

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6633228号
(P6633228)

(45) 発行日 令和2年1月22日 (2020.1.22)

(24) 登録日 令和1年12月20日 (2019.12.20)

(51) Int. Cl.	F I	
GO 6 F 21/60 (2013.01)	GO 6 F 21/60	
GO 6 F 21/44 (2013.01)	GO 6 F 21/44	
HO 4 L 9/10 (2006.01)	HO 4 L 9/00	6 2 1 A
GO 6 F 21/31 (2013.01)	GO 6 F 21/31	
GO 6 F 21/35 (2013.01)	GO 6 F 21/35	

請求項の数 25 (全 25 頁)

(21) 出願番号	特願2018-553854 (P2018-553854)	(73) 特許権者	518236720
(86) (22) 出願日	平成29年1月3日 (2017.1.3)		クレブエックス エルエルシー
(65) 公表番号	特表2019-511791 (P2019-511791A)		C L E V X, L L C
(43) 公表日	平成31年4月25日 (2019.4.25)		アメリカ合衆国 98034 ワシントン
(86) 国際出願番号	PCT/US2017/012060		州 カークランド エヌイー ワンハンド
(87) 国際公開番号	W02017/123433		レッドアンドトゥエンティフィフス スト
(87) 国際公開日	平成29年7月20日 (2017.7.20)		リート 9306
審査請求日	令和1年5月22日 (2019.5.22)	(74) 代理人	100105957
(31) 優先権主張番号	14/987,749		弁理士 恩田 誠
(32) 優先日	平成28年1月4日 (2016.1.4)	(74) 代理人	100068755
(33) 優先権主張国・地域又は機関	米国 (US)		弁理士 恩田 博宣
早期審査対象出願		(74) 代理人	100142907
			弁理士 本田 淳

最終頁に続く

(54) 【発明の名称】 暗号を伴うデータセキュリティシステム

(57) 【特許請求の範囲】

【請求項 1】

データセキュリティシステムをセキュアにするための方法であって、

サーバによって認証される認証対象のユーザからの認証情報を、無線通信用の装置送受信機を有するワイヤレス装置にあるデータセキュリティシステムアプリケーションによって受信する工程であって、前記データセキュリティシステムは、ストレージサブシステム及び無線通信用のデータセキュリティ送受信器を備え、前記データセキュリティシステムアプリケーションは、前記ワイヤレス装置上で実行されて前記データセキュリティシステムとの接続状態を管理する、前記受信する工程と、

前記データセキュリティシステムアプリケーションによってかつ前記サーバから、前記認証情報に基づく前記ユーザの認証を要求する工程と、

前記サーバが前記ユーザを成功裏に認証したのに応答して、前記データセキュリティシステムアプリケーションによってかつ前記サーバから、前記ユーザによって前記データセキュリティシステムアプリケーションに提供された個人用識別番号に基づく前記データセキュリティシステムのアンロックを要求する工程であって、前記アンロックが、前記データセキュリティ送受信器と前記装置送受信機との間の無線接続を介して前記ワイヤレス装置から前記データセキュリティシステムに通信される、前記アンロックを要求する工程と、

前記サーバがアンロック信号を前記データセキュリティシステムアプリケーションに提供すると、前記データセキュリティシステムアプリケーションによって、前記ワイヤレス

10

20

装置から前記データセキュリティシステムへの接続状態をアンロックし前記ワイヤレス装置から前記データセキュリティシステムの前記ストレージサブシステムへのアクセスを可能にする工程とを備えることを特徴とする、データセキュリティシステムの動作方法。

【請求項 2】

前記ワイヤレス装置に対する前記無線接続の信号強度測定値に基づき前記データセキュリティシステムが前記ワイヤレス装置から近接範囲内にあるときに前記データセキュリティシステムアプリケーションが前記接続状態を維持する工程をさらに備える、請求項 1 に記載の動作方法。

【請求項 3】

所定の期間についての前記ワイヤレス装置に対する前記無線接続の信号強度測定値に基づき前記データセキュリティシステムが前記ワイヤレス装置から近接範囲内にあるときに前記データセキュリティシステムアプリケーションが前記接続状態を維持する工程をさらに備える、請求項 1 に記載の動作方法。

【請求項 4】

前記無線接続は、前記データセキュリティシステムと前記ワイヤレス装置との間の双方向通信を含む、請求項 1 に記載の動作方法。

【請求項 5】

前記無線接続は、前記データセキュリティシステムと前記ワイヤレス装置との間の単方向通信を含む、請求項 1 に記載の動作方法。

【請求項 6】

前記サーバは、ユーザ認証情報を有するユーザ管理データベースを含む、請求項 1 に記載の動作方法。

【請求項 7】

前記データセキュリティシステムは、前記データセキュリティシステムへのアクセスをコントロールするためのセキュリティコントローラをさらに備える、請求項 1 に記載の動作方法。

【請求項 8】

前記データセキュリティシステムのアンロックを要求する工程は、
前記データセキュリティシステムの識別情報を前記サーバに提供し、
前記データセキュリティシステムの前記識別情報が前記サーバにおいて有効である場合に前記データセキュリティシステムをアンロックすることをさらに備える、請求項 1 に記載の動作方法。

【請求項 9】

前記ワイヤレス装置にあるデータセキュリティシステム管理者アプリケーションが、
管理者パスワードを受け取り、
前記管理者パスワードを前記ワイヤレス装置から前記データセキュリティシステムに送信し、
前記データセキュリティシステムに前記管理者パスワードを設定し、前記データセキュリティシステムをアンロックすることをさらに備える請求項 1 に記載の動作方法。

【請求項 10】

前記データセキュリティシステムのアンロックを要求する工程は、
前記ワイヤレス装置から前記データセキュリティシステムに装置識別情報と共にアンロック要求を提供し、
前記データセキュリティシステムにおいて前記アンロック要求を受信し前記データセキュリティシステムをアンロックすることをさらに備える、請求項 1 に記載の動作方法。

【請求項 11】

前記認証情報は、ユーザ名またはパスワードまたはそれらの組み合わせを含む、請求項 1 に記載の動作方法。

【請求項 12】

前記データセキュリティシステムのアンロックを要求する工程は、

前記ワイヤレス装置から前記サーバに前記個人用識別番号を送信し、

前記ワイヤレス装置から前記個人用識別番号を受信した後、前記サーバによって、前記個人用識別番号が有効であるときを判定し、

前記サーバが前記個人用識別番号が有効であると判定した場合に、前記ワイヤレス装置を介して前記データセキュリティシステムをアンロックすることをさらに備える、請求項1に記載の動作方法。

【請求項13】

前記ワイヤレス装置が有効位置にあるときを前記サーバによって判定する工程と、

前記ワイヤレス装置が前記有効位置にあると前記サーバが判定したときに、前記データセキュリティシステムアプリケーションが、前記ワイヤレス装置を介して前記データセキュリティシステムをアンロックする工程とをさらに備える、請求項1に記載の動作方法。

10

【請求項14】

前記データセキュリティシステムアプリケーションが、前記ワイヤレス装置における現在時刻を判定する工程と、

前記データセキュリティシステムアプリケーションが、前記現在時刻を前記サーバに送信する工程と、

前記現在時刻が所定の時間範囲内にあるかどうかを判定するための条件を、前記サーバによってチェックする工程と、

前記ワイヤレス装置が前記所定の時間範囲内にあると前記サーバが判定した場合に、前記データセキュリティシステムアプリケーションが、前記データセキュリティシステムをアンロックする工程とをさらに備える、請求項1に記載の動作方法。

20

【請求項15】

前記ワイヤレス装置からのコマンド待機信号に応答して、前記サーバが、前記ワイヤレス装置にコマンドを提供する工程と、

前記コマンドが前記サーバから提供されたときに、前記ワイヤレス装置が、前記データセキュリティシステムにおいて前記コマンドを実行する工程とをさらに備える請求項1に記載の動作方法。

【請求項16】

前記ワイヤレス装置からのパスワード変更信号に応答して、前記サーバが、前記ワイヤレス装置にパスワード変更コマンドを提供する工程と、

前記データセキュリティシステムアプリケーションが、変更後パスワードコマンドで前記データセキュリティシステムをアンロックする工程とをさらに備える請求項1に記載の動作方法。

30

【請求項17】

前記データセキュリティシステムが、当該データセキュリティシステムに電力供給するためにホストコンピュータに接続されて、前記データセキュリティシステムを前記ホストコンピュータによって発見可能にする、請求項1に記載の動作方法。

【請求項18】

前記ワイヤレス装置から前記データセキュリティシステムの前記ストレージサブシステムへのアクセスは、前記無線接続から分離した外部通信チャンネル上で行われる、請求項1に記載の動作方法。

40

【請求項19】

データセキュリティシステムであって、

ワイヤレスデータセキュリティ送受信器と、

前記ワイヤレスデータセキュリティ送受信器に動作可能に接続された認証サブシステムと、

前記認証サブシステムに接続されたストレージサブシステムとを備え、

前記認証サブシステムは、前記ワイヤレスデータセキュリティ送受信器を介して、ワイヤレス装置にあるデータセキュリティシステムアプリケーションと通信するように構成さ

50

れており、

前記データセキュリティシステムアプリケーションは、ユーザによって提供された認証情報に基づき前記ユーザの認証を、サーバから、要求するように構成されており、

前記サーバによる前記ユーザの認証に応答して、前記データセキュリティシステムアプリケーションは、前記ユーザによって提供され前記ワイヤレスデータセキュリティ送受信器を介して前記ワイヤレス装置から前記データセキュリティシステムに送信された個人用識別番号に基づき前記データセキュリティシステムのアンロックを、前記サーバから、要求するように構成されており、

前記サーバが前記ワイヤレス装置にアンロック信号を提供したのに応答して、前記ワイヤレス装置は、前記アンロック信号を前記データセキュリティシステムに提供して前記ワイヤレス装置から前記データセキュリティシステムへの接続状態をアンロックするとともに前記ワイヤレス装置から前記データセキュリティシステムの前記ストレージサブシステムへのアクセスを可能にする、データセキュリティシステム。

