへのアクセスが許可され、かつこのパーティション3a、3bまたは3cに記憶されているデータは、携帯電話1を介してアクセスされることが可能である。
【０１８４】
幾つかの実施形態において、パーティション3a、3bまたは3cへのアクセスが認可されるためには、ユーザが有する「何か」、例えば遺伝学的または生体測定的IDの形式（例えば、指紋または虹彩スキャン）等の第3の形式の認証も必要とされる。他の実施形態では、これが、パーティション3a、3bまたは3cのパスコードまたはPINの代わりに要求される。
【０１８５】
各パーティション3a、3bおよび3cに記憶されるコンテンツまたはデータは暗号化され、よって、特定のパーティション3a、3bまたは3cへのアクセスが許可されると、このパーティション3a、3bまたは3cのコンテンツは、パーティション3a、3bまたは3cのパスコードまたはPINおよびSIM識別コードまたはSIM2に記憶されているキーを用いて復号される。
【０１８６】
パーティション3a、3bまたは3cへのアクセスが認可されていて、そのコンテンツが復号されると、このコンテンツを携帯電話1の画面上で見ることができる。
【０１８７】

携帯電話1は、パーティション3a、3bおよび3cを制御する管理者デバイスである。しかしながら、ユーザ（または他のユーザ）は、さらなるデバイスからパーティション3a、3bおよび3cへのアクセスを希望してもよい。例えば、図2に示されているように、ユーザは、SIM5aを有するタブレットデバイス5を有し、これからパーティション3a、3bおよび3cへのアクセスを希望する。タブレットデバイス5において正しいPINまたはパスコードおよび／または正しい遺伝学的または生体測定的情報が入力されると、タブレットデバイス5にパーティション3a、3bまたは3cへのアクセスが認可されるように、タブレットデバイス5のSIM5aもパーティション3a、3bまたは3cに登録される。パーティション3a、3bまたは3cへのアクセスが認可される方法は、携帯電話1に関して先に述べたものと同じ方法で制御される。

【０１８８】

図3は、非認証ユーザがクラウドサーバ4に記憶されているパーティション3Mへのアクセスを求める事例を示している。非認証ユーザは、各々SIM7aまたは7bを有する携帯電話6aまたは6bを有する。パーティションへのアクセスは、アクセスコントローラ12によって制御される。アクセスコントローラ12は、クラウド内に構成される。実施形態によっては、アクセスコントローラ12は、携帯電話プロバイダシステムの一部である。

【０１８９】

非認証ユーザは、その携帯電話6aまたは6bにPINまたはパスコードを入力するが、PINまたはパスコードが不正確であり、かつ／またはSIM識別コードが不正確であることから、パーティション3Mへのアクセスは認可されない。アクセスコントローラ12は、携帯電話6aおよび6bがパーティション3Mへアクセスすることを許可しない。しかしながら、これは、メイン携帯電話1がパーティション3Mへアクセスすることを許可する。

【０１９０】

図4は、非認証ユーザおよび勧誘されたユーザがクラウドサーバ4に記憶されているパーティション3Mへのアクセスを求める事例を示している。

【０１９１】

この場合も、図3の事例と同様に、アクセスコントローラ12は、非認証ユーザの携帯電話6aに対し、パーティション3Mへのアクセスを拒絶する。

【０１９２】

勧誘されたユーザにアクセスが認可されるためには、メインユーザがその携帯電話1からクラウドサーバ4へ、パーティション3Mへのアクセスに関するワンタイムパスワード（OTP）の要求を送信する。クラウドサーバ4は、携帯電話1のSIM2の識別コードがパーティション3Mに登録されていること、およびこのSIM2に関連づけられるユーザが、パーティション3Mへアクセスするように他のユーザを勧誘することを許可されていることについて検証し、これが事実であれば、携帯電話1へOTPを送信し返す。メインユーザは、次に、このOTPを勧誘されたユーザの携帯電話8へ送信する。勧誘されたユーザは、次に、アクセスコントローラ12へパーティションMにアクセスする要求を送信してOTPを入力する。アクセスコントローラ12は、OTPを検証し、OTPが正しいものであれば、勧誘されたユーザは、パーティション3Mへのアクセスを認可される。

【０１９３】

代替実施形態（不図示）において、メインユーザは、その携帯電話1内でOTPを生成し、次に、パーティション3Mに対する登録のために、このOTPをクラウドサーバ4へ送信する。また、OTPは、携帯電話1から、勧誘されたユーザの携帯電話8へも送信される。パーティション3Mに対してOTPが登録されると、勧誘されたユーザは、先に述べたように、OTPを入力してパーティション3Mにアクセスすることができる。

