(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-128757
(P2012-128757A)
(43)公開日　平成24年7月5日(2012.7.5)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	560C	5B017
H04L 9/32	(2006.01)	H04L	9/00	675A	5J104
G09C 1/00	(2006.01)	G09C	1/00	640D	

審査請求 未請求　請求項の数 5　ＯＬ　（全 9 頁）

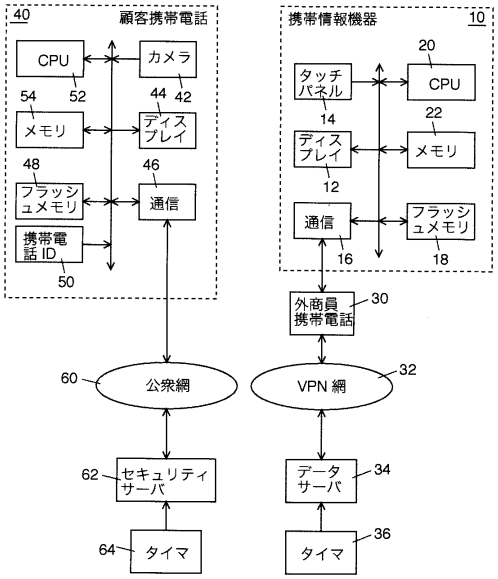
(21)出願番号　特願2010-281169 (P2010-281169)
(22)出願日　平成22年12月17日 (2010.12.17)

(71)出願人　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100090284
弁理士　田中　常雄
(72)発明者　西村　公佐
埼玉県ふじみ野市大原二丁目１番１５号株式会社ＫＤＤＩ研究所内
(72)発明者　竹森　敬祐
埼玉県ふじみ野市大原二丁目１番１５号株式会社ＫＤＤＩ研究所内

Ｆターム(参考)　5B017 AA08 BA09 CA16
5J104 AA08 AA16 AA32 EA04 EA10 EA19 JA21 LA06 NA02 NA12 NA37 NA38 PA07

(54)【発明の名称】改竄検知方法及び情報機器

(57)【要約】
【課題】
アンケートに対する記入内容の改竄の有無を検知する。
【解決手段】
ディスプレイ１２に表示されるアンケートに対し、タッチパネル１４で顧客に記入させる。携帯情報機器１０は記入内容とアンケートからハッシュ値を計算する。セキュリティサーバ６２のＵＲＬとハッシュ値が図形コードで携帯電話４０に転送され、携帯電話４０はサーバ６２にハッシュ値をアップロードする。サーバ６２はハッシュ値を収容するセキュリティトークンを生成する。携帯情報機器１０は記入内容をデータサーバ３４にアップロードする。記入内容の参照時に、携帯情報機器１０は、記入内容とアンケートからハッシュ値を再計算する。携帯電話４０又はセキュリティサーバ６２で、記入時のハッシュ値と再計算ハッシュ値を照合する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
資料に対する記入内容の改竄の有無を検知する方法であって、
当該資料を特定する資料特定情報と共に当該記入内容を第１の記憶手段に保管する記入内容保管ステップと、
当該資料と当該記入内容を結合して所定ハッシュ関数でハッシュ値を記入時ハッシュ値として計算するハッシュ値計算ステップと、
当該記入時ハッシュ値を暗号化してセキュリティトークンを生成するトークン生成ステップと、
当該セキュリティトークンを、当該第１の記憶手段とは異なる場所に位置する第２の記憶手段に保管するトークン保管ステップと、
当該記入内容の改竄を確認するために、当該記入内容を当該第１の記憶手段から読み出し、当該資料特定情報で特定される資料を読み出す読み出しステップと、
当該読み出しステップで読み出した当該資料及び当該記入内容を結合して当該所定ハッシュ関数でハッシュ値を再計算するハッシュ値再計算ステップと、
当該ハッシュ値再計算ステップで再計算されたハッシュ値と、当該セキュリティトークンに含まれる当該記入時ハッシュ値とを照合する照合ステップ
とを具備することを特徴とする改竄検知方法。
【請求項２】
更に、
当該記入時ハッシュ値を含む図形コードを生成する図形コード生成ステップと、
当該図形コードを携帯端末で読み取り、当該図形コードに含まれる当該記入時ハッシュ値をセキュリティサーバに送信するハッシュ値送信ステップ
とを具備し、
当該トークン生成ステップが、セキュリティサーバが、当該記入時ハッシュ値と現在日時を示す日時情報とを公開鍵暗号化方式の秘密鍵で暗号化してセキュリティトークンを生成するステップを含む
ことを特徴とする請求項１に記載の改竄検知方法。
【請求項３】
当該第２の記憶手段が、当該セキュリティサーバ及び当該携帯端末の何れかであることを特徴とする請求項２に記載の改竄検知方法。
【請求項４】
更に、当該資料をタッチパネルディスプレイで表示し、当該記入内容の記入を受け入れるステップを具備することを特徴とする請求項１乃至３の何れか１項に記載の改竄検知方法。
【請求項５】
資料を表示可能なディスプレイと、
当該ディスプレイの表示面に配置されるタッチパネルと、
遠隔の記憶装置と接続する通信手段と、
当該通信手段を介して、当該資料に対して当該タッチパネルで入力された記入内容を、当該資料を特定する資料特定情報と共に遠隔の記憶装置に格納する手段と、
当該資料と当該記入内容を結合して所定ハッシュ関数でハッシュ値を記入時ハッシュ値として計算するハッシュ値計算手段と、
当該記入時ハッシュ値を含む図形コードを生成して、当該ディスプレイに表示させる図形コード生成手段と、
当該記入内容の改竄を確認するために、当該通信手段を介して当該遠隔の記憶装置第１の記憶手段から当該記入内容を読み出し、当該資料特定情報で特定される資料を読み出す読み出し手段と、
当該読み出し手段で読み出した当該資料及び当該記入内容を結合して当該所定ハッシュ関数でハッシュ値を再計算するハッシュ値再計算手段