【請求項 20】

前記ワイヤレスデータセキュリティ送受信器および前記認証サブシステムに接続されたセキュリティコントローラをさらに備える請求項 19 に記載のデータセキュリティシステム。

【請求項 21】

前記データセキュリティシステムアプリケーションは、前記ワイヤレス装置に対する無線接続の信号強度測定値に基づき前記データセキュリティシステムが前記ワイヤレス装置から近接範囲内にあるときに接続状態を維持するためのものである、請求項 19 に記載のデータセキュリティシステム。

【請求項 22】

前記データセキュリティシステムは、前記データセキュリティシステムが前記ワイヤレス装置から近接範囲内にあるときに接続状態を維持するために、及び、所定期間にわたってデータ読み出し動作またはデータ書き込み動作がないときに前記データセキュリティシステムをロックするために、セキュリティコントローラと通信する、請求項 19 に記載のデータセキュリティシステム。

【請求項 23】

前記データセキュリティシステムと前記ワイヤレス装置との間の無線通信が双方向通信を含む、請求項 19 に記載のデータセキュリティシステム。

【請求項 24】

前記データセキュリティシステムと前記ワイヤレス装置との間の無線通信が単方向通信を含む、請求項 19 に記載のデータセキュリティシステム。

【請求項 25】

ホストコンピュータと接続するための外部通信チャネルをさらに備える、請求項 19 に記載のデータセキュリティシステム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、一般に電子装置に関し、より詳細にはメモリ装置に関する。

【背景技術】

【0002】

セキュリティは、コンピュータの使用におけるほぼあらゆる面で重要な問題である。コンピュータに接続されるハードディスクドライブなどの記憶媒体には、データ盗難リスクのある貴重な情報が含まれている。個人情報、企業情報、および政府のセキュリティ情報を保護するために多額の資金と努力が払われている。

【0003】

ポータブルメモリストレージ装置は、小型になり、紛失し易くなり、一層ユビキタス化し、安価になり、その上、メモリ容量が増えてきているので、セキュリティ上の問題が顕

10

20

30

40

50

著になっている。ユニバーサルシリアルバスフラッシュドライブおよびマイクロドライブ、携帯電話、ビデオカメラ、デジタルカメラ、i P O D、M P 3 / 4 プレーヤー、スマートフォン、パームコンピュータ、ラップトップコンピュータ、ゲーム機器、オーセンティケータ、トークン（メモリを含む）等のポータブルメモリストレージ装置、一般には大容量ストレージ装置（M S D）に、大量の情報を秘密裏にダウンロードすることが可能である。

【0004】

具体的には、コンピュータから情報を簡単にダウンロードして持ち去ることのできる、バックアップ用、転送用、中間記憶用、および主記憶用の様々なM S Dがある。どんなM S Dであってもその主目的は、「ポータブルコンテンツ」つまり特定のコンピュータでは

10

【0005】

最も一般的なストレージセキュリティ提供手段は、コンピュータに入力したパスワードでユーザを認証することである。パスワードは、M S D格納値に対して検証され、一致した場合、ドライブが開かれることとなる。あるいは、パスワード自体がM S Dに格納されたデータを暗号化・復号化するための暗号鍵として使用される。

【0006】

オンザフライ暗号化をサポートするドライブの場合、暗号鍵は暗号化された形式で記憶媒体に保存されることもある。暗号鍵は記憶媒体に格納されるので、標準インターフェースを迂回して記憶媒体を直接読み取りたい者がそれをすぐに利用できるようになる。したがって、暗号鍵を暗号化するための鍵としてパスワードが使用される。

20

【0007】

自己認証ドライブの場合、それらの認証サブシステムがセキュリティ維持の責任を担い、その接続先のホストコンピュータに依存することはない。したがって、M S Dをアンロックするためにホストからパスワードは送信され得ない（その必要がない）。実際、記憶媒体に暗号鍵を保存する必要は最早なくなっており、認証サブシステムは、暗号鍵を管理する手段になっている。

【発明の概要】

【発明が解決しようとする課題】

【0008】

したがって、セキュリティ向上が依然として必要とされている。消費者の期待の高まりと、市場における有意な製品差別化の機会の薄れとともに、商業的競争圧力がいっそう高まっていることを鑑みると、これらの問題の解決策を見出すことが重要である。さらに、コストを削減し、効率とパフォーマンスを向上させ、競争圧力に対応する必要性によって、これらの問題に対する解決策を見出すための緊急性がさらに高まっている。

30

【0009】

これらの問題の解決策は長い間求められてきたが、先の開発は何ら解決策を教示も示唆もしておらず、したがってこれらの問題に対する解決策は長きにわたって当業者に見つけられずにいる。

【課題を解決するための手段】

40

【0010】

本発明は、データセキュリティシステムの動作方法を提供するものであり、その方法は、モバイル装置にデータセキュリティシステムとの接続のためのデータセキュリティシステムアプリケーションを提供する工程と、データセキュリティシステムアプリケーションを起動する工程と、データセキュリティシステムとモバイル装置との接続状態を維持する工程とを含む。

【0011】

本発明は、データセキュリティ送受信器または受信器と、前記データセキュリティ送受信器または受信器に動作可能に接続された認証サブシステムと、前記認証サブシステムに接続されたストレージサブシステムとを備えるデータセキュリティシステムを提供する。

50

【0012】

本発明の特定の実施形態は、上記の態様に加えてまたはその代わりに他の態様を有する。それら態様は、添付図面を参照して以下の詳細な説明を読むことにより、当業者に明らかになるであろう。

【図面の簡単な説明】

【0013】

【図1】本発明の一実施形態によるデータセキュリティシステムの概略図。

【図2】データセキュリティシステムを用いて使用される認証鍵配信方法を示す図。

【図3】ユーザがデータセキュリティシステムと対話するための別のシステムを示す図。

【図4】ユーザがホストコンピュータシステムを使用してデータセキュリティシステムと対話する方法を示す図。

10

【図5】データセキュリティシステム用のユーザ検証を用いるデータセキュリティ方法を示す図。

【図6】例示的なデータセキュリティ通信システムを示す図。

【図7】モバイル装置とデータセキュリティシステムとの動作のシーケンスを示す管理者シーケンス図。

【図8】モバイル装置が認証因子である場合のアンロックシーケンス図。

【図9】モバイル装置からのPINエントリを用いたアンロックを示すアンロックシーケンス図。

【図10】サーバ／コンソールを介するPINエントリおよびユーザID／位置／時間の検証を用いるアンロックを示すアンロックシーケンス図。

20

【図11】サーバ／コンソールを使用するデータセキュリティシステムのリセットを示すリセットシーケンス図。

【図12】サーバ／コンソールを使用するデータセキュリティシステムのアンロックを示すアンロックシーケンス図。

【図13】サーバ／コンソールを使用するユーザパスワード変更シーケンス図。

【発明を実施するための形態】

【0014】

以下の実施形態は、当業者が本発明を実施し使用することができるよう十分に詳細に記載されている。本開示に基づく他の実施形態が明らかであり、本発明の範囲から逸脱することなくシステム、プロセス、または機械的変更を行い得ると理解されたい。

30

【0015】

以下、本発明を完全に理解できるように多くの特定の詳細を説明する。しかしながら、本発明は、これらの特定の詳細なしに実施され得ることは明らかであろう。いくつかの周知の回路、システム構成、および処理工程については、本発明を不明瞭にすることを避けるために詳細に開示していない。

【0016】

同様に、システムの実施形態を示す図面は、半概略図であり、一定の縮尺ではなく、特に、図面の明瞭化目的で大きさを示しており、図面に誇張されて示されている。いくつかの特徴を共通に有する複数の実施形態が開示され記載されている場合、それらの図示、説明、および理解を明瞭にするために、類似または同様の特徴は、通常、類似または同一の参照番号を付して記述する。同様に、説明を容易にするために図面の視点は概して同様の配向で示すが、この図示の仕方は大部分において任意である。一般に、本発明は任意の配向で実施され得る。

40

【0017】

本明細書で使用される「システム」という用語は、その用語が使用される文脈に応じて、本発明の方法および装置を指し、本発明の方法としておよび装置として定義される。本明細書で使用される「方法」という用語は、装置の動作工程を指し、その動作工程として定義される。

【0018】

50

便宜のためであって限定するものではないが、「データ」という用語は、コンピュータによって生成またはコンピュータに格納できる情報として定義される。「データセキュリティシステム」という用語は、記憶媒体を組み込んだ任意の可搬型メモリ装置を意味するものとして定義される。本明細書で使用する「記憶媒体」という用語は、ソリッドステート、NANDフラッシュ、および／または磁気データ記録システムを指し、それらと定義される。「ロックされた」という用語は、記憶媒体にアクセスできない状態のデータセキュリティシステムを指し、「アンロックされた」という用語は、記憶媒体にアクセス可能な状態のデータセキュリティシステムを指す。

【0019】

ストレージ装置を耐改竄性にするには、一般的に2つの方法があり、第1は、構成要素にエポキシを塗布する方法であり、プリント回路基板に塗布されたエポキシ樹脂は、記憶媒体を破壊せずにストレージ装置を分解することを困難にできる。第2は、メモリデータを暗号化する方法であり、データは記憶媒体に書き込まれるときに暗号化され、そのデータを解読(decipher)するためには暗号鍵が必要とされる。

【0020】

図1を参照すると、本発明の一実施形態によるデータセキュリティシステム100の概略図が示されている。データセキュリティシステム100は、外部通信チャンネル102と、認証サブシステム104と、ストレージサブシステム106とからなる。