【０１９４】

実施形態によっては、OTPは、5分等の所定の時間期間でのみ有効である。

【０１９５】

実施形態によっては、勧誘されたユーザによるパーティション3Mへのアクセスは、1－24時間等の所定の時間期間でのみ認可される。

【０１９６】
実施形態によっては、OTPは、パーティション3Mに対する1回のアクセス試行に対してのみ有効である。一度使用されると、これを再度用いて3Mにアクセスすることはできない。引き続きパーティション3Mにアクセスするためには、メインユーザによってさらなるOTPが要求されなければならない。
【０１９７】
実施形態によっては、メインユーザは、所望されれば、勧誘されたユーザによるパーティション3Mへのアクセスを監視しかつ／または阻止することができる。
【０１９８】
クラウドサーバ4においてパーティションが設定される場合、これは、誰もがここに記憶されるデータにアクセスし得るように「オープンな」パーティションとして設定されてもよい。図5は、このようなオープンパーティション30Aの一例を示している。実施形態によっては、一部のユーザがパーティション30Aに記憶されているデータに対する「読取り」アクセスのみを有するのに対して、勧誘されるユーザおよび／またはメインユーザ等の他のユーザは、そこに記憶されているデータへの「読取り」および「書込み」アクセスの双方を有する。
【０１９９】
図5に示されている事例では、パーティション30Aが、メイン携帯電話1、勧誘されたユーザの携帯電話8および別の（勧誘されていない）ユーザの携帯電話10からアクセスされるオープンパーティションであることから、パーティション30Aへのアクセスは、メモリ30A-hにおいて監視されかつ記録される。記録されるデータは、例えば、パーティション30Aにアクセスするデバイスに関連づけられる識別コードおよび／またはアクセス試行の時刻より成る。他のデータも、記録されてもよい。これにより、メインユーザは、パーティション30Aへのアクセスを監視し、かつ記録されるデータに基づいて、かつ所望されれば、特定のユーザによるパーティション30Aへのアクセスを阻止することができるようになる可能性がある。
【０２００】
図6は、図5に類似するものであるが、パーティション30Aへのアクセス監視のないことが異なる。
【０２０１】
デバイスを登録して特定のパーティションにアクセスできるようにするためには、デバイスが、パーティションにアクセスするための適切なソフトウェア（例えば、アプリケーション）をインストールしていなければならない。これは、例えば、デバイスに関連づけられるセキュアエレメントまたはメモリカードに記憶される。
【０２０２】
デバイスを登録して特定のパーティションにアクセスできるようにするためには、次に、図7に示されているような下記のプロセスが実行される。
【０２０３】
S1において、登録されるべきデバイスのユーザは、1つ以上のパーティションへのアクセスを得るための要求を、デバイスから管理者デバイスへパーティション・アクセス・コントローラを介して送信する。要求は、例えば、eメールまたはSMSの形式である。要求は、認証された2ファクタコードを含む。このコードは、デバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードから、およびパスコードまたはPINまたはユーザに固有の何かを表すデータの何れかから生成される。これにより、どのデバイスがパーティションへのアクセスを要求しているかを監査可能な追跡が可能になる。
【０２０４】
S2において、パーティション管理者は、管理者デバイスにおいて要求を受信すると、パーティションへのアクセスを認可すべきか、アクセスを拒絶すべきかを決定する。管理者は、ユーザに対する、読取り専用、またはパーティションにおけるコンテンツを編集し／削除し／追加する能力等のアクセス許可も設定することができる。

【０２０５】
所有者は、ユーザに対してパーティションへのアクセスを許可することを決定すると、S3において、管理者デバイスからアクセスコントローラへ、デバイスがパーティションにアクセスできるようにデバイスがパーティションに対して（管理者により指定されるアクセスパーティションへ）登録されることに同意する旨を確認する信号を送信する。
【０２０６】
次に、S4において、アクセスコントローラは、デバイス（即ち、そのメモリカードまたはセキュアエレメントに関連づけられる識別コード）を、パーティションに対して、指定されたアクセスパーティションに登録する。
【０２０７】
ユーザは、パーティションにアクセスするためにアプリケーションを開く、またはこれにログインすると、PINまたはパスコード、またはそのパーティションに対応するユーザに固有の何かを表すデータを入力することによってパーティションにアクセスすることができる。異なるデバイスは、異なるPINまたはパスコード、または所定のパーティションにアクセスするためのユーザに固有の何かを表すデータを保有することができる。
【０２０８】
登録されるべきデバイスのユーザは、管理者と同じ者であることも、異なる者であることも可能である。
【０２０９】
パーティションの管理者もまた、誰かをパーティションにアクセスするように勧誘して、その旨の勧誘を送信することができる。上述の事例と同様に、勧誘されたユーザは、そのデバイスにパーティションへアクセスするための適切なソフトウェア（例えば、アプリケーション）をインストールしていなければならない。勧誘は、アクセスコントローラを介して送信される。勧誘は、eメールまたはSMSメッセージ等のメッセージ形式であることが可能であり、かつ／またはこれは、パーティション・アクセス・アプリケーション内のメッセージングシステムを介して送信されかつ閲覧可能である可能性もある。ユーザは、このアプリケーションを開く、またはこれにログインすると、特定のパーティションへアクセスするための勧誘が受信されていることに気づく。次に、ユーザは、パーティションにアクセスすることができる。
【０２１０】
勧誘は、ユーザが（パーティション・アクセス・アプリケーション経由ではなく）ウェブブラウザを介してパーティションへアクセスするために、ウェブブラウザに入力できるOTP（ワンタイムパスワード）を含むことが可能である。
【０２１１】
ユーザは何れも、パーティション・アクセス・アプリケーションを開く、またはこれにログインするために、アプリケーション用のPINまたはパスコードまたは生体測定的情報を入力しなければならず、これが、ユーザデバイスに関連づけられるセキュアエレメントまたはメモリカードの識別コードと共にチェックされる。
【０２１２】
図8は、デバイスの認証または検証プロセスの一実施形態を示すフロー図である。S5において、デバイスのユーザは、ユーザデバイス上でパーティション・アクセス・アプリケーションを開いてログインする。これにより、アプリケーションが開いていることを示す信号がパーティション・アクセス・コントローラへ自動的に送信される。次には、マシンーマシンのハンドシェイクが実行されるが、これには、アクセスコントローラがSIM（または他のセキュアエレメントまたはメモリカード）の識別コードの登録をチェックすること、ならびにデバイスがアクセスコントローラのID証明をチェックすること、が含まれる。これは、アクセスコントローラからデバイスへ「チャレンジ」が送信され、デバイスがこれに「回答」で応答することによって実行される。これらのチェックが正当であると確認されると、デバイスとアクセスコントローラとの間にセキュアなチャネルが開かれる。
【０２１３】