とを具備することを特徴とする情報機器。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、資料に対して電子的に記録される記入内容の改竄を検知する方法及びこの方法に用いる情報機器に関する。
【背景技術】
【０００２】
近年、電子ディスプレイ上に、加圧又は接触などにより位置座標を入力可能な入力機能を備えた「タッチパネルディスプレイ」の普及が進んでいる。タッチパネルディスプレイは主に、パーソナルコンピュータ（ＰＣ）及び種々の情報機器の操作及び文字入力に使われている。タッチパネルディスプレイを用いることで、ディスプレイ上に表示した書類に手書きの署名などを入力することも可能である。
【０００３】
タッチパネルディスプレイを使って、署名を入力及び記録し、個人認証に使用するシステムが、特許文献１～３に記載されている。
【０００４】
また、複数者間で合意した文書を安全かつ低コストに保存することが可能な文書合意システムが特許文献４に記載されている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００３－２７１９６６号公報
【特許文献２】特開２００３－２０３２００号公報
【特許文献３】特開２０００－１９４６１８号公報
【特許文献４】特開２００９－２７３０３２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
このようなタッチパネルディスプレイの利用方法の一例として、金融機関の外商員が顧客宅を訪問し、顧客に対して有価証券の募集または売り出しの提案交渉を行う場合を考える。外商員は目論見書を顧客に提示して説明を行う。多くの場合、外商員は、顧客が目論見書の内容を理解したことを確認する書類（以下では一般的に「アンケート」と表記する）を準備し、顧客の記入・署名を求める。アンケートは契約書ではなく、契約準備行為の証拠書類として作成・保管されるケースが多い。このアンケートの表示及び記入・署名は、タッチパネルディスプレイを用いることで電子的に処理することが可能である。しかし、電子データは本質的に改変が容易であるので、顧客が記入・署名した内容が改竄されていないことを保証する手段が必要となる。
【０００７】
何らかの契約準備行為において証拠書類を作成する場合が、他にも多くある。このようなケースで、タッチパネルディスプレイを用いて電子的に記入・署名された書類の信頼性を保証するには、電子データの非改竄を証明する手段が必要となる。
【０００８】
上記のアンケートの例では記入又は署名された書類の電子データを外商員が保有するＰＣ又は携帯情報機器にそのまま保存するだけでは、非改竄を保証することは困難である。すなわち、電子データを保存すると同時にその電子データが改竄されないように保護するか、もしくはその電子データが改竄された場合にはそれを検知できるような対策を施す必要がある。
【０００９】
本発明は、記入又は署名された電子化書類の非改竄を容易に検知できる改竄検知方法及