【0021】

ストレージサブシステム106は、インターフェースコントローラ108、暗号化エンジン110、及び記憶媒体112を含む電子回路である。記憶媒体112は、内蔵または外付けのハードディスクドライブ、USBフラッシュドライブ、ソリッドステートドライブ、ハイブリッドドライブ、メモリカード、テープカートリッジ、および光ディスク(例えば、ブルーレイディスク、デジタル多用途ディスクすなわちDVD、およびコンパクトディスクすなわちCD)を含む任意の光学式媒体であってよい。記憶媒体112は、データ保護装置、アーカイブ記憶システム、およびクラウドデータストレージシステムを含むことができる。クラウドストレージシステムは、ブラウザアプリケーションにインストールされたプラグインアプリケーションまたは拡張ソフトウェアを使用して、ホストコンピュータに、または有線のまたはRFのまたは光学式の無線ネットワークを介してホストコンピュータに結合された別のシステムに、またはワールドワイドウェブにアクセスすることができる。

【0022】

インターフェースコントローラ108は、ソフトウェアまたはハードウェアの暗号化エンジン110を備えたマイクロコントローラなどの電子コンポーネントを含むが、暗号化エンジン110は、ストレージサブシステム106内の別個のコントローラ内にあってもよい。

【0023】

認証サブシステム104は、電氣的に消去可能なプログラマブルリードオンリーメモリ(EEPROM)などの不揮発性メモリをそれ自身が有することがあるマイクロコントローラのような認証コントローラ114を含む電子回路である。

【0024】

外部通信チャンネル102は、ホストコンピュータシステム120とのデータ交換手段を提供する。ユニバーサルシリアルバス(USB)は、データセキュリティシステム100をホストコンピュータシステム120に接続する最も一般的な手段の1つである。外部通信チャンネル102の他の例には、Firewire、無線USB、シリアルATA(SATA)、高詳細度マルチメディアインターフェース(HDMI(登録商標))、RS-232(Recommended Standard 232)、および無線周波数無線ネットワークが含まれる。

【0025】

インターフェースコントローラ108は、USBパケットデータを、USBフラッシュ

10

20

30

40

50

ドライブ内の記憶媒体 112 に書き込むことができるデータに変換することができる。

暗号化エンジン 110 は、インターフェースコントローラ 108 の一部として実装され、ホストコンピュータシステム 120 からのクリアテキストおよび／またはデータ（情報）を受け取り、それを MSD または記憶媒体 112 に書き込まれる暗号化された形式に変換する。暗号化エンジン 110 は、記憶媒体 112 からの暗号化情報を変換し、それをホストコンピュータシステム 120 用のクリア情報に復号する。暗号化エンジン 110 は、通信プロトコル、メモリ、および他の動作条件を管理しながらオンザフライでデータを暗号化／復号化する暗号化機能を有する暗号コントローラと、通信、暗号鍵管理、および暗号化コントローラとの通信を取り扱うための通信／セキュリティコントローラとを有する 2 つのコントローラサブシステムであってもよい。

10

【0026】

暗号化エンジン 110 は、情報を暗号化／復号化するために暗号鍵 116 を必要とする。暗号鍵 116 は、データを判読不能にまたは判読可能にするためにデータを暗号化アルゴリズムで暗号化／復号化するアルゴリズム（例えば、256 ビットの高度暗号化規格（AES）暗号化）において使用される。暗号鍵 116 は、認証コントローラ 114 の内部または外部のいずれかに格納することができる。

【0027】

識別番号または鍵を有するユーザ 122 が認証鍵 118 に対して確認されると、暗号鍵 116 が認証サブシステム 104 によって暗号化エンジン 110 に送信される。

本発明の様々な実施形態の可搬型メモリストレージ装置は、認証鍵 118 および暗号鍵 116 を使用することによって、以前はそのような装置では利用できなかった極めて高いレベルのセキュリティを提供できることが分かった。

20

【0028】

データセキュリティシステム 100 がロックされると、認証鍵 118 は認証サブシステム 104 の内部に残り、外部からは読み取ることができない。認証鍵 118 を隠す一つの方法は、認証鍵 118 を認証サブシステム 104 内の認証コントローラ 114 に格納することである。認証制御部 114 の安全ヒューズを設定することにより、ユーザ 122 が確認されて認証制御部 114 が取り出しを許可しない限り、認証鍵 118 にアクセスすることを不可能にする。多くのマイクロコントローラには、安全ヒューズが装備されており、その安全ヒューズが飛ぶと内部メモリにアクセスできなくなる。これは公知で広く使用されているセキュリティ機能である。このようなマイクロコントローラを認証コントローラ 114 に使用できる。認証コントローラ 114 は、マイクロコントローラまたはマイクロプロセッサとすることができる。

30

【0029】

認証鍵 118 は、いくつかの機能において使用することができ、
1…情報を直接暗号化／復号化するための暗号鍵 116 として使用でき、
2…インターフェースコントローラ 108 によってアクセスすることができるデータセキュリティシステム 100 に記憶された暗号鍵 116 を回復するための鍵として使用でき、
3…外部通信チャネル 102 を起動するためにインターフェースコントローラ 108 によって直接比較するために使用できる。

40

【0030】

図 2 を参照すると、データセキュリティシステム 100 を用いて使用される認証鍵配信方法が示されている。この図では、認証鍵 118 と暗号鍵 116 は同一である。暗号化エンジン 110 は、暗号鍵 116 として認証鍵 118 を用いる。

【0031】

ユーザ 122 は、ユーザ識別情報 202（番号または鍵）を認証サブシステム 104 に提供することによって、認証サブシステム 104 と対話しなければならない。認証サブシステム 104 は、ユーザ 122 を認証鍵 118 に対して認証する。次に、認証サブシステム 104 は、暗号鍵 116 として認証鍵 118 をインターフェースコントローラ 108 に送信する。

50

【0032】

インターフェースコントローラ108内の暗号化エンジン110は、チャンネル206に沿ってクリア情報を暗号化情報に変換したり暗号化情報をクリア情報に変換するのにその認証鍵118を使用する。暗号鍵116なしで記憶媒体112から暗号化情報を読み取ろうとする試みは、どんなコンピュータによっても使用できない情報をもたらすだけであろう。

【0033】

図3を参照すると、ユーザ122がデータセキュリティシステム300と対話するための別のシステムが図示されている。この対話は、物理的接触、有線接続、または携帯電話、スマートフォン、スマートウォッチ、ウェアラブル機器、または他のワイヤレス装置からの無線接続によるものであり得る、通信コンビネーション301によって行うことができる。

10

【0034】

一認証システムでは、モバイル送受信器302を使用して、ユーザ識別情報304を認証サブシステム310内のデータセキュリティ送受信器306に送信する。例示目的で、双方向通信の柔軟性のために複数の送受信器を使用しているが、単方向通信用の送受信機の組み合わせも使用できる。認証サブシステム310は、ストレージサブシステム106内のインターフェースコントローラ108に接続された認証コントローラ114を含む。ユーザ識別情報304は、データセキュリティシステム300のストレージサブシステム106の外部からモバイルトランシーバ302によって認証サブシステム310内のデータセキュリティ送受信器306に供給される。無線通信は、ワイファイ(WiFi)、ブルートゥース(BT(登録商標))、ブルートゥーススマート、近距離通信(NFC)、全地球測位システム(GPS)、光、セルラー通信(例えば、LTE-A)、符号分割多元接続(CDMA)、広帯域符号分割多元接続(WCDMA(登録商標))、ユニバーサル移動体通信システム(UMTS)、無線ブロードバンド(WiBro)、または移動通信用グローバルシステム(GSM(登録商標))等を含むことができる。

20

【0035】

認証サブシステム310は、モバイル送受信器302から送信されたコードが認証鍵118に対して照合されたものであることによって、ユーザ122を認証鍵118に対して認証する。次に、認証サブシステム310は、暗号鍵116を通信コンビネーション301を介してインターフェースコントローラ108に送信する。

30

【0036】

次いで、暗号化エンジン110は、チャンネル206に沿ってクリア情報を暗号化情報に変換したり暗号化情報をクリア情報に変換するのに暗号鍵116を使用する。暗号鍵116なしで記憶媒体112から暗号化情報を読み取ろうとしても、ホストコンピュータシステム120によって使用不可能な情報が得られるだけであろう。

【0037】

任意選択の第2の認証機構では、認証サブシステム310が、ユーザ122にバイオメトリックセンサ320を使用させて、そのユーザの身元が認証されたユーザであると確認するためのバイオメトリック入力322を供給させることによって、認証鍵118に対してユーザ122が認証される。生体認証の種類には、指紋、虹彩スキャン、声紋などがある。

40

【0038】

任意選択の第3の認証機構では、認証サブシステム310が、ユーザ122に電気機械式入力機構330を使用させて、そのユーザの身元が認証されたユーザであると確認するための固有コード332を供給させることによって、ユーザ122を認証鍵118に対して認証する。固有コード332は、PINなどの、数値、英数字またはアルファベットコードを含むことができる。電気機械式入力機構330は、認証サブシステム310内にある。電気機械式入力機構330は、ユーザ122からの固有コード332をデータセキュ

50

リティシステム300の外部から受信する。固有コード332は、データセキュリティシステム300のストレージサブシステム106の外部から認証サブシステム310内の電気機械式入力機構330に供給される。

【0039】

ユーザ122の照合にどちらの方法を使用するにしても、ユーザ122が認証されるまで、認証鍵118および暗号鍵116は隠されたままである。

図4を参照すると、ユーザ122がホストコンピュータシステム120を使用してデータセキュリティシステム400と対話する方法が示されている。

【0040】

ホストコンピュータシステム120は、ホストアプリケーション402を備えている。ホストアプリケーション402は、データセキュリティシステム400の外部通信チャネル102を介して通信するソフトウェアまたはファームウェアである。

【0041】

ホストアプリケーション402は、内部コンポーネント（例えばハードドライブ）の通し番号、ネットワークカードのメディアアクセス制御（MAC）アドレス、ユーザのログイン名、ネットワークインターネットプロトコル（IP）アドレス、データセキュリティシステムによって作成されてホストに保存されたID、データセキュリティシステムによって作成されてネットワークに保存されたIDなどの、環境に関連付けられた、ホスト識別子406を配信する。ホスト識別子406は、データセキュリティシステム400内の認証サブシステム408によって使用される。