次に、S6において、アクセスコントローラは、セキュアなチャネルを介して、アクセスを希望するパーティションに対するPINまたはパスコードをユーザが入力するように、要求をデバイスに送信する。

【０２１４】

S7において、ユーザは、PINまたはパスコードを入力し、SIM（または、デバイスに関連づけられる他のセキュアエレメントまたはメモリカード）は、それが正しいことをチェックする。正しければ、SIM（または他のセキュアエレメントまたはメモリカード）は、入力されたPINまたはパスコードに基づいて証明(certificate)を生成する。

【０２１５】

ある代替実施形態では、PINまたはパスコードの代わりに、またはこれに加えて、ユーザは、生体測定的データ等のユーザ固有の何かを表すデータを要求されてもよく、その場合にはこれを入力する。証明は、このデータに基づくものとなり得る。

【０２１６】

次に、S8において、生成された証明は、デバイスからセキュアなチャネルを介してアクセスコントローラへ送信される。

【０２１７】

S9において、アクセスコントローラは、証明をチェックし、これが、要求されているパーティションに対して登録されていれば、デバイスによる要求されたパーティションへのアクセス許可が与えられ、デバイスは、要求されたパーティションにアクセスする。

【０２１８】

図9は、勧誘されたユーザがパーティションにアクセスするためのアクセスコードを暗号化することができる方法を示すフロー図である。

【０２１９】

非登録デバイスから、別のユーザがパーティションにアクセスできるように（または、管理者がそのパーティションにアクセスできるように）、管理者がそのパーティションのアクセスコードを提供することを希望する場合、S10において、PIN要求がアクセスコントローラから管理者デバイスへ送信される。

【０２２０】

S11において、管理者が、管理者デバイスに、許可を希望するアクセス先であるパーティションに関してPINを入力すると、管理者デバイスのSIM（または、デバイスに関連づけられる他のセキュアエレメントまたはメモリカード）が暗号化コードを発生させる。

【０２２１】

次に、S12において、暗号化コードは、管理者デバイスからセキュアなチャネルを介してアクセスコントローラへ送信される。

【０２２２】

次に、S13において、アクセスコントローラは、このパーティションへのアクセスが続いて入力されれば当該アクセスが許可され得るように、この暗号化コードをパーティションに対して登録する。

【０２２３】

アクセスコントローラは、勧誘されたデバイスもパーティションにアクセスできるように、暗号化コードをセキュアなチャネルを介して勧誘されたデバイスへも送信する。

【０２２４】

実施形態によっては、暗号化コードの有効性は、1回のアクセスのみ、かつ／または制限された時間期間に限定される。他の実施形態では、暗号化コードは、無期限に有効であってもよく、または期限切れにならない。

【０２２５】

実施形態によっては、パーティション・アクセス・アプリケーションは、Apache Cordova Javascriptブリッジとしてアクセスされるapiである。これは、セキュアエレメントまたはメモリカードに記憶され、かつオンボードで（即ち、セキュアエレメントまたはメモリカード内で）発生される次のようなキーおよびPINを保持する。