びこの方法に用いる情報機器に関する。
【課題を解決するための手段】
【００１０】
本発明に係る改竄検知方法は、資料に対する記入内容の改竄の有無を検知する方法であって、当該資料を特定する資料特定情報と共に当該記入内容を第１の記憶手段に保管する記入内容保管ステップと、当該資料と当該記入内容を結合して所定ハッシュ関数でハッシュ値を記入時ハッシュ値として計算するハッシュ値計算ステップと、当該記入時ハッシュ値を暗号化してセキュリティトークンを生成するトークン生成ステップと、当該セキュリティトークンを、当該第１の記憶手段とは異なる場所に位置する第２の記憶手段に保管するトークン保管ステップと、当該記入内容の改竄を確認するために、当該記入内容を当該第１の記憶手段から読み出し、当該資料特定情報で特定される資料を読み出す読み出しステップと、当該読み出しステップで読み出した当該資料及び当該記入内容を結合して当該所定ハッシュ関数でハッシュ値を再計算するハッシュ値再計算ステップと、当該ハッシュ値再計算ステップで再計算されたハッシュ値と、当該セキュリティトークンに含まれる当該記入時ハッシュ値とを照合する照合ステップとを具備することを特徴とする。
【００１１】
本発明に係る情報機器は、資料を表示可能なディスプレイと、当該ディスプレイの表示面に配置されるタッチパネルと、遠隔の記憶装置と接続する通信手段と、当該通信手段を介して、当該資料に対して当該タッチパネルで入力された記入内容を、当該資料を特定する資料特定情報と共に遠隔の記憶装置に格納する手段と、当該資料と当該記入内容を結合して所定ハッシュ関数でハッシュ値を記入時ハッシュ値として計算するハッシュ値計算手段と、当該記入時ハッシュ値を含む図形コードを生成して、当該ディスプレイに表示させる図形コード生成手段と、当該記入内容の改竄を確認するために、当該通信手段を介して当該遠隔の記憶装置第１の記憶手段から当該記入内容を読み出し、当該資料特定情報で特定される資料を読み出す読み出し手段と、当該読み出し手段で読み出した当該資料及び当該記入内容を結合して当該所定ハッシュ関数でハッシュ値を再計算するハッシュ値再計算手段とを具備することを特徴とする。
【発明の効果】
【００１２】
本発明によれば、タッチパネルディスプレイを用いた手書き入力による記入内容の電子データの改竄の有無の客観的証明が可能となり、証拠能力が向上する。
【図面の簡単な説明】
【００１３】
【図１】本発明の一実施例の概略構成ブロック図である。
【図２】本実施例におけるアンケート台紙への記入時の動作フローチャートである。
【図３】記入内容を確認する際の動作フローチャートである。
【発明を実施するための形態】
【００１４】
以下、図面を参照して、本発明の実施例を詳細に説明する。
【実施例１】
【００１５】
図1は、本発明の一実施例の概略構成ブロック図である。ここでは、外商員が顧客に提示したアンケートに顧客が記入するケースを例に、本実施例の機能を説明する。
【００１６】
外商員は、タッチパネルディスプレイを装備する携帯情報機器１０を具備する。外商員は、所持する携帯電話（外商員携帯電話）３０と、携帯電話網上に構築されたＶＰＮ（Virtual Private Network）網３２を介して、携帯情報機器１０を自社のデータサーバ３４に接続することができる。携帯情報機器１０と携帯電話３０は、有線又は無線で相互に接続する。携帯電話３０に相当する通信モジュールを携帯情報機器１０に内蔵しても良い。
【００１７】

