(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4281966号
(P4281966)
(45)発行日　平成21年6月17日(2009.6.17)　(24)登録日　平成21年3月27日(2009.3.27)

(51)Int.Cl.　　F I
H04M 11/00 (2006.01)　　H04M 11/00　301
H04M 1/67 (2006.01)　　H04M 1/67

請求項の数 19　(全 27 頁)

(21)出願番号　特願2005-121448(P2005-121448)
(22)出願日　平成17年4月19日(2005.4.19)
(65)公開番号　特開2006-303817(P2006-303817A)
(43)公開日　平成18年11月2日(2006.11.2)
審査請求日　平成18年1月26日(2006.1.26)

(73)特許権者　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町２２番２２号
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明
(74)代理人　100107489
弁理士　大塩　竹志
(72)発明者　松本　大
大阪府大阪市阿倍野区長池町２２番２２号
シャープ株式会社内
(72)発明者　田中　洋
大阪府大阪市阿倍野区長池町２２番２２号
シャープ株式会社内
最終頁に続く

(54)【発明の名称】携帯端末装置の情報保全システム、携帯端末装置の情報保全方法、制御プログラム、可読記録媒体および電子情報装置

(57)【特許請求の範囲】
【請求項１】
遠隔操作情報に応じた所定の情報保全処理を実行可能とする携帯端末装置に対する情報保全要求時に、該携帯端末装置の所有者であるか否かを本人情報により識別する個人認証処理を行う認証装置と、
該認証装置による個人認証が該本人情報と一致した場合に、該携帯端末装置を情報保全処理するための該遠隔操作情報を生成し、該遠隔操作情報を該携帯端末装置に送信処理する管理装置とを有し、
該携帯端末装置は、
送信されてくる遠隔操作情報として、該携帯端末装置との間で予め定められた保全モード情報および保全処理情報を受信する受信手段と、
該管理装置との間で予め定められた保全モード情報および保全処理情報を記憶する第１記憶手段と、
該受信手段で受信した、該携帯端末装置との間で予め定められた保全モード情報および保全処理情報を記憶する第２記憶手段と、
該第２記憶手段の保全モード情報が該第１記憶手段の保全モード情報と一致するかどうかを識別する保全モード情報識別手段と、
該第２記憶手段の保全処理情報が該第１記憶手段の保全処理情報と一致するかどうかを識別する保全処理情報識別手段と、
該保全モード情報識別手段および該保全処理情報識別手段による各識別結果に基づい

て、該遠隔操作情報に応じた所定の情報保全処理を行う情報保全処理手段と、
該情報保全処理手段によって情報保全処理が実行された後の状態を記憶する第３記憶手段としての不揮発性記憶手段とを有する携帯端末装置の情報保全システム。

【請求項２】

前記認証装置は、

連絡者側の通信手段と接続可能とする接続手段と、

前記情報保全要求の該接続手段による接続時に、該連絡者が前記携帯端末装置の所有者であるか否かを前記本人情報により識別する個人認証を行う認証手段と、

該個人認証が該本人情報と一致した場合に、情報保全処理命令を前記管理装置に出力する命令出力手段とを有する請求項１に記載の携帯端末装置の情報保全システム。

【請求項３】

前記認証手段は、前記連絡者側の通信手段と前記接続手段が接続した前記情報保全要求時に、生年月日および暗証番号の少なくともいずれかを該通信手段を介して該連絡者側にする質問に対して、該連絡者が該通信手段のキー番号で回答する本人情報と、予め記憶させている本人情報とを比較してそれらが一致するかどうかを識別する個人認証を行う請求項２に記載の携帯端末装置の情報保全システム。

【請求項４】

前記管理装置は、

前記情報保全処理命令を受信可能とする接続手段と、

該情報保全処理命令の該接続手段による受信時に、該携帯端末装置の情報保全処理を行うために遠隔操作情報を生成する遠隔操作情報生成手段と、

該遠隔操作情報生成手段で生成した遠隔操作情報を該携帯端末装置に送信する遠隔操作情報送信手段とを有する請求項１に記載の携帯端末装置の情報保全システム。

【請求項５】

前記管理装置は、前記遠隔操作情報を中継基地局を介して前記携帯端末装置に送信する請求項１または４に記載の携帯端末装置の情報保全システム。

【請求項６】

前記管理装置は、

前記携帯端末装置との通信状況を管理する管理手段と、

該管理手段が管理する通信状況に基づいて、該携帯端末装置が前記遠隔操作情報を受信したか否かを確認する確認手段とを有し、

該確認手段が該携帯端末装置への該遠隔操作情報の受信を確認できない場合に、該管理装置が該携帯端末装置への該遠隔操作情報の再送信を前記遠隔操作情報送信手段に実行させる請求項１または４に記載の携帯端末装置の情報保全システム。