【０２２６】
・　アプリケーション用の1つのRSA 2048公開鍵／秘密鍵ペア
・　ユーザを認証するためのパーティション毎に1つの可変サイズPIN
・　暗号化ファイルに用いるためのパーティション毎に1つの3DES-2マスターキー
サーバまたはアクセスコントローラは、デバイス毎に多様化されることが可能な2つの3DES-2マスターキーを保持する。これらの2つのキーは、その生成に続いてアプリケーションへ送信され、アプリケーション・セキュリティドメインのセキュアなチャネルによって保護される：
・　アプリケーションの真正を検証するために、セキュアエレメント・アプリケーションによって返される公開鍵データを暗号化するために使用される初期化キー
・　パーティションのリモート・アクセス・コードを発生させる際に、セキュアタイムのソースを提供するために使用される時間鍵
セキュアタイムは、ターゲットデバイスにより与えられるノンスであり、UNIX（登録商標）タイムスタンプ、時間鍵により暗号化された3DES-2 CBCがこれに続く。
【０２２７】
ターゲットファイルのサイズに従って、パーティションキーを用いてファイルデータを直に暗号化すること、または、キーをハンドセットで操作してファイルデータを暗号化することが可能である。
【０２２８】
以下、ユーザであるサラが、そのパーティションデータを別の人、ロバートと共有することを希望する場合に辿るプロセスについて説明する。
【０２２９】
前提条件：
●　ロバートのデバイスの公開鍵が、認証サーバ（アクセスコントローラ）に登録され、公開識別子（ロバートのeメール等）によって識別される
●　サラは、共有するためのパーティションへログオンする
●　サラは、このパーティションをロバートと共有することを要求する
○　サーバは、サラのアプリケーションに関してセキュアタイム・ノンスを取得する
○　サーバは、共にサラのアプリケーション用に暗号化されているロバートの公開鍵およびカレント・セキュアタイムを送信する
○　ハンドセットアプリケーションは、共有ブロブを取得し、かつ共有コードをサラへ表示する
○　共有ブロブはサーバへ送信されて、ロバートの公開IDに関連づけられる
○　サラは、共有コードをロバートへ（eメール、SMS、電話、音声...によって）提供する
●　ロバートは、サーバへ接続することによって、新しいパーティションが自分と共有されることを見てとり、サラにより提供される共有コードを入力する
○　サーバは、ロバートのアプリケーションに関するセキュアタイム・ノンスを取得する
○　サーバは、共有ブロブ、およびサラのアプリケーション用に暗号化されたカレント・セキュアタイムを送信する
○　パーティションのアクセスキーが、ロバートのセキュアエレメントまたはロバートのアプリケーションによって回復される
以下、低レベル管理APIを規定する：
isSecureElementPresent()
セキュアエレメントが存在すれば、真を返す
getSecureElementID()
（CPLCから抽出される）セキュアエレメントの一意のIDをHexStringとして返す
getCCSEApplicationVersion()
CCパーティションアプリケーションのバージョンを文字列として返すか、アプリケ

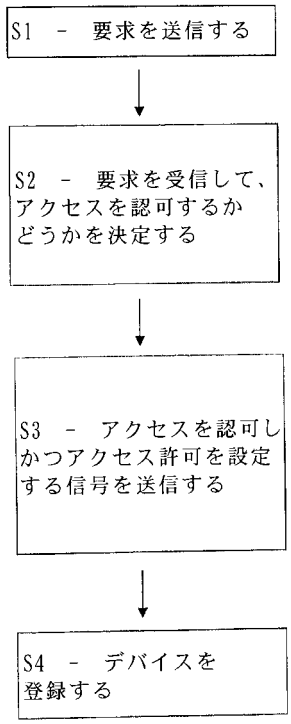
ーションがインストールされていなければ、「不確定」を返す
以下、アプリケーション更新および初期化APIを規定する：
getKeysetCounter(aid,keysetVersion)(HexString,Number)
所定のセキュリティドメインAIDおよびキーセットバージョンのカウンタを返す
executeAPDUScript(apdus)(Array of HexString)
セキュアエレメント上でAPDUスクリプトを実行し、各APDUに90 00ステータスワードを予期する。
【０２３０】
以下、高レベル管理APIを規定する：
getPublicKey()
初期化キーで暗号化されたアプリケーションの公開鍵、3DES-2 CBCを返す
createPartition(shortName,pin)(String,HexString)
ショートネームおよびPINを所与としてパーティションを生成し、1バイトのパーティションIDを返す
listPartitions()
セキュアエレメント上に生成されたパーティションを識別する［id,shortName］のアレイを返す
deletePartition(id)(Number)
パーティションを削除する。ユーザは、削除するためにパーティションへログオンしなければならず、またはパーティションのPINがブロックされなければならない
以下、使用APIを規定する：
loginPartition(id,pin)(Number,HexString)
所定のパーティションへログインする
logoutPartition()
その時点でログインされているパーティションからログアウトする
encryptData(data,iv)(HexString,HexString)
所定のIVおよびその時点で選択されているパーティションキーによる3DES-2 CBC暗号化を用いてデータを暗号化する
decryptData(data,iv)(HexString,HexString)
所定のIVおよびその時点で選択されているパーティションキーによる3DES-2 CBC暗号化を用いてデータを復号する
getSecureTimeNonce()
次のセキュアタイムを提供するために、サーバへ送られるべき8バイトのノンスを返す
getSharingCode(secureTime,encryptedPublicKey,validityMinutes)(HexString,HexString,Number)
別のデバイスに関する共有コードを得る。2エレメント、例えば、リモートデバイスへ送られるべきブロブおよび発生される8ディジットコード、のアレイを返す。ブロブは、 パーティションキーと連結されかつリモートデバイス公開鍵によりPKCS#1パディングを用いて暗号化された共有コードの有効期間の終わりのタイムスタンプを含む。他の実施形態において、コードは、任意の長さであることが可能であり、かつ／または英数字であることが可能である。
【０２３１】
useSharingCode(secureTime,blob,accessCode)(HexString,HexString,String)
リモートデバイスから取得される共有コードを用いる。ブロブ、アクセスコードおよび時間有効性がアプリケーションにより承認されれば、ファイルは、ユーザがログアウトするまで、またはセキュアエレメントの電源が切られるまで、抽出されるパーティションキーによりパーティションId 0xffを用いて暗号化されかつ復号されることが可能である。
【０２３２】