データサーバ３４は、顧客に提示すべきアンケート台紙を保存しており、後述するように、顧客が記入し、署名したアンケート（記入済みアンケート）も保存できる。データサーバ３４には、現在日時を計時するタイマ又はリアルタイムクロック（ＲＴＣ）３６が接続する。データサーバ３４は、タイマ３６を参照して、データファイルを保存する際に、そのデータファイルに現在日時をタイムスタンプとして埋め込む。

【００１８】

携帯情報機器１０は、アンケート台紙及び図形コード等の種々のデータを画像として表示可能なディスプレイ１２、ディスプレイ１２の表示画面に重ねて設置され、自由筆記を入力可能なタッチパネル１４を具備する。ディスプレイ１２及びタッチパネル１４は、いわゆるタッチパネルディスプレイを構成する。省電力から、ディスプレイ１２には電子ペーパが好ましい。タッチパネル１４は、記入の際に表面に手が触れても感知しない方が書き込みやすいという点で電磁誘導方式が好ましい。

【００１９】

携帯情報機器１０は、更に、通信回路１６、フラッシュメモリ１８、ＣＰＵ２０及びメモリ２２を具備する。通信回路１６は、外商員携帯電話３０及びＶＰＮ網３２を介してデータサーバ３４と通信し、データサーバ３４からアンケート台紙を受信し、記入内容等をデータサーバ３４に送信するのに使用される。フラッシュメモリ１８は、データサーバ３４からダウンロードしたアンケート台紙、記入内容、及び、その他のデータを記憶するのに使用される。ＣＰＵ２０はメモリ２２をワークエリアとして使用して、携帯情報機器１０全体を制御する。

【００２０】

顧客の所持する携帯電話（顧客携帯電話）４０は、図形コード読み取り機能と、公衆網（携帯電話網）６０を介して、第三者の設置するセキュリティサーバ６２と通信する機能を具備する。具体的には、携帯電話４０は、カメラ４２、ディスプレイ４４、通信回路４６、フラッシュメモリ４８、携帯電話ＩＤ（不揮発性メモリに記憶される）５０、ＣＰＵ５２及びメモリ５４を具備する。携帯電話４０にインストールされた図形コード解読ソフトウエアを使って、カメラ４２により図形コードを読み取ることができる。ディスプレイ４４には、読み取られた図形コードの内容等が表示される。通信回路４６は公衆網６０に接続可能であり、携帯電話４０は、公衆網６０を介してセキュリティサーバ６２との間で後述するデータを送受信できる。携帯電話ＩＤ５０は、携帯電話４０のユーザ（顧客）を特定する情報であり、例えば、携帯電話会社から付与される携帯電話番号、又は、ユーザ識別番号である。

【００２１】

フラッシュメモリ４８は、セキュリティサーバ６２とやりとりするデータを記憶するのに使用される。ＣＰＵ５２はメモリ５４をワークエリアとして使用して、携帯電話４０の全体を制御する。ＣＰＵ５２上で、図形読み取りのプログラムが動作する。

【００２２】

セキュリティサーバ６２は、詳細を後述するように、顧客が記入した内容の改竄の有無を確認可能にするために設置される。セキュリティサーバ６２には、現在日時を計時するタイマ又はリアルタイムクロック（ＲＴＣ）６４が接続する。セキュリティサーバ６２は、タイマ６４を参照して現在日時データを取得する。

【００２３】

図２は、携帯情報機器１０、携帯電話３０、携帯電話４０、データサーバ３４及びセキュリティサーバ６２間の動作フローを示す。図２を参照して、本実施例の動作を説明する。

【００２４】

外商員は、顧客と対面する前に又は対面しつつ、携帯情報機器１０に携帯電話３０を接続し、データサーバ３４からアンケート台紙をダウンロードする（Ｓ１）。そして、顧客の面前でディスプレイ１２にアンケート台紙を表示する（Ｓ２）。顧客は、タッチパネル１４及びこれに付属のスタイラスを使って、表示されたアンケート台紙の各設問に記入す

る（Ｓ３）。

【００２５】

携帯情報機器１０のＣＰＵ２０は、アンケート台紙と記入内容とを一定の方法で結合又は一体化し、その結合結果に対して特定のハッシュ関数を用いてハッシュ値を計算する（Ｓ４）。ＣＰＵ２０は、セキュリティサーバ６２のＵＲＬとハッシュ値とを示す図形コードを生成して、ディスプレイ１２に表示し（Ｓ５）、外商員は、面前の顧客に図形コードの読み取りを促す。