【0042】

認証サブシステム408が、ホスト識別子406を検証することによってユーザ122を認証鍵118に対して認証すると、データセキュリティシステム400はアンロックになる。

【0043】

例えば、ユーザ122は、ロックされているデータセキュリティシステム400をホストコンピュータシステム120に接続する。ホストアプリケーション402は、そのネットワークカードのMACアドレスをデータセキュリティシステム400に送信する。データセキュリティシステム400は、図1のユーザ122にユーザ識別情報を入力させることなしで、このMACアドレスが正当であると認識し、アンロックになる。これは、ユーザ122との対話を必要としない実装例である。この場合、検証されるのはホストコンピュータシステム120およびそれに関連付けられた環境である。

【0044】

データセキュリティシステム400は、認証サブシステム104に格納された認証鍵118を提供すること、認証サブシステム104によってホストコンピュータシステム120を検証すること、認証サブシステム104によって暗号鍵116をストレージサブシステム106に提示すること、記憶媒体のコンテンツを解読することによってストレージサブシステム106による記憶媒体112へのアクセスを可能にすることを含む。

【0045】

データセキュリティシステムは、バイオメトリック入力を解釈しユーザ122を検証するための認証サブシステム104をさらに含む。

データセキュリティシステムはさらに、認証鍵118を暗号鍵116として直接使用することを含む。

【0046】

データセキュリティシステムはさらに、認証鍵118を使用して、内部コンテンツを解読するのに使用される暗号鍵116を解読及び取り出すことを含む。

データセキュリティシステムは、信号入力の解釈および送信ユニットの検証のための認証サブシステム104をさらに含む。

【0047】

データセキュリティシステムは、手動入力された入力の解釈およびユーザ122の検証

10

20

30

40

50

のための認証サブシステム 104 をさらに含む。

データセキュリティシステムはさらに、ホストコンピュータシステム 120 の検証のためのホスト常駐ソフトウェアアプリケーションによって送られた入力を解釈するための認証サブシステム 104 を含む。

【0048】

データセキュリティシステムは、インターフェースコントローラ 108 の外部にある暗号化エンジン 110 であって、クリアデータをデータセキュリティシステム 100 をアンロックするための暗号化データに変換する目的で外部通信チャネル 102 に接続された暗号化エンジン 110 をさらに含む。

【0049】

図 5 を参照すると、データセキュリティシステム 100 に対するユーザ検証を用いるデータセキュリティ方法 500 が示されている。データセキュリティ方法 500 は、ブロック 502 において認証鍵に対してユーザを検証する工程と、ブロック 504 において暗号鍵を取り出すために認証鍵を使用する工程と、ブロック 506 においてホストコンピュータシステムと記憶媒体との間のストレージサブシステムを介した暗号化されていない通信を可能にするために暗号鍵を使用する工程とを含む。

【0050】

図 6 を参照すると、例示的なデータセキュリティ通信システム 600 が示されている。例示的なデータセキュリティ通信システム 600 は、モバイル装置 610、データセキュリティシステム (DSS) 620、ホストコンピュータ 630、およびサーバ/コンソール 640 を含む。モバイル装置 610 およびサーバ/コンソール 640 は、有線接続によって、またはインターネットクラウドであり得るクラウド 650 を介する無線接続によって接続される。モバイル装置 610 とデータセキュリティシステム 620 は、通信コンビネーション 301 によって接続される。

【0051】

例示的なデータセキュリティ通信システム 600 における通信コンビネーション 301 は、データセキュリティシステム 620 内のデータセキュリティ送受信器 624 のアンテナ 622 と無線通信するアンテナ 614 を有するモバイル装置 610 内のモバイル送受信器 612 を含む。

【0052】

一実施形態では、モバイル装置 610 は、スマートフォンであってよい。モバイル装置 610 において、モバイル送受信器 612 は、従来のモバイル装置コンポーネントと接続されてよく、またデータセキュリティシステム 620 と共に使用される情報を提供するデータセキュリティシステム (SS) アプリケーション 618 と接続されてよい。

【0053】

データセキュリティ送受信器 624 は、セキュリティコントローラ 626 に接続されているが、このセキュリティコントローラ 626 には、異なるモバイル装置のものを含めて、データセキュリティシステム 620 にアクセスすることができる識別情報、パスワード、プロフィール等の情報を保有させることができる。セキュリティコントローラ 626 は、認証サブシステム 310、ストレージサブシステム 106 (一部の実施形態では、データを暗号化するための暗号を有することができる)、および外部通信チャネル 102 と同様のサブシステムに接続される。

【0054】

外部通信チャネル 102 は、ホストコンピュータ 630 に接続可能であり、規定状況下でストレージサブシステム 106 内のデータへのアクセスを可能にする。

データセキュリティシステム 620 の一実装例では、図 3 のバイオメトリックセンサ 320 および電気機械式入力機構 330 を省略し、スマートフォン等のモバイル装置 610 への無線リンクのみを有するものとすることができる。この実装例は、データセキュリティシステム 620 をより安全で有用にできることが分かった。

【0055】

データセキュリティシステムアプリケーション618は、モバイル装置610がモバイル装置610の近くのすべてのデータセキュリティシステムを発見し、それらのステータス（ロック／アンロック／ブランク、ペアあり／ペアなしなど）を示すことを可能にする。

【0056】

データセキュリティシステムアプリケーション618は、モバイル装置610が接続／ペアリング、ロック、アンロック、名前とパスワードの変更、およびデータセキュリティシステム620上のすべてのデータのリセットをできるようにする。

【0057】

データセキュリティシステムアプリケーション618は、データセキュリティシステム620が所定長さの非アクティブ期間の後に自動的にロックする非アクティブオートロックモードをモバイル装置610が設定できるようにし、または、予め定められた期間にわたってモバイル装置610が所定の近接範囲内にないときにデータセキュリティシステム620が（信頼性を改善し、信号のデバウンスを回避するために）ロックされるように近接オートロックモードをモバイル装置610が設定できるようにする。

10

【0058】

データセキュリティシステムアプリケーション618は、モバイル装置610がパスワードを記憶し、Touch IDおよびApple Watchを使用することを可能にする（Touch IDおよびApple Watchの両方が例としてのみ挙げられているが、バイオメトリックセンサおよびウェアラブルを有する多くの他のモバイル装置が存在する同様のモードで使用される）ことで、モバイル装置へのパスワードの再入力なしでデータセキュリティシステム620はアンロックされ得る。

20

【0059】

データセキュリティシステムアプリケーション618は、他のモバイル装置ではデータセキュリティシステム620をアンロックできなくするために、モバイル装置610などの特定のモバイル装置があるときにのみ動作するようにモバイル装置610を設定できる（iPhone）。

【0060】

データセキュリティシステムアプリケーション618は、モバイル装置610がデータセキュリティシステム620を読み取り専用モードに設定することを可能にする。

30

データセキュリティシステムアプリケーション618は、モバイル装置610がユーザモードまたは管理者モード（管理者モードはユーザ設定を無視する）で動作し、サーバ／コンソール640を使用することを可能にする。サーバ／コンソール640は、コンピュータと、そのコンピュータに情報を入力するためのコンソールとの組み合わせである。

【0061】

サーバ／コンソール640はユーザ管理データベース642を含み、このユーザ管理データベース642は、モバイル装置610に追加の機能を与えるためにクラウド650を介してモバイル装置610に送信され得る追加の情報を含む。

【0062】

ユーザ管理データベース642は、サーバ／コンソール640が、ユーザID（ユーザ名およびパスワード）を使用してユーザを作成および識別し、データセキュリティシステム620のアンロックを禁止／許可し、遠隔ヘルプを提供することを可能にする。

40

【0063】

ユーザ管理データベース642は、サーバ／コンソール640がデータセキュリティシステム620を遠隔からリセットまたはアンロックすることを可能にする。

ユーザ管理データベース642は、サーバ／コンソール640がデータセキュリティシステムユーザPINを遠隔的に変更することを可能にする。

【0064】

ユーザ管理データベース642は、サーバ／コンソール640が（ジオフェンシングの使用によって）特定の場所からデータセキュリティシステム620をアンロックすること

50

を制限／許可することを可能にする。

【0065】

ユーザ管理データベース642は、サーバ／コンソール640が、データセキュリティシステム620のアンロックを規定時間期間および異なる時間帯に制限／許可することを可能にする。

【0066】

ユーザ管理データベース642は、サーバ／コンソール640が、規定チーム／組織／ネットワーク等の外によるデータセキュリティシステム620のアンロックを制限することを可能にする。

【0067】

図7を参照すると、モバイル装置610とデータセキュリティシステム620との間の動作シーケンスを示す管理者シーケンス図が示されている。

まず、装置とシステムとの相互発見、装置とシステムとのペアリング、および装置とシステムとの接続によって、データセキュリティシステム620とモバイル装置610との接続状態700が確立される。この接続状態700は共有秘密情報の使用によって保護され、その共有秘密情報は、その後の通信セッションの間、データセキュリティシステム620とモバイル装置610との間の通信を保護（暗号化）するために使用される。データセキュリティシステム620上で実行するのに効率的でかつ世界的なセキュリティ規格に承認される標準的な暗号化アルゴリズムが選択される。

【0068】

データセキュリティシステム620とモバイル装置610とが互いに所定の距離内にある限り、データセキュリティシステムアプリケーション618によってまたはセキュリティコントローラ628によってまたはそれら両者が協働して接続状態700は維持される。その所定の距離から離れた場合、所定の時間期間にわたって接続状態700が維持された後、データセキュリティシステム620はロックされる。

【0069】

モバイル装置610とデータセキュリティシステム620との接続後、モバイル装置610においてデータセキュリティシステム管理者アプリケーション開始動作702が行われる。次に管理者パスワード動作704において管理者がパスワードを設定する。モバイル装置610とデータセキュリティシステム620との接続後、データセキュリティシステム接続、給電、発見可能化動作706において、データセキュリティシステム620は、データセキュリティシステム620内のホストコンピュータ630によって給電されるとともに発見可能となるように図6のホストコンピュータ630に接続される。