図10は、移動体デバイス1と、クラウド4と、第三者ウェブサービス14とを備えるシステムを示す概略図である。移動体デバイス1は、クラウドパーティション3dを介してウェブサービス14へのアクセスを許可するように動作可能なアプリケーションを実行するように構成される。アプリケーションが開始されると、ユーザは、PINコードを入力するように促される。正しいPINコードが提供されれば、クラウドパーティション3dが開かれる。パーティションが開かれると、ウェブサービス14にアクセスするための資格認証情報Cがパーティション3dから転送され、ウェブサービス14へのアクセスが許可される。

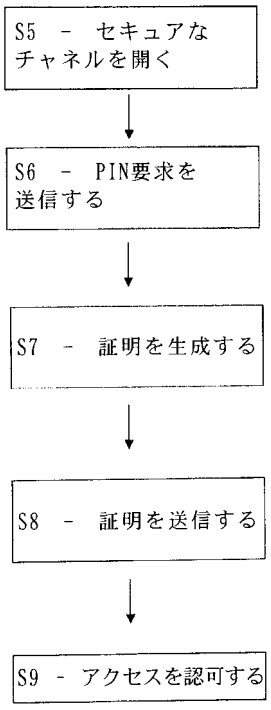
【０２３３】

図11は、図10に類似するシステムを示す概略図であるが、デバイスと第三者パーティション3eとの間で第2の認証が実行される事例を示している。図10の場合のように、移動体デバイス1は、クラウドパーティション3dを介してウェブサービス14へのアクセスを許可するように動作可能なアプリケーションを実行するように構成される。アプリケーションが開始されると、ユーザは、PINコードを入力するように促される。正しいPINコードが提供されれば、クラウドパーティション3dおよび第三者パーティション3eが開かれる。第三者パーティションは、次のステップ、即ち、デバイスから新しいPINコードを質問するステップと、正しいPINが受信されれば、デバイスのセキュアエレメントと第三者クラウドのセキュアエレメントとの間で相互的な認証プロセスを開始するステップとを含む新しいプロセスを開始する。ウェブサービス14にアクセスするための資格認証情報Cは、デバイスのセキュアエレメントから第三者パーティション3eへ転送され、これにより、ウェブサービス14へのアクセスが許可される。