【００２６】

顧客は、自己の携帯電話４０の図形コード読み取り機能を使って、携帯情報機器１０のディスプレイ１２に表示される図形コードを読み取らせる（Ｓ６）。携帯電話４０のＣＰＵ５２は、読み取った図形コードに含まれるＵＲＬ及びハッシュ値をディスプレイ４４に表示し、ユーザの接続指示に従い、当該ＵＲＬで示されるサーバ、すなわち、セキュリティサーバ６２にアクセスする。セキュリティサーバ６２ではウェブアプリケーションケーションが起動し、顧客が、ウェブアプリケーション上で「登録」を選択すると、図形コードで読み取られたハッシュ値と自己の携帯電話４０を特定する携帯電話ＩＤ５０がセキュリティサーバ６２にアップロードされる（Ｓ７）。

【００２７】

セキュリティサーバ６２は、受信したハッシュ値及び携帯電話ＩＤを一体に保管し（Ｓ８）、ハッシュ値にタイマ６４からの現在日時を加えて公開鍵暗号方式の秘密鍵で暗号化してセキュリティトークンを生成する（Ｓ９）。よく知られているとおり、公開鍵暗号方式で暗号化されたこのセキュリティトークンは、セキュリティサーバ６２が公開している公開鍵で容易に復号化できるが、公開鍵だけの情報でセキュリティトークンを改竄することは極めて困難である。セキュリティサーバ６２は、生成したセキュリティトークンと、秘密鍵に対応する公開鍵を携帯電話４０に返信する（Ｓ１０）。また、事後の照合のために、セキュリティサーバ６２は、一定期間、セキュリティトークンを携帯電話ＩＤに関連付けて保管し、期間経過後に消去する。

【００２８】

携帯電話４０は、セキュリティサーバ６２からのセキュリティトークンと公開鍵をフラッシュメモリ４８に格納し、セキュリティトークンの正常受信をディスプレイ４４に表示する（Ｓ１１）。顧客は、ディスプレイ４４の画面でセキュリティトークンの正常受信を確認すると、携帯情報機器１０のディスプレイ１２に表示されるアップロードボタンを操作して、アンケート記入内容のアップロードを指示する（Ｓ１２）。この指示に従い、携帯情報機器１０は、アンケート用紙を特定する台紙番号、アンケート記入内容、及び、顧客を特定する顧客ＩＤをデータサーバ３４にアップロードする（Ｓ１３）。なお、顧客情報（住所、電話番号及び顧客ＩＤ等）、アンケート用紙を特定する台紙番号、携帯電話３０に通常装備されるＧＰＳ装置からの現在位置情報及び現在日時が、データサーバ３４へのアップロードに際して、アンケート記入内容にメタ情報として付加される。データサーバ３４は、アップロードされた台紙番号、アンケート記入内容及び顧客ＩＤに、タイマ３６からの現在日時データをタイムスタンプとして付加して、保管する（Ｓ１４）。なお、台紙番号は、データサーバ３４上でのデータ管理の目的で付加されているバージョン情報を含む。

【００２９】

図３は、事後に顧客がアンケート記入内容を確認する際の動作フローを示す。例えば、外商員が顧客を再訪し、先のアンケート結果に基づき、更なる商談を進めるようなケースである。

【００３０】

外商員は、携帯情報機器１０を使って、訪問先の顧客によるアンケート記入内容をデータサーバ３４上で検索し、発見された記入内容のメタデータから該当するバージョンのアンケート台紙も特定する（Ｓ２１）。そして、データサーバ３４から、アンケート台紙と記入内容を携帯情報機器１０にダウンロードする（Ｓ２２）。