【0070】

管理者パスワード動作704の後、モバイル装置610は、管理者パスワード設定およびアンロック信号708をデータセキュリティシステム620に送信する。管理者パスワード設定及びアンロック信号708は、データセキュリティシステム620において、管理者パスワード設定及びデータセキュリティシステムアンロック動作716を生じさせる。

【0071】

管理者パスワード設定およびデータセキュリティシステムアンロック動作716が完了すると、データセキュリティシステムアンロックの確認信号712がモバイル装置610に送信され、モバイル装置610において管理者動作714としてのデータセキュリティシステムアンロックの確認が実行される。管理者動作714としてのデータセキュリティシステムアンロックの確認があると、モバイル装置610を使用して実行される他の制限の設定動作716が許可される。他の制限の設定動作716があると、管理者制限設定信号718がデータセキュリティシステム620へと送信され、データセキュリティシステム620において管理者制限が設定され、制限設定確認信号720がモバイル装置610に返信される。その後、モバイル装置610およびデータセキュリティシステム620は、完全に動作可能な通信状態である。

【0072】

データセキュリティシステム620と物理的接触を持つことなくデータセキュリティシステム620と通信することが可能なので、データセキュリティシステム620との重要な対話には、データセキュリティシステム620自体に印字されるかまたはデータセキュリティシステム620のパッケージに付属したものであってデータセキュリティシステム620の所有者が容易に利用できるデータセキュリティシステム固有識別子を同伴することが必要とされる。

【0073】

この固有識別子（固有ID）は、データセキュリティシステム620のアンロックまたはリセットといったユーザデータに影響を与える動作を要求する際に必要とされる。正しい識別子なしでこれらの動作を実行しようとする試みは無視され、無害化される。この固有識別子は、ユーザがデータセキュリティシステム620上で物理的な制御を持たせるとともにモバイル装置610とデータセキュリティシステム620といった認証済みで先にペアになった装置とシステムとの接続状態700が確立されていることを検証するための方法で、モバイル装置610にデータセキュリティシステム620を識別させるのに使用される。装置のペアになると、共有秘密情報を使用して通信を機密にする。

10

【0074】

ペアリングは、モバイル装置とデータセキュリティシステムとが過去のある時点で一意でかつ決められた関係を確認し維持していることを包含する。

固有識別子は、データセキュリティシステムに対する物理的制御がユーザにあるときに、ユーザにデータセキュリティシステムに対する何らかの制御を与える。

20

【0075】

モバイル装置610がスマートフォンである場合にデータセキュリティシステム620との通信のセキュリティを高めるために、ユーザは本実施形態で「1Phone」と呼ぶ機能などの機能の有効化を選択することができる。この機能は、データセキュリティシステム620との重要なユーザ対話を唯一のモバイル装置610だけに限定する。これは、上述したデータセキュリティシステム固有識別子を、データセキュリティシステム620とモバイル装置610との間で安全に共有されるランダム識別子に置き換えることによって行われる。したがって、例えば、ユーザがデータセキュリティシステム620をアンロックするときに、データセキュリティシステム固有識別子を提示する代わりに、1Phone識別子を提示しなければならない。実際には、これにより、ユーザのモバイル装置610が、PINまたはパスワードに加えて、データセキュリティシステム620を使用するための第2の認証因子になる。一例として、「1Phone」として選択されペアになったユーザ電話は、PINなしで使用でき、ユーザ認証単一因子として、および／または、他のユーザ認証因子と組み合わせて、使用することができる。もしこの機能（1Phone）が選択された場合、管理者アンロックが前もって有効にされている場合を除いて、他の電話機でデータセキュリティシステム620を開くことはできない。

30

【0076】

他の実施形態では、1Phone機能を使用するために、データセキュリティシステム620上で管理者パスワードを要求するようにしてよいことが理解されよう。別の実施形態では、モバイル装置610の1Phoneデータが失われた場合に、サーバ／コンソール640がデータセキュリティシステム620を回復できるようにしてもよい。

40

【0077】

ユーザは、データセキュリティシステム620の近接自動ロック機能を有効化することができる。通信セッション中に、図6のデータセキュリティ送受信器624がデータセキュリティシステム620にモバイル装置610の信号強度測定値を報告する。モバイル装置610上のデータセキュリティシステムアプリケーション618は、データセキュリティシステム620に、発信元の信号出力レベルと近接範囲の閾値との両方を送信する。

【0078】

信号強度は送受信器周辺の環境条件によって変化するので、データセキュリティシステ

50

ム 6 2 0 は、信号強度測定値を数学的に平滑化して、偽陽性の可能性を低減する。データセキュリティシステム 6 2 0 は、受信した信号強度が所定の期間にわたって規定の閾値を下回ったことを検出すると、すぐにデータセキュリティシステム 6 2 0 をロックし、図 6 のストレージサブシステム 1 0 6 へのアクセスを防止する。

【0079】

データセキュリティシステム 6 2 0 は、3つの異なるモードで 사용할 ことができる。すなわち、データセキュリティシステム 6 2 0 の機能をユーザが決定できるユーザモード、管理者が管理者パスワードを設定でき、データセキュリティシステム 6 2 0 に、ユーザでは解除できないいくつかの制限（例えば、所定期間の非活動後の自動ロック、読み取り専用、1 P h o n e）を加えることができる管理者モード、および、サーバ／コンソール 6 4 0 がデータセキュリティシステム 6 2 0 を遠隔からリセットしたり、ユーザパスワードを変更したり、データセキュリティシステム 6 2 0 をアンロックしたりするための管理者役割を設定するサーバモードである。

10

【0080】

図 8 を参照すると、モバイル装置 6 1 0 が認証因子である場合のアンロックシーケンス図が示されている。この図は、特定のモバイル装置であるモバイル装置 6 1 0 からのデータセキュリティシステムアプリケーション 6 1 8 によって開始されたデータセキュリティシステム 6 2 0 の自動アンロックプロセスを示す。ユーザは、データセキュリティシステム 6 2 0 と先にペアになった単一のモバイル装置のみを使用することができる。ペアになったモバイル装置 6 1 0 を紛失すると、（図 7 に示すように管理者パスワードが以前に設定されていない限り）データセキュリティシステム 6 2 0 をアンロックできないであろう。

20

【0081】

図 7 と類似しているが、接続状態 7 0 0 が確立された後にデータセキュリティシステムアプリケーション開始動作 8 0 0 が行われる。データセキュリティシステム接続、給電、発見可能化動作 7 0 6 の後に、モバイル装置 6 1 0 からデータセキュリティシステム 6 2 0 にモバイル装置 I D を伴うアンロック要求信号 8 0 2 が送信される。データセキュリティシステムアンロック動作 8 0 4 が行われ、データセキュリティシステムアンロック確認信号 7 1 2 がデータセキュリティシステム 6 2 0 から送信される。データセキュリティシステムアンロック確認動作 8 0 6 の後、モバイル装置 6 1 0 およびデータセキュリティシステム 6 2 0 は、完全に動作可能な通信状態である。

30

【0082】

P I N（個人用識別番号）が設定されていない場合、ペアになったモバイル装置が 1－認証因子として使用される。

図 9 を参照すると、モバイル装置 6 1 0 からの P I N エントリを使用するアンロック動作を示すアンロックシーケンス図が示されている。この図は、モバイル装置 6 1 0 内のデータセキュリティシステムアプリケーション 6 1 8 に P I N を入力することによって、データセキュリティシステム 6 2 0 をアンロックするプロセスを示す。正しい P I N の入力なしでデータセキュリティシステム 6 2 0 をアンロックすることはできない。

40

【0083】

図 7 および図 8 と類似しているが、データセキュリティシステムアプリケーション開始動作 8 0 0 の後に、ユーザ名／パスワード入力動作 9 0 0 が行われる。ユーザ名／パスワード入力動作 9 0 0 の後、モバイル装置 6 1 0 は、サーバ／コンソール 6 4 0 にユーザ I D 検証信号 9 0 2 を送信する。次に、サーバ／コンソール 6 4 0 は、ユーザ名／パスワード適正判定 9 0 4 を行う。

【0084】

ユーザ名／パスワード適正判定 9 0 4 がユーザを検証すると、適正ユーザ信号 9 0 6 がモバイル装置 6 1 0 に送信され、モバイル装置 6 1 0 の P I N 入力動作 9 0 8 においてユーザに正しい P I N を入力させる。次いで、モバイル装置 6 1 0 は、正しい P I N がサーバ／コンソール 6 4 0 に入力されたかどうかを判定するために、アンロック検証信号 9 1

50

0を送信する。

【0085】

サーバ／コンソール640は、ユーザ認証判定912を行い、ユーザが、PINが認可されている特定のデータセキュリティシステム（例えば、データセキュリティシステム620）を使用することが許可されているかどうかを判定する。認証された場合、アンロック許可信号914がモバイル装置610に送信され、モバイル装置610はアンロック要求信号916をデータセキュリティシステム620に渡す。

【0086】

データセキュリティシステムアンロック動作804が実行され、データセキュリティシステムアンロック確認信号712がモバイル装置610に送信され、データセキュリティシステムアンロック動作確認806が実行される。

10

【0087】

図10を参照すると、サーバ／コンソール640を介したPINエントリおよびユーザID／位置／時間の検証を使用するアンロック動作を示すアンロックシーケンス図が示されている。この図は、モバイル装置610からデータセキュリティシステムアプリケーション618にPINを入力し、ユーザID（ユーザ名／パスワード）を使用してサーバ／コンソール640サーバで確認することによって、および特定の場所およびある時間範囲でデータセキュリティシステム620をアンロックするためのジオフェンシング許可を検証することによって、データセキュリティシステム620をアンロックする最もセキュリティの高いプロセスを示す。データセキュリティシステム620は、PIN、ユーザ名およびパスワードの入力と、モバイル装置610が特定の（予め決められた）位置で特定の（予め決められた）時間に存在することとがなければ、アンロックできないであろう。