【請求項７】

前記管理装置は、前記携帯端末装置と前記中継基地局との通信状況を管理する管理手段を有し、

前記中継基地局は、該携帯端末装置が前記遠隔操作情報を受信したか否かを確認する確認手段を有し、

該確認手段が該携帯端末装置への前記遠隔操作情報の受信を確認できない場合にこれを該中継基地局から該管理装置の管理手段に送信して、該管理装置が該携帯端末装置への該遠隔操作情報の再送信を前記遠隔操作情報送信手段に実行させる請求項５に記載の携帯端末装置の情報保全システム。

【請求項８】

前記管理装置は、

前記携帯端末装置との間で予め定められた保全モード情報と保全処理情報とを記憶する記憶手段を更に有し、前記遠隔操作情報生成手段は、前記遠隔操作情報を、該保全モード情報と該保全処理情報とに基づいて生成する請求項４に記載の携帯端末装置の情報保全システム。

【請求項９】

前記情報保全処理手段は、
前記携帯端末装置の盗難または紛失時に、送信されてきた前記遠隔操作情報の識別結果に基づいて、該携帯端末装置の所有者が被害を被ることを排除する所定の情報保全処理を行う請求項１に記載の携帯端末装置の情報保全システム。
【請求項１０】
前記情報保全処理手段は、
前記携帯端末装置の盗難または紛失時に、送信されてきた前記遠隔操作情報の識別結果に基づいて、該携帯端末装置の所有者への送信相手が被害を被ることを排除する所定の情報保全処理を行う請求項１または９に記載の携帯端末装置の情報保全システム。
【請求項１１】
前記情報保全処理手段は、
（１）盗難または紛失した前記携帯端末装置の本来の機能を停止させて、所有者以外の他人が使用できないようにする「電源オフ」の情報保全処理、
（２）盗難または紛失した該携帯端末装置を所有者以外の他人が使用すると、視覚または聴覚に対してアラームを発生する「警告発生」の情報保全処理、
（３）盗難または紛失した該携帯端末装置を所有者以外の他人が使用すると、所有者が予め入力して前記記憶手段に記憶させた連絡先またはメッセージを所定の表示部に表示し、該携帯端末装置を回収するための「メッセージ表示」の情報保全処理、
（４）盗難または紛失した該携帯端末装置の本来の機能を停止させて、所有者が予め入力して該記憶手段に記憶させた連絡先にのみ交信処理する「所有者連絡発信」の情報保全処理、
（５）盗難または紛失した該携帯端末装置の本来の機能のうち、所有者が予め入力した機能を停止処理する「発信機能禁止」の情報保全処理、
（６）盗難または紛失した該携帯端末装置の記録手段からデータの出力を禁止する「データ出力禁止」の情報保全処理、
（７）盗難または紛失した該携帯端末装置の記録手段からデータを消去させ、他人に見られたり使用されないようにする「記憶データ消去」の情報保全処理、
（８）盗難または紛失した該携帯端末装置の通信回線番号を消滅させ、他人が使用できないようにする「通信回線番号消滅」の情報保全処理、
（９）盗難または紛失した該携帯端末装置の記録手段から記憶データを他の所定の電子装置に転送させ、該記憶データを回収するための「記憶データ転送」の情報保全処理、
（１０）前記識別手段により使用者を識別し、所有者以外の他人が該携帯端末装置を使用できないようにする「使用者識別」の情報保全処理のうち、少なくとも一つの情報保全処理を実行する請求項９に記載の携帯端末装置の情報保全システム。
【請求項１２】
前記情報保全処理手段は、
（１）前記携帯端末装置に送信した相手に、所有者が受信できない事情にあるという所定の情報を送信する情報保全処理、
（２）該携帯端末装置に送信した相手からの受信情報を受信する機能を停止する情報保全処理、
（３）該携帯端末装置に送信した相手に、通話中または使用中のデータを送信する情報保全処理、
（４）該携帯端末装置に送信した相手に、送信情報を送信する機能を停止する情報保全処理、
（５）該携帯端末装置に送信した相手に、所有者が予め入力して前記記憶手段に記憶させた紛失メッセージを送信する情報保全処理、
（６）該携帯端末装置に送信した相手に、該携帯端末装置の情報保全システムの使用を防止する情報保全処理のうち、少なくとも一つの情報保全処理を実行する請求項１０に記載の携帯端末装置の情報保全システム。
【請求項１３】