【００３１】
携帯情報機器１０は、顧客の面前で、ダウンロードしたアンケート台紙とその記入内容をディスプレイ１２に表示する（Ｓ２３）。外商員又は顧客がタッチパネル１４上の改竄確認ボタンを操作すると、携帯情報機器１０は、アンケート台紙と記入内容から、アンケート記入時と同様のハッシュ関数に従いハッシュ値を再計算する（Ｓ２４）。携帯情報機器１０は、セキュリティサーバ６２のＵＲＬと、再計算したハッシュ値と、記入内容をデータサーバ３４に保管した日時とを示す図形コードを作成してディスプレイ１２に表示する（Ｓ２５）。
【００３２】
顧客は、自己の携帯電話４０で図形コードを読み取り、セキュリティサーバ６２のＵＲＬ、再計算ハッシュ値及び保管日時を復元する（Ｓ２６）。携帯電話４０のＣＰＵ５２は、携帯情報機器１０に表示されるアンケート台紙の記入内容に対するセキュリティトークンをフラッシュメモリ４８に保持しているか否かを調べる（Ｓ２７）。
【００３３】
セキュリティトークンをフラッシュメモリ４８に保持している場合、当該セキュリティトークンを公開鍵で解読して、アンケート記入時のハッシュ値を復元する（Ｓ２８）。複数のセキュリティトークンを保持している場合、図形コードに含まれる記入内容の保管日時と、セキュリティトークンの保管日時を照合することで、対応するセキュリティトークンを決定できる。もちろん、日時が厳密に一致することは無いので、一定時間幅で検索することになる。携帯電話４０のＣＰＵ５２は、再計算ハッシュ値とアンケート記入時のハッシュ値を照合し（Ｓ２９）、照合結果をディスプレイ４４に表示する（Ｓ３０）。
【００３４】
対応するセキュリティトークンをフラッシュメモリ４８に保持していない場合、携帯電話４０は、図形コードに記載されたＵＲＬのセキュリティサーバ６２にアクセスし、図形コードに含まれる再計算ハッシュ値と保管日時情報に携帯電話ＩＤ５０を付加して、セキュリティサーバ６２に送信する（Ｓ３１）。
【００３５】
セキュリティサーバ６２は、携帯電話ＩＤ及び保管日時情報を参照し、アンケート記入時のセキュリティトークンを検索する（Ｓ３２）。セキュリティトークンの保管日時を携帯電話４０からの保管日時情報と一定の時間差範囲内で対比することで、該当するセキュリティトークンを限定できる。
【００３６】
セキュリティサーバ６２は、検索されたセキュリティトークンのハッシュ値（アンケート記入時のハッシュ値）と、再計算ハッシュ値を照合し（Ｓ３３）、照合結果を携帯電話４０に送信する（Ｓ３４）。同一携帯電話ＩＤに対して複数のセキュリティトークンが発見された場合、セキュリティサーバ６２は、ハッシュ値の一致するものが見つかるまで、発見されたセキュリティトークンの解読とハッシュ値の照合（Ｓ３３）を実行する。携帯電話４０は、セキュリティサーバ６２からの照合結果をディスプレイ４４に表示する（Ｓ３０）。
【００３７】
照合結果として両ハッシュ値が一致する場合、記入内容は改竄されていないことになり、一致しない場合、携帯情報機器１０に表示される記入内容は改竄されていたことになる。
【００３８】
セキュリティサーバ６２に格納するセキュリティトークン又は、その元となるハッシュ値及び携帯電話ＩＤには、使用したアンケート台紙を特定する台紙番号を付加しても良い。こうすることにより、記入内容を照合する対象を特定しやすくなる。台紙番号に、外商員の勤務先の会社を特定する番号を含めることで、複数の会社のアンケートにも対応可能となることは明らかである。
【００３９】

セキュリティトークンがセキュリティサーバ６２に保管されておらず、携帯電話４０にのみ保管されている場合、セキュリティサーバ６２が、記入時のハッシュちと再計算ハッシュ値の照合を行っても良い。この場合、携帯電話４０は、図形コードに含まれるハッシュ値と、フラッシュメモリ４８に記憶されるセキュリティトークン及びその公開鍵とをセキュリティサーバ６２に送信し、セキュリティサーバ６２は、ステップＳ３３，Ｓ３４を実行する。これはまた、携帯電話３０に、公開鍵によりセキュリティトークンを復号化するアプリケーションケーションがインストールされていない場合、又は、インストールできない場合に、適用可能である。