20

【0088】

図7～図9と類似しているが、サーバ／コンソール640において、データセキュリティシステム620などの指定データセキュリティシステムが動作するのに必要な条件の設定を可能にするために、指定データセキュリティシステムアンロック動作1000が行われる。例えば、条件は、特定の地理的領域内におよび／または特定の時間枠の範囲内にあることとであってもよい。

【0089】

モバイル装置610において、位置及び／又は現在時刻取得動作1002のような、現在状態の判定が行われる。この動作は、モバイル装置610がどこに位置しているか、および／または、モバイル装置610が位置している場所での現在時刻を判定するために実行される。モバイル装置610の周りの他の現在状態が判定されるとともに、アンロック検証信号1004によってサーバ／コンソール640に送信されてよく、そのサーバ／コンソール640で条件適合判定1006がなされる。

30

【0090】

所望の条件に適合したとき、アンロック許可信号1008がモバイル装置610に送信され、PIN入力動作908を実行させる。PINの入力後、PINと、モバイル装置610に動作可能に近接しているデータセキュリティシステム620の識別情報とともに、アンロック検証信号1010が送信される。検証アンロック信号1010がサーバ／コンソール640によって受信されると、データセキュリティシステム許可判定1012が行われて、認証ユーザによる指定データセキュリティシステムのアンロックが許可されることを判定する。サーバ／コンソール640は、この「特定」ユーザが指定データセキュリティシステムを使用することを認可されていると確認する。

40

【0091】

正しい情報が提供されたと判定された後、サーバ／コンソール640は、モバイル装置610にアンロック許可信号914を提供し、モバイル装置610は、アンロック要求信号916を提供する。アンロック要求信号916は、データセキュリティシステム620を動作させる。

【0092】

50

図11を参照すると、サーバ／コンソール640を使用してデータセキュリティシステム620をリセットする動作を示すリセットシーケンス図が示されている。この図は、サーバ／コンソール640を介してデータセキュリティシステム620を遠隔からリセットできる機能を示す。データセキュリティシステム620は、ワイヤレス接続を介してモバイル装置610からのコマンドのみを受信し得る。しかしながら、サーバ／コンソール640に特定のデータセキュリティシステム（シリアルナンバーを使用）用の「リセット」フラグを設定することにより、モバイル装置610上で動作しているデータセキュリティシステムアプリケーション618は、サーバ／コンソール640にユーザ管理データベース642にある任意のフラグ／保留中要求を問い合わせることとなる。ユーザがデータセキュリティシステム620に接続すると、モバイル装置610上のデータセキュリティシステムアプリケーション618は、「リセット」待ちコマンドを実行することとなる。リセットが成功した後（すべてのユーザデータおよび資格情報が失われた後）、サーバ／コンソール640はリセットフラグを除去するので、モバイル装置610が特定のデータセキュリティシステムに次回接続されたときにリセットは実行されない。

10

【0093】

図7～図10と類似しているが、モバイル装置610は適正ユーザ信号906に応答して、任意コマンド待ち信号1100をサーバ／コンソール640に送信してリセットコマンド判定1102を行う。リセットコマンドが存在するとき、リセット実行信号1104がモバイル装置610に送信される。

20

【0094】

モバイル装置610は、セキュリティシステムリセット信号1106をデータセキュリティシステム620に送信して、データセキュリティシステムリセット動作1108を開始させる。データセキュリティシステムリセット動作1108が完了すると、データセキュリティシステム620は、データセキュリティシステムリセット確認信号1110をモバイル装置610に送信して、データセキュリティシステムリセット確認動作1112を実施させるように設定する。その後、モバイル装置610およびデータセキュリティシステム620は、リセットされたデータセキュリティシステム620と、完全に動作可能な通信状態である。

【0095】

図12を参照すると、サーバ／コンソール640を使用してデータセキュリティシステム620をアンロックする動作を示すアンロックシーケンス図が示されている。この図は、サーバ／コンソール640を介してデータセキュリティシステム620を遠隔からアンロックできる機能を示す。データセキュリティシステム620は、ワイヤレス接続を介してモバイル装置610からのコマンドのみを受信し得る。しかしながら、特定のデータセキュリティシステム（シリアルナンバーを使用）についてサーバ／コンソール640コンソール上に「管理者アンロック」フラグを設定することにより、モバイル装置610上で動作しているデータセキュリティシステムアプリケーション618は、サーバ／コンソール640に任意のフラグ／保留中の要求を問い合わせることとなる。ユーザがデータセキュリティシステム620に接続すると、モバイル装置610上のデータセキュリティシステムアプリケーション618は、「管理者アンロック」待ちコマンドを実行する。管理者アンロックが成功した後、ユーザデータはそのままであるが、ユーザパスワードは削除される（データセキュリティシステム620はユーザによってアンロックされ得ない）。サーバ／コンソール640は、データセキュリティシステム620用のリセットフラグを除去するので、モバイル装置610がデータセキュリティシステム620に次回接続されたときにリセットは実行されない。

30

40

【0096】

図7～図11と類似しているが、サーバ／コンソール640は、任意のコマンド待ち信号1100を受信した後、管理者パスワードでアンロックするコマンドがある場合にアンロック1200を実行する。管理者パスワード付きアンロック信号1202がモバイル装置610に送信されると、モバイル装置610は管理者パスワード付きアンロック信号1

50

204をデータセキュリティシステム620に提供して、データセキュリティシステムアンロック動作804を開始させる。その後、モバイル装置610およびデータセキュリティシステム620は、完全に動作可能な通信状態である。

【0097】

図13を参照すると、サーバ/コンソール640を使用するユーザパスワード変更シーケンス図が示されている。この図は、サーバ/コンソール640を介してデータセキュリティシステム620のユーザパスワードを遠隔から変更できる機能を示す。データセキュリティシステム620が無線接続を介してモバイル装置610からのみコマンドを受信できるが、特定のデータセキュリティシステム（シリアルナンバーを使用）用の「ユーザパスワード変更」フラグをサーバ/コンソール640コンソールにセットすることによって、モバイル装置610上で動作しているデータセキュリティシステムアプリケーション618は、任意のフラグ/保留中の要求をサーバ/コンソール640に問い合わせることとなる。ユーザが自分のデータセキュリティシステム620に接続するとき、モバイル装置610にあるデータセキュリティシステムアプリケーション618は、「ユーザパスワードの変更」待ちコマンドを実行する。アンロックが成功しパスワードが変更された後、ユーザデータはそのままであるが、データセキュリティシステム620は新しいユーザパスワードでアンロックされ得る。サーバ/コンソール640は、このデータセキュリティシステム620用の「ユーザパスワードの変更」フラグを除去するので、モバイル装置610が特定のデータセキュリティシステムに次回接続されたときにユーザパスワード変更は実行されない。

【0098】

図7～図12と類似しているが、サーバ/コンソール640は、パスワード変更判定1300を行うことによって、任意のコマンド待ち信号1100に応答する。サーバ/コンソール640でパスワード変更があると、ユーザパスワード変更信号1302がモバイル装置610に送信され、モバイル装置610は、ユーザパスワード変更信号1304をデータセキュリティシステム620に送信する。その後、モバイル装置610およびデータセキュリティシステム620は、新しいパスワードで完全に動作可能な通信状態である。

【0099】

データセキュリティシステムの動作方法は、モバイル装置にデータセキュリティシステムとの接続のためのデータセキュリティシステムアプリケーションを提供する工程と、前記データセキュリティシステムアプリケーションを起動する工程と、前記データセキュリティシステムと前記モバイル装置との接続状態を維持する工程とを備える。

【0100】

上述の方法において、前記接続状態を維持する工程は、前記データセキュリティシステムが前記モバイル装置から所定の近接範囲内にあるときに前記接続状態を維持する。

上述の方法において、前記接続状態を維持する工程は、前記データセキュリティシステムが所定の期間にわたって前記モバイル装置から所定の近接範囲内にあるときに前記接続状態を維持する。

【0101】

上記の方法において、前記接続状態を確立することは、前記データセキュリティシステムと前記モバイル装置との間の双方向通信を使用することを含む。

上記の方法において、前記接続状態を確立することは、前記データセキュリティシステムと前記モバイル装置との間の単方向通信を使用することを含む。

【0102】

上記の方法は、前記データセキュリティシステムアプリケーションを有する前記モバイル装置と、ユーザ管理データベースを含むサーバとの間の通信をさらに備える。

上記の方法は、前記データセキュリティシステムのセキュリティコントローラにセキュリティ情報を提供する工程をさらに備える。

【0103】

上記の方法は、指定データセキュリティシステムの識別情報をサーバに提供する工程と

、前記データセキュリティシステムに特定識別情報を提供する工程と、前記指定データセキュリティシステムの前記識別情報が前記データセキュリティシステムの前記特定識別情報と同じであるときに前記データセキュリティシステムをアンロックする工程とを更に備える。

【0104】

上記の方法において、モバイル装置に前記データセキュリティシステムアプリケーションを提供する工程は、データセキュリティシステム管理者アプリケーションを提供し、さらに、前記モバイル装置に管理者パスワードを設定することと、前記管理者パスワードを前記モバイル装置から前記データセキュリティシステムに送信することと、前記データセキュリティシステムに前記管理者パスワードを設定し、前記データセキュリティシステムをアンロックすることを含む。

10

【0105】

上記方法は、前記モバイル装置から前記データセキュリティシステムにモバイル装置識別情報と共にアンロック要求を提供する工程と、前記データセキュリティシステムにおいて前記アンロック要求を受信し前記データセキュリティシステムをアンロックする工程とをさらに備える。

【0106】

上記の方法は、前記モバイル装置にユーザ名またはパスワードを入力する工程と、前記モバイル装置から前記ユーザ名またはパスワードを受信した後に前記ユーザ名またはパスワードがサーバにおいて有効であるときに判定する工程と、前記ユーザ名またはパスワードが有効である場合に、前記サーバから前記モバイル装置に通信する工程と、前記ユーザ名またはパスワードが前記データセキュリティシステムをアンロックするのに有効であるとき、前記モバイル装置から前記データセキュリティシステムに通信する工程とを更に備える。