前記通信手段は、携帯電話装置または公衆電話装置である請求項２または３に記載の携帯端末装置の情報保全システム。

【請求項１４】

請求項１に記載の携帯端末装置の情報保全システムを用いて情報保全処理を実行する携帯端末装置の情報保全方法であって、

サーバが、コンピュータ制御プログラムに基づいて、

携帯端末装置の情報保全要求時に個人認証処理を行うステップと、

該個人認証が本人情報と一致した場合に、該携帯端末装置との間で予め定められた保全モード情報と該保全処理情報とに基づいて遠隔操作情報を生成して中継基地局を介して該携帯端末装置に送信する管理ステップとを実行すると共に、

該携帯端末装置が、コンピュータ制御プログラムに基づいて、

送信されてくる遠隔操作情報として、該携帯端末装置との間で予め定められた保全モード情報および保全処理情報を受信する受信ステップと、

該受信ステップで受信した保全モード情報が、該管理装置との間で予め定められ、記憶手段に記憶した保全モード情報と一致するかどうかを識別する保全モード情報識別ステップと、

該受信ステップで受信した保全処理情報が、該管理装置との間で予め定められ、該記憶手段に記憶した保全処理情報と一致するかどうかを識別する保全処理情報識別ステップと、

該保全モード情報識別ステップおよび該保全処理情報識別ステップによる各識別結果に基づいて、該遠隔操作情報に応じた所定の情報保全処理を行う情報保全処理ステップとを実行し、該情報保全処理後の状態を不揮発性記憶手段に記憶する携帯端末装置の情報保全方法。

【請求項１５】

前記認証ステップは、

前記情報保全要求時に、連絡者が前記携帯端末装置の所有者であるか否かを前記本人情報により識別する個人認証を行うステップと、

該個人認証が該本人情報と一致した場合に、情報保全処理命令を出力する命令出力ステップとを有する請求項１４に記載の携帯端末装置の情報保全方法。

【請求項１６】

前記管理ステップは、

前記情報保全処理命令の受信時に、前記携帯端末装置の情報保全処理を行うために遠隔操作情報を生成する遠隔操作情報生成ステップと、

生成した該遠隔操作情報を該携帯端末装置に送信する遠隔操作情報送信ステップとを有する請求項１５に記載の携帯端末装置の情報保全方法。

【請求項１７】

前記管理ステップは、

前記携帯端末装置との通信状況を管理する管理ステップと、

該通信状況に基づいて、該携帯端末装置が前記遠隔操作情報を受信したか否かを確認する確認ステップとを有し、

該確認ステップで該携帯端末装置への該遠隔操作情報の受信を確認できない場合に、該携帯端末装置への該遠隔操作情報の再送信を実行させる請求項１４または１６に記載の携帯端末装置の情報保全方法。