【００４０】

以上に詳述したように、本実施例によると、顧客は外商員の会社が保有する機器を利用しながらも、記入内容の改竄の有無を、顧客自身が保有する携帯電話を用いて、主体的かつ客観的に確認できるようになる。顧客自身が行う作業は特別なアプリケーションを必要とせず、通信内容もハッシュ値化されたデータであるので容量は小さく、通信料金の負担も僅かである。

【００４１】

外商員携帯電話３０の識別情報、携帯情報機器の固有識別情報、及び、セキュリティトークンを生成した時の顧客の携帯電話３０の位置情報といった付加的な情報をセキュリティトークンに埋め込むようにしても良い。すなわち、これらの情報を図形コードで顧客携帯電話４０に転送し、携帯電話４０がセキュリティサーバ６２に転送する。これらの情報は、外商員が用いた機器類やそれを用いた場所の特定に役立つので、証拠能力を強化できる。

【００４２】

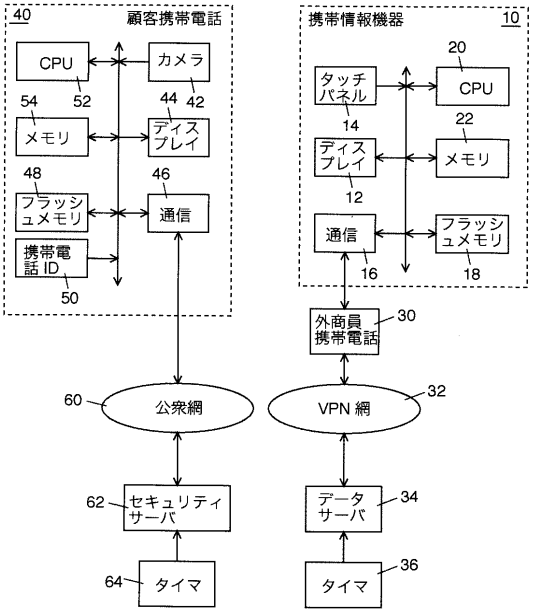
特定の説明用の実施例を参照して本発明を説明したが、特許請求の範囲に規定される本発明の技術的範囲を逸脱しないで、上述の実施例に種々の変更・修整を施しうることは、本発明の属する分野の技術者にとって自明であり、このような変更・修整も本発明の技術的範囲に含まれる。

【符号の説明】

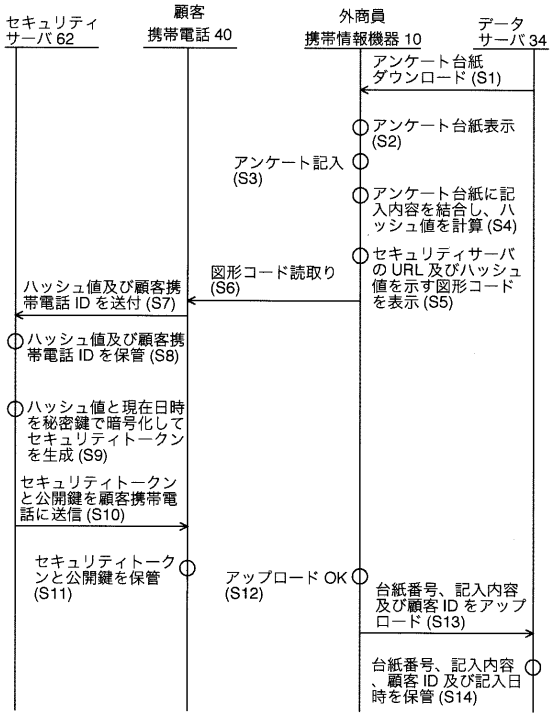
【００４３】

１０：携帯情報機器
１２：ディスプレイ
１４：タッチパネル
１６：通信回路
１８：フラッシュメモリ
２０：ＣＰＵ
２２：メモリ
３０：外商員携帯電話
３２：ＶＰＮ網
３４：データサーバ
３６：タイマ（ＲＴＣ）
４０：顧客携帯電話
４２：カメラ
４４：ディスプレイ
４６：通信回路
４８：フラッシュメモリ
５０：携帯電話ＩＤ
５２：ＣＰＵ
５４：メモリ
６０：公衆網
６２：セキュリティサーバ
６４：タイマ（ＲＴＣ）