20

【0107】

前記上述の方法は、前記モバイル装置にユーザ名またはパスワードを入力する工程と、前記モバイル装置から前記ユーザ名またはパスワードを受信した後に前記ユーザ名またはパスワードがサーバにおいて有効であるときに判定する工程と、前記ユーザ名またはパスワードが有効である場合に前記サーバから前記モバイル装置に通信する工程と、前記モバイル装置から識別番号を受信した後に前記識別番号が前記サーバにおいて有効であるときに判定する工程と、前記サーバが前記識別番号が有効であると判定した場合に、前記モバイル装置を介して前記データセキュリティシステムをアンロックする工程とを更に備える。

30

【0108】

上記の方法は、前記モバイル装置の有効位置をサーバに提供する工程と、前記モバイル装置が前記有効位置にあるときに前記サーバにおいて判定する工程と、前記モバイル装置が前記有効位置にあると前記サーバが判定したときに、前記モバイル装置を介して前記データセキュリティシステムをアンロックする工程とをさらに備える。

【0109】

上述の方法は、前記モバイル装置における前記データセキュリティシステムに対する動作の現在時刻をサーバに提供する工程と、前記モバイル装置が前記現在時刻内にあるときに前記サーバにおいて判定する工程と、前記モバイル装置が前記現在時刻を有すると前記サーバが判定した場合に、前記モバイル装置を介して前記データセキュリティシステムをアンロックする工程とをさらに備える。

40

【0110】

上記の方法は、サーバにコマンドを設ける工程と、前記モバイル装置からのコマンド待機信号に応答して前記サーバから前記モバイル装置に前記コマンドを提供する工程と、前記コマンドが前記サーバから提供されたときに、前記モバイル装置を介して前記データセキュリティシステムにおいて前記コマンドを実行する工程とをさらに備える。

【0111】

50

上記の方法は、サーバにパスワード変更コマンドを設ける工程と、前記モバイル装置からのパスワード変更信号に応答して、前記サーバから前記モバイル装置に前記パスワード変更コマンドを提供する工程と、前記データセキュリティシステム内の変更後パスワードで前記データセキュリティシステムをアンロックする工程とをさらに備える。

【0112】

上記の方法は、前記データセキュリティシステムを電力のためにホストコンピュータに接続し、前記ホストコンピュータによって発見可能にすることをさらに備える。

データセキュリティシステムは、データセキュリティ送受信器または受信器と、前記データセキュリティ送受信器または受信器に動作可能に接続された認証サブシステムと、前記認証サブシステムに接続されたストレージサブシステムとを備える。

10

【0113】

上記のシステムは、前記データセキュリティ送受信器または受信器および前記認証サブシステムに接続されたセキュリティコントローラをさらに備える。

上記のシステムは、前記データセキュリティシステムがモバイル装置から所定の近接範囲内にあるときに接続状態を維持するために前記セキュリティコントローラと協働するデータセキュリティシステムアプリケーションを有するモバイル装置をさらに備える。

【0114】

上記のシステムは、前記データセキュリティシステムが所定期間にわたってモバイル装置から所定の近接範囲内にあるときに接続状態を維持するために前記セキュリティコントローラと協働するデータセキュリティシステムアプリケーションを有する前記モバイル装置をさらに備える。

20

【0115】

上記のシステムは、前記データセキュリティシステムとモバイル装置との間の双方向通信を使用することを含む接続状態を維持するためのモバイル送受信器または受信器を有する前記モバイル装置をさらに備える。

【0116】

上記のシステムは、前記データセキュリティシステムとモバイル装置との間の単方向通信を使用することを含む接続状態を維持するためのモバイル送受信器または受信器を有する前記モバイル装置をさらに備える。

【0117】

上記のシステムは、モバイル装置とデータセキュリティシステムアプリケーションを有するモバイル装置とユーザ管理データベースを含むサーバとの間の有線または無線接続通信と、ユーザ管理データベースを含むサーバとをさらに備える。

30

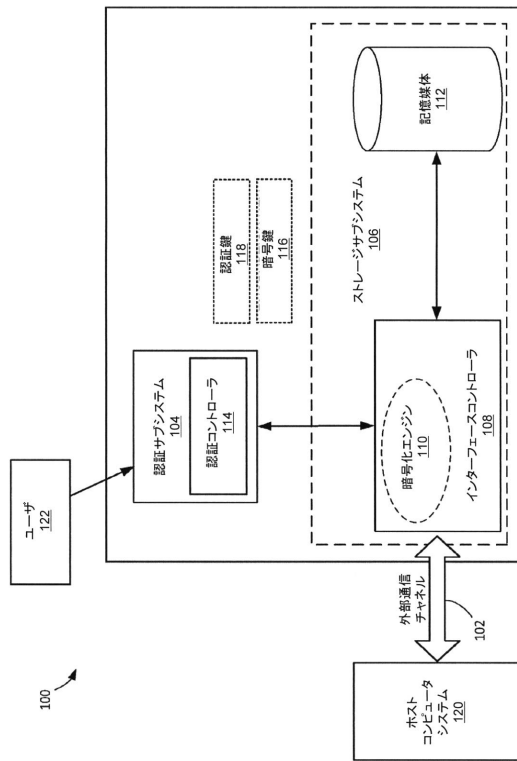
【0118】

上記のシステムにおいて、前記データセキュリティシステムはホストコンピュータと接続するための外部通信チャネルを含む。

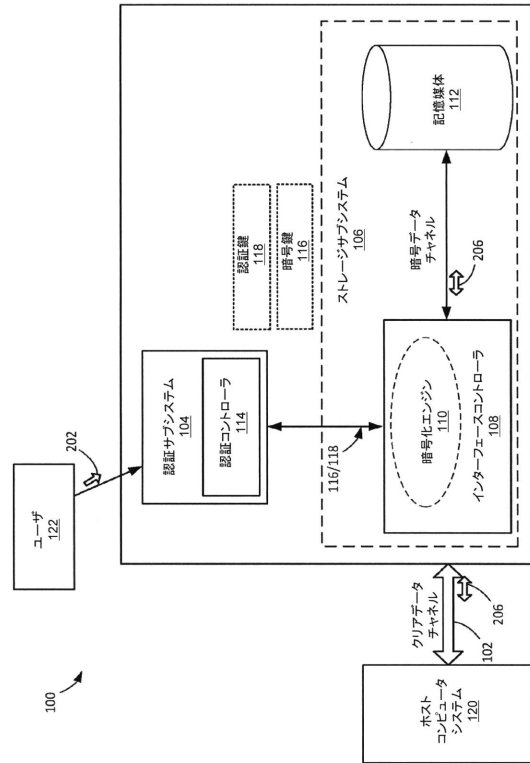
本発明を特定の最良の形態に関連して説明してきたが、前述の説明に照らして、多くの代替、変更、および変形が当業者には明らかであると理解されるべきである。したがって、添付の特許請求の範囲に入るそのような代替物、変更物および変形物のすべてを包含することが意図される。本明細書に記載されるか、または添付の図面に示されるすべての事項は、例示的かつ非限定的な意味で解釈されるべきである。