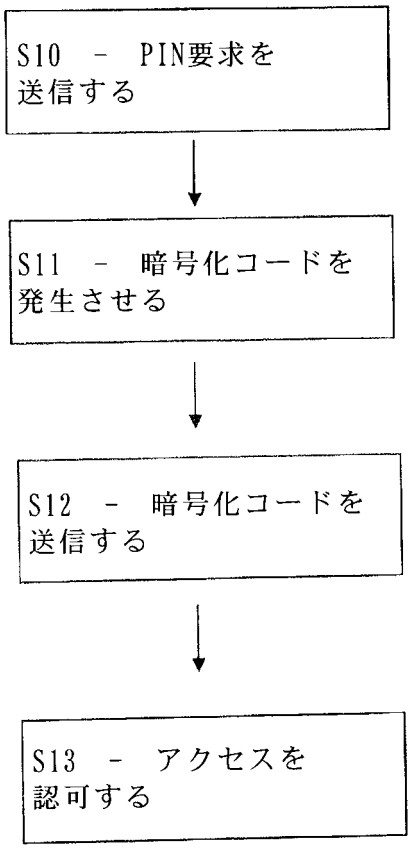
【図７】



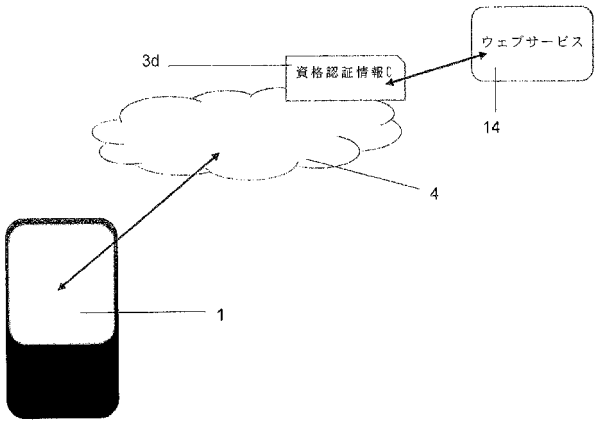
【図８】



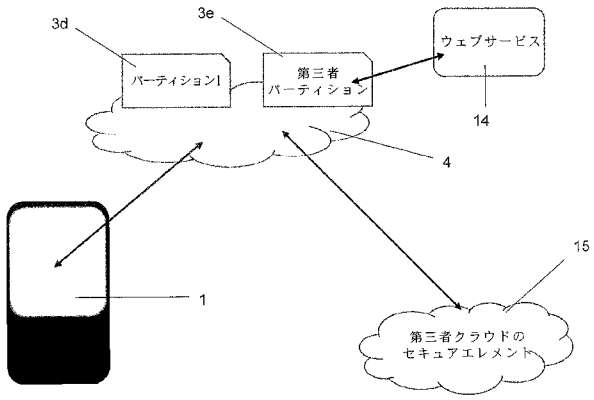
【図９】


S10 - PIN要求を送信する
S11 - 暗号化コードを発生させる
S12 - 暗号化コードを送信する
S13 - アクセスを認可する

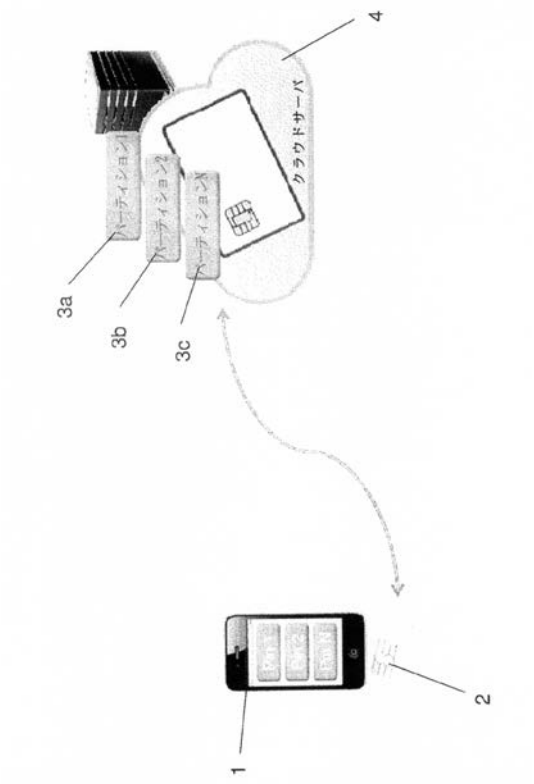
【図１０】


3d
資格認証情報
ウェブサービス
14
4
1

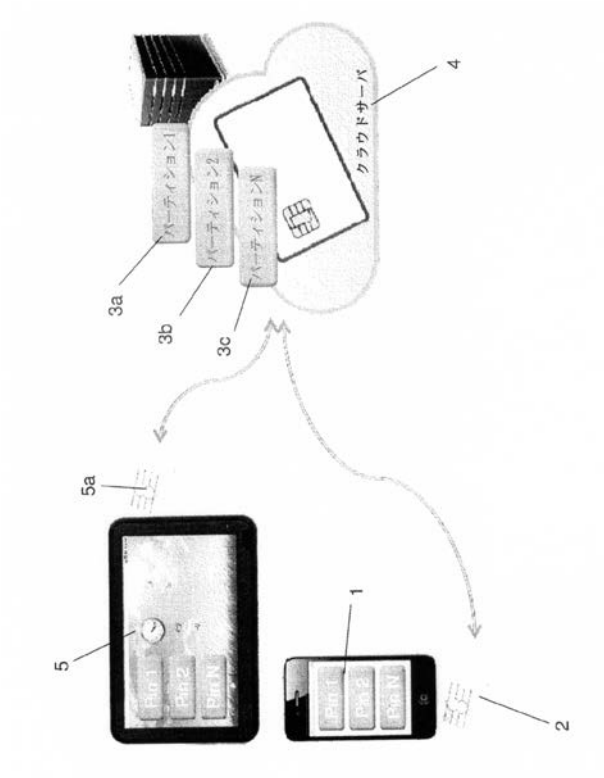
【図１１】


3d
3e
パーティション1
第三者パーティション
ウェブサービス
14
4
1
15
第三者クラウドのセキュアエレメント