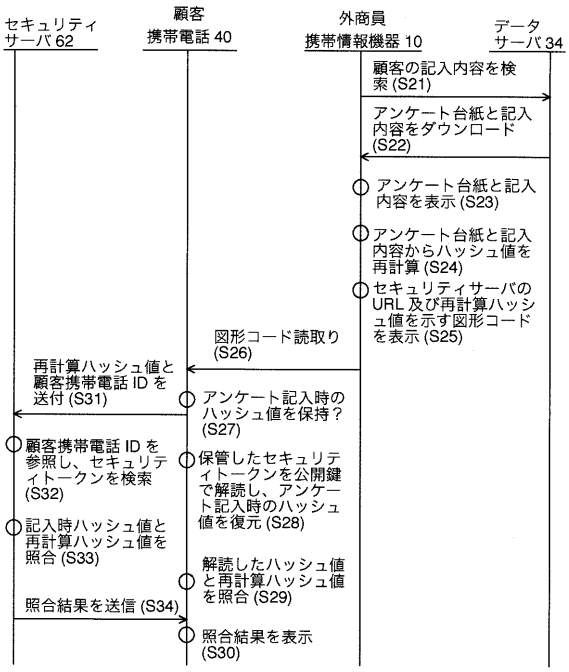
【図１】


40
顧客携帯電話
CPU
52
カメラ
44
42
54
メモリ
ディスプレイ
48
46
フラッシュメモリ
通信
携帯電話ID
50
携帯情報機器
10
20
タッチパネル
CPU
14
22
ディスプレイ
メモリ
12
通信
フラッシュメモリ
16
18
外商員携帯電話
30
60
公衆網
VPN網
32
62
セキュリティサーバ
データサーバ
34
64
タイマ
タイマ
36

【図２】


セキュリティサーバ 62
顧客携帯電話 40
外商員携帯情報機器 10
データサーバ 34
アンケート台紙ダウンロード (S1)
アンケート台紙表示 (S2)
アンケート記入 (S3)
アンケート台紙に記入内容を結合し、ハッシュ値を計算 (S4)
セキュリティサーバの URL 及びハッシュ値を示す図形コードを表示 (S5)
図形コード読取り (S6)
ハッシュ値及び顧客携帯電話 ID を送付 (S7)
ハッシュ値及び顧客携帯電話 ID を保管 (S8)
ハッシュ値と現在日時を秘密鍵で暗号化してセキュリティトークンを生成 (S9)
セキュリティトークンと公開鍵を顧客携帯電話に送信 (S10)
セキュリティトークンと公開鍵を保管 (S11)
アップロード OK (S12)
台紙番号、記入内容及び顧客 ID をアップロード (S13)
台紙番号、記入内容、顧客 ID 及び記入日時を保管 (S14)

【図３】


セキュリティサーバ 62
顧客携帯電話 40
外商員携帯情報機器 10
データサーバ 34
顧客の記入内容を検索 (S21)
アンケート台紙と記入内容をダウンロード (S22)
アンケート台紙と記入内容を表示 (S23)
アンケート台紙と記入内容からハッシュ値を再計算 (S24)
セキュリティサーバの URL 及び再計算ハッシュ値を示す図形コードを表示 (S25)
図形コード読取り (S26)
再計算ハッシュ値と顧客携帯電話 ID を送付 (S31)
アンケート記入時のハッシュ値を保持？ (S27)
顧客携帯電話 ID を参照し、セキュリティトークンを検索 (S32)
保管したセキュリティトークンを公開鍵で解読し、アンケート記入時のハッシュ値を復元 (S28)
記入時ハッシュ値と再計算ハッシュ値を照合 (S33)
解読したハッシュ値と再計算ハッシュ値を照合 (S29)
照合結果を送信 (S34)
照合結果を表示 (S30)