40

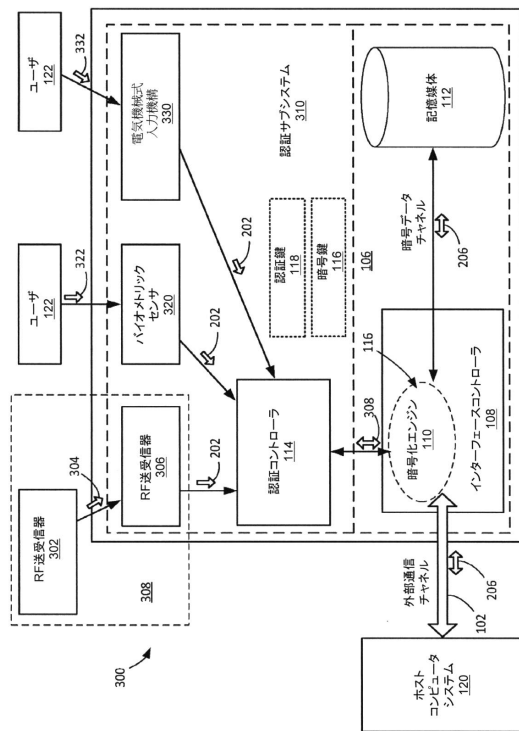
【図 1】



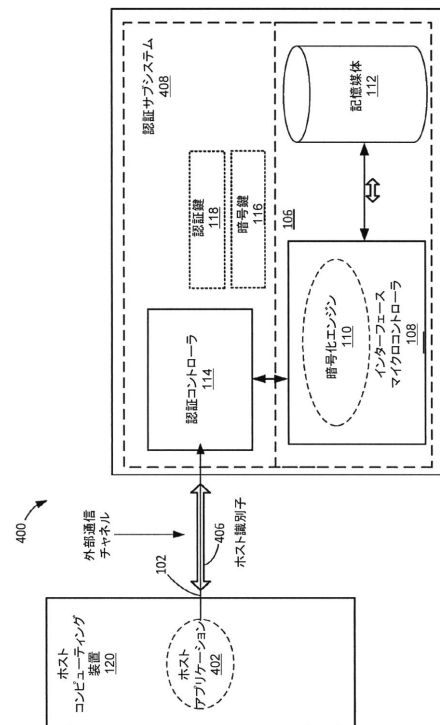
【図 2】



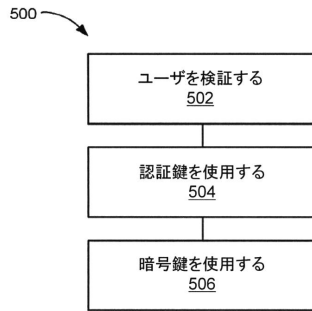
【図 3】



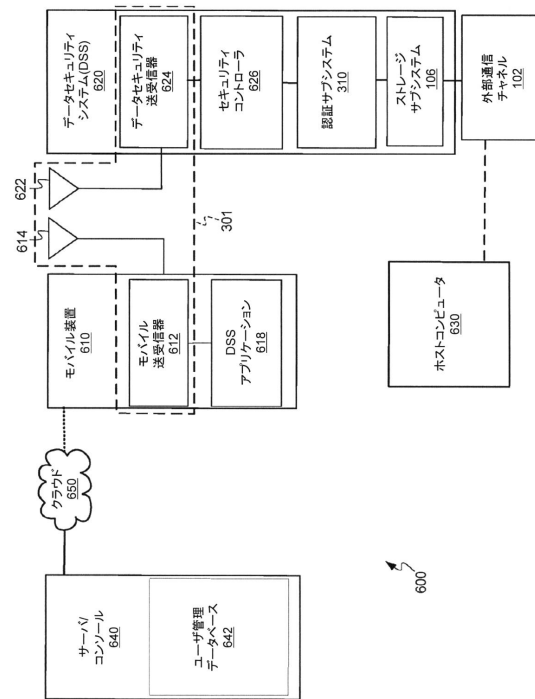
【図 4】



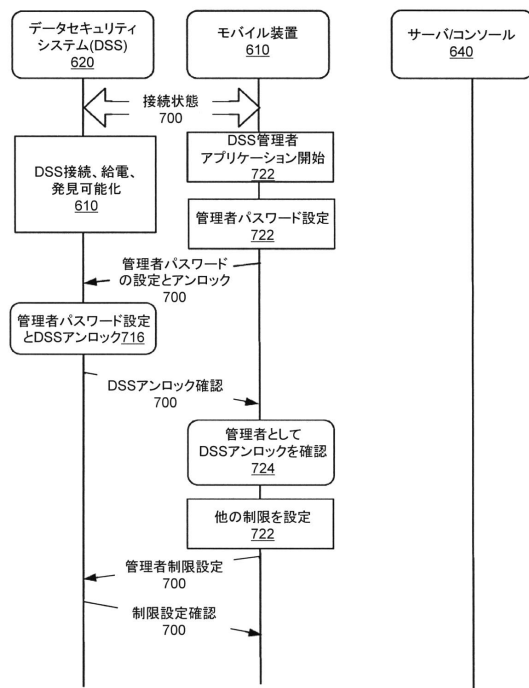
【図 5】



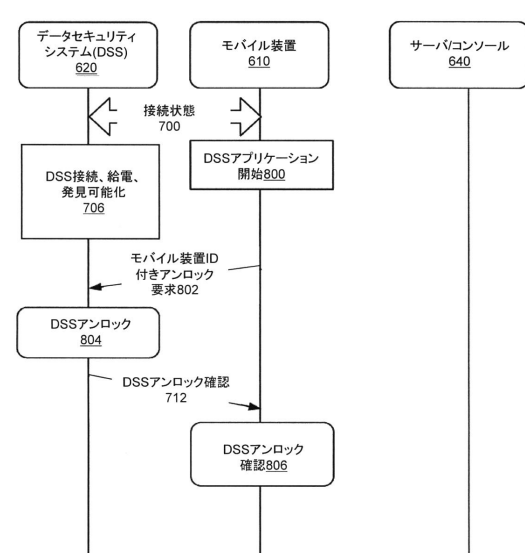
【図 6】



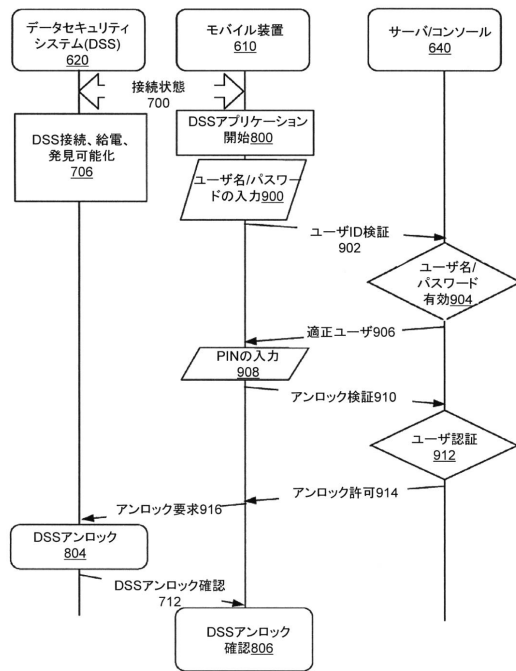
【図 7】



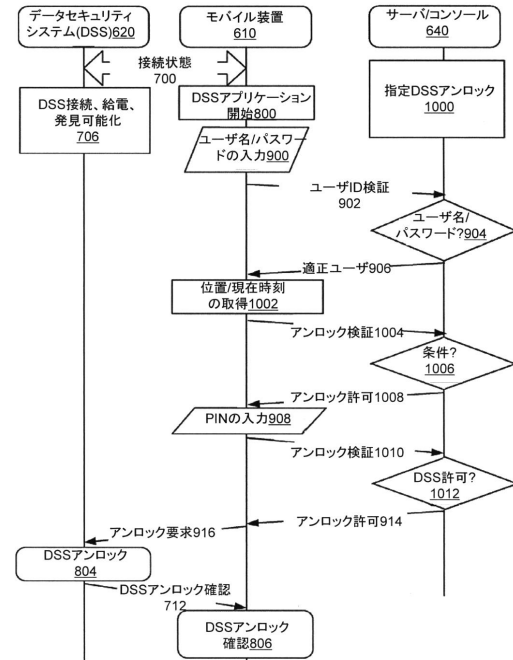
【図 8】



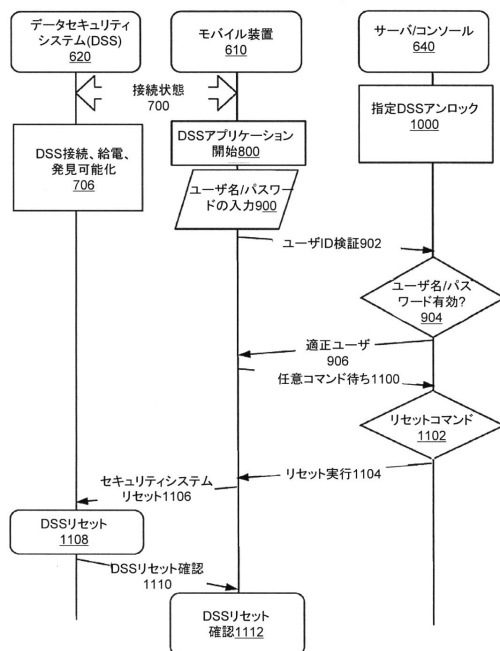
【図 9】



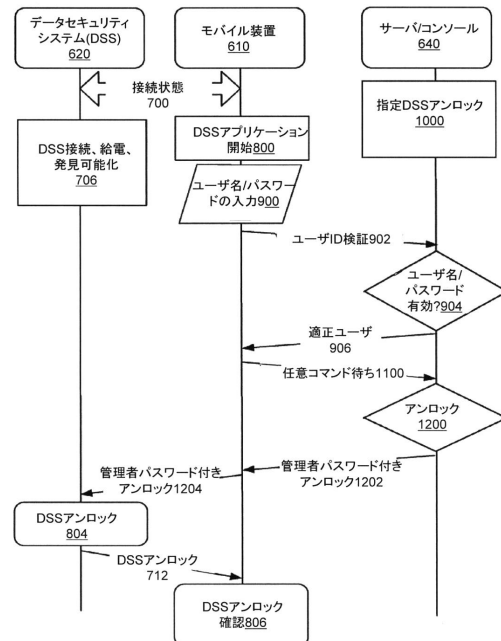
【図 10】



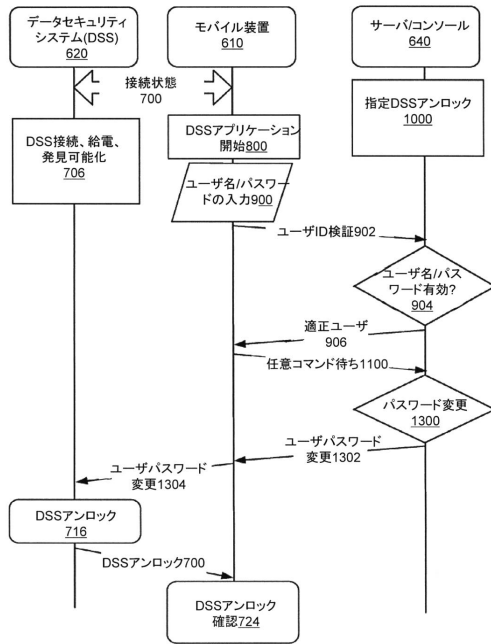
【図 11】



【図 12】



【図 13】



フロントページの続き

- (72)発明者 ボロティン、レブ エム.
アメリカ合衆国 98034 ワシントン州 カークランド エヌイー ワンハンドレッドアンド
トゥエンティフィフス ストリート 9306
- (72)発明者 レメレブ、アレックス
カナダ国 L6A 0G8 オンタリオ州 メープル リバーミル クレセント 245
- (72)発明者 シンガー、マーク
アメリカ合衆国 98105 ワシントン州 シアトル トゥエルフス アベニュー エヌイー
5510

審査官 岸野 徹

- (56)参考文献 特開2006-251857 (JP, A)
特開2006-139757 (JP, A)
特開2004-326763 (JP, A)
特表2009-524880 (JP, A)
米国特許出願公開第2003/0093693 (US, A1)
米国特許出願公開第2003/0176218 (US, A1)
米国特許第06529949 (US, B1)

- (58)調査した分野(Int.Cl., DB名)
- | | |
|------|-------|
| G06F | 21/60 |
| G06F | 21/31 |
| G06F | 21/35 |
| G06F | 21/44 |
| H04L | 9/10 |