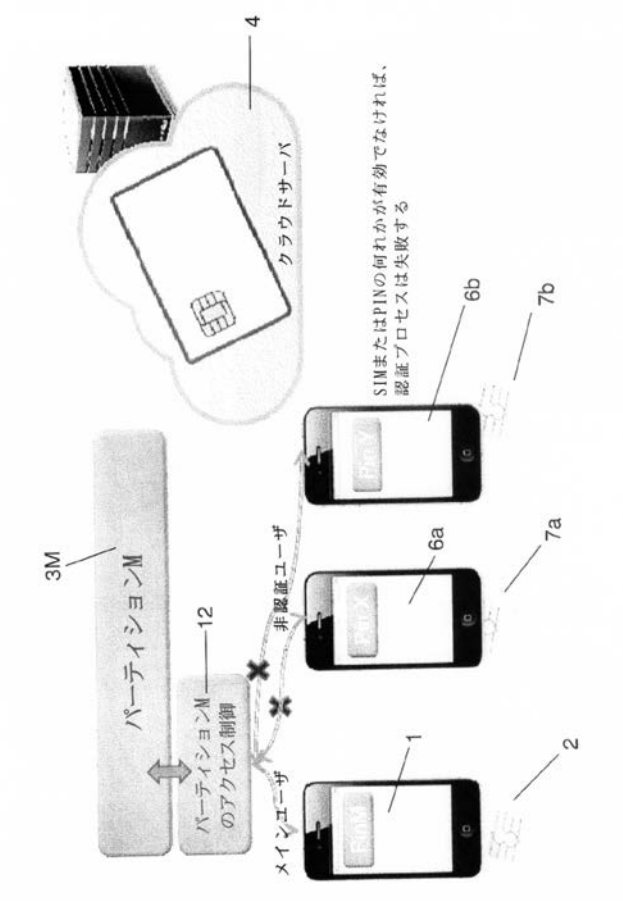
【図１】


4
クラウドサーバ
パーティション1
パーティション2
パーティション3
3a
3b
3c
2
1

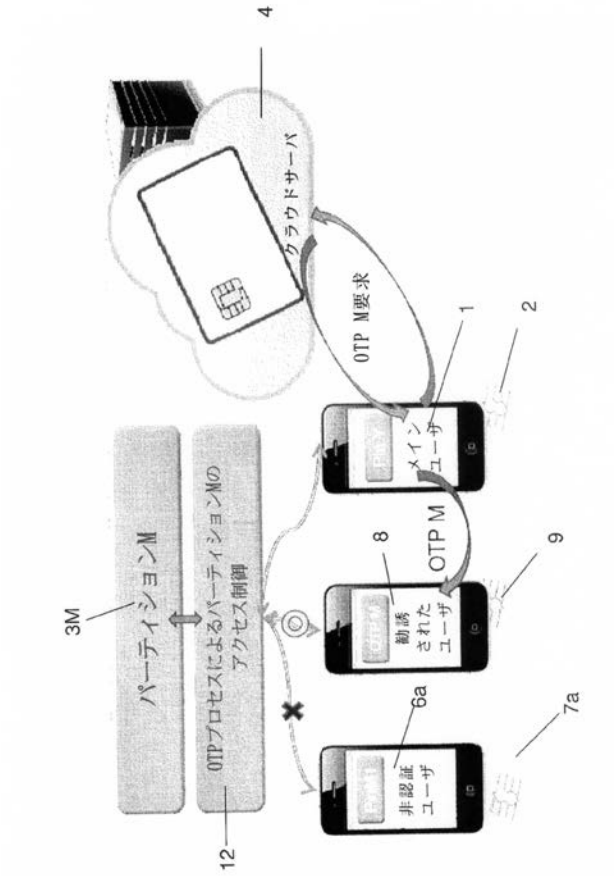
【図２】


パーティション1
パーティション2
パーティションM
クラウドサーバ
4
3a
3b
3c
5a
5
1
2
Pin1
Pin2
Pin N

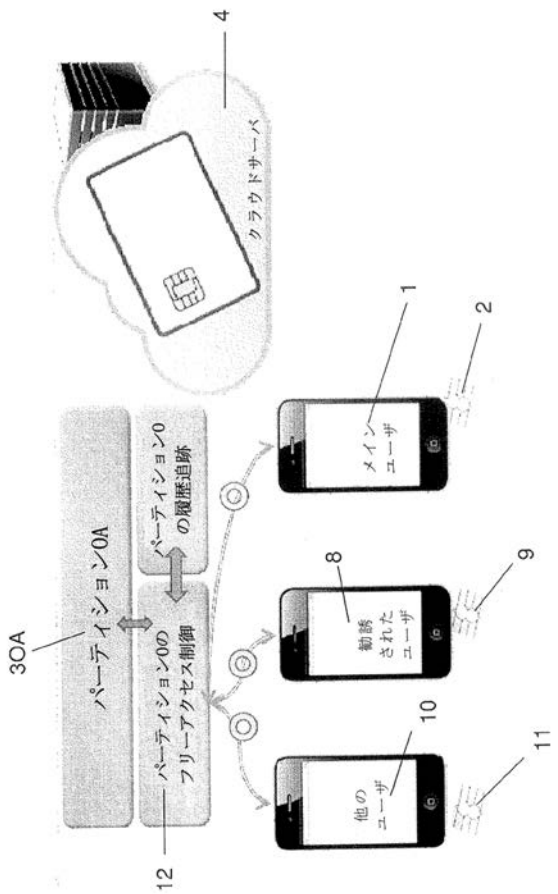
【図３】


4
クラウドサーバ
SIMまたはPINの何れかが有効でなければ、
認証プロセスは失敗する
6b
7b
3M
パーティションM
12
パーティションM
のアクセス制御
非認証ユーザ
6a
7a
メインユーザ
1
2
Pin Y
Pin X
Pin N

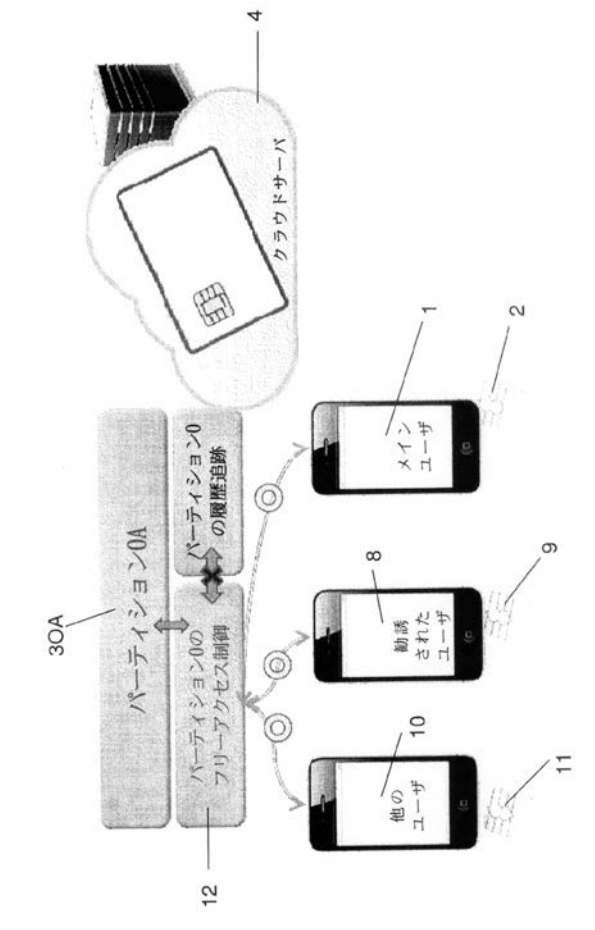
【図４】


4
クラウドサーバ
OTP M要求
1
2
3M
パーティションM
OTPプロセスによるパーティションMの
アクセス制御
メイン
ユーザ
8
OTP M
9
勧誘
された
ユーザ
6a
非認証
ユーザ
7a
12
Pin Y
Pin N

【図５】


4
クラウドサーバ
1
2
3OA
パーティションOA
パーティションOの
フリーアクセス制御
パーティションOの
履歴追跡
メイン
ユーザ
8
勧誘
された
ユーザ
9
10
他の
ユーザ
11
12

【図６】


4
クラウドサーバ
1
2
メイン
ユーザ
パーティション0
の履歴追跡
パーティション0A
30A
パーティション0の
フリーアクセス制御
8
9
勧誘
された
ユーザ
10
11
他の
ユーザ
12

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2014/052640

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/32 G06F21/34 G06F21/40 G06F21/73
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2010/323664 A1 (SIVARAM GIRISH [US] ET AL) 23 December 2010 (2010-12-23) paragraphs [0009] - [0014], [0017] - [0023], [0026] - [0028], [0032] - [0038], [0044] - [0048] figures 1a, 1b, 2a, 3a	1-100
X	US 2007/066288 A1 (SOELBERG EMILY L [US] ET AL) 22 March 2007 (2007-03-22) paragraphs [0002], [0008] - [0010], [0014] - [0019], [0023] - [0024] figures 1, 2	1-100
A	US 2007/094715 A1 (BROWN DARRYL J [US] ET AL) 26 April 2007 (2007-04-26) paragraphs [0004], [0011] - [0013], [0020] figures 1, 4	1-100

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 November 2014	25/11/2014

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Volpato, Gian Luca

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2014/052640

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2013/212653 A1 (HOGHAUG ROBERT JOHN [US]) 15 August 2013 (2013-08-15) paragraphs [0021] - [0026], [0036] figure 1 -----	1-100

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2014/052640

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010323664 A1	23-12-2010	NONE	
US 2007066288 A1	22-03-2007	NONE	
US 2007094715 A1	26-04-2007	NONE	
US 2013212653 A1	15-08-2013	US 2013212653 A1	15-08-2013
		WO 2013119967 A1	15-08-2013

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG

（特許庁注：以下のものは登録商標）
１．ＺＩＧＢＥＥ

Ｆターム(参考) 5J104 AA07 KA01 KA16 KA20 KA21 NA05 NA36