【請求項１８】

請求項１４～１７のいずれかに記載の携帯端末装置の情報保全方法の各ステップをコンピュータに実行させるための制御プログラム。

【請求項１９】

請求項１８に記載の制御プログラムが記録されたコンピュータ読み取り可能な可読記録媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＰＨＳ（Ｐｅｒｓｏｎａｌ Ｈａｎｄｙ Ｐｈｏｎｅ Ｓｙｓｔｅｍ）、携帯電話装置などを含む通信手段を有するデータ処理端末装置である携帯端末装置に、これが盗難や紛失したときに、その携帯端末装置内の情報に関するセキュリティを高める情報保全処理機能を持たせた携帯端末装置の情報保全システム、携帯端末装置の情報保全方法、この方法をコンピュータに実行させるための各処理手順が記述された制御プログラム、その制御プログラムが記述されたコンピュータ読み取り可能な可読記録媒体およびこの可読記録媒体から制御プログラムを読み取ってこの方法を実行可能な電子情報装置に関する。
【背景技術】
【０００２】
現在、携帯電話装置などの携帯端末装置は、その特色上、広い不特定領域の屋外に装置を持ち出して使用されている。また、通信回線が登録されている携帯端末装置は、ＰＨＳやデータ処理端末装置など、デジタル信号情報のコンピュータ周辺端末装置として用途が拡大されていると共に、その持ち出し使用領域も広がりつつある。さらに、携帯端末装置は、その使用方法も容易であり、多くの人々からの需要がある。さらに、昨今の携帯端末装置の多機能化により、大容量のメモリやカメラ機能などが搭載されて、その所有者は、電話帳に多くの相手情報を登録したり、大量のメールやカメラデータなどを保持したりできるようになっている。
【０００３】
しかしながら、このように、従来の携帯端末装置は、所有者がその装置自体を屋外などに持ち出して、手軽に携帯して使用することができるため、盗難や紛失する機会も多い。盗難や紛失した携帯端末装置が第三者に拾得された場合にも、第三者に容易に使用される可能性があり、電話帳やメール、カメラデータなどの貴重な個人情報や各種情報、重要データなどを盗み見されるなど、所有者が被害を被るという問題が発生している。
【０００４】
このため、その所有者側で、携帯端末装置のセキュリティに対する意識レベルが高くなってきており、携帯端末装置の情報保全システムが必須となってきている。このような盗難や紛失時における問題を解決するために、従来より、様々な携帯端末装置の情報保全方法が提案されている。
【０００５】
例えば、携帯端末装置の全所定対応機種では、非特許文献１に示されているような遠隔ロック機能を搭載している。この遠隔ロック機能は、予め所定の携帯端末装置に情報保全用として登録した電話番号により、紛失した携帯端末装置に発信し、これを指定回数行うことによって、携帯端末装置の情報保全を実施する仕組みである。
【０００６】
図９は、上記非特許文献１の遠隔ロック機能の処理手順を説明するためのフローチャートである。なお、図９では、指定回数を３回とした場合について説明する。
【０００７】
図９に示すように、まず、予め所定の携帯端末装置に登録した電話番号に基づいて、紛失した携帯端末装置側に発信する。ステップＳ９１で第１回目の受信の呼び出し信号回数をカウントし、ステップＳ９２でそのカウント値が予め設定された第１回目のコール回数であると識別されたか否かを判定する。ステップＳ９２で、否定判定された場合（ＮＯ）にはステップＳ９１の処理に戻り、肯定判定された場合（ＹＥＳ）には次のステップＳ９３の処理に移行する。
【０００８】
次に、ステップＳ９３で第２回目の受信の呼び出し信号回数をカウントし、ステップＳ９４でそのカウント値が予め設定された第２回目のコール回数と識別されたか否かを判定

する。ステップＳ９４で、否定判定された場合（ＮＯ）にはステップＳ９１の処理に戻り、肯定判定された場合（ＹＥＳ）には次のステップＳ９５の処理に移行する。

【０００９】

ステップＳ９５で第３回目の受信の呼び出し信号回数をカウントし、ステップＳ９６でそのカウント値が予め設定された第３回目のコール回数と識別されたか否かを判定する。ステップＳ９６で、否定判定された場合（ＮＯ）にはステップＳ９１の処理に戻り、肯定判定された場合（ＹＥＳ）にはステップＳ９７の処理に移行する。

【００１０】

ステップＳ９７で情報保全システムを立ち上げて、ステップＳ９８でその情報保全システムによる情報保全処理を実施する。

【００１１】

この従来技術によれば、予め入力して記憶手段に蓄積記憶させた呼び出し信号回数のパターンを、盗難・紛失した携帯端末装置が受信した場合に、所定の情報保全処理が実施されて、盗難や紛失した携帯端末装置の所有者が、個人情報やその他の重要データを盗み見されるなどの被害を被ることを排除することができる。ところが、盗難・紛失した携帯端末装置を拾得した者が、その予め設定された呼び出し信号回数のパターンに応答した場合や、その時点では盗難・紛失した携帯端末装置と交信ができないような事態が生じている場合には、所定の情報保全処理が実施されない。これを解決するために、例えば特許文献１に「携帯型電子装置の保全システム」が提案されている。

【００１２】

即ち、特許文献１には、所有者が直接、公衆電話装置や携帯電話装置などの通信手段を利用して、キーワードおよび遠隔操作データを送ることによって、盗難・紛失した携帯端末装置内の情報を保全できる情報保全システムが開示されている。

【００１３】

図１０は、特許文献１の携帯端末装置の保全システムによる処理手順を説明するためのフローチャートである。

【００１４】

図１０に示すように、まず、ステップＳ１０１で、携帯端末装置の所有者は、パーソナルコンピュータやプッシュ電話装置などを用いて、所有する携帯端末装置に対して通信を開始するべく、遠隔操作データを入力する。この場合、携帯端末装置の内部に記憶されている情報の重要度により、情報保全内容を意味する遠隔操作データの内容を選択して送信する。この選択項目としては、例えば、記憶データの出力禁止や記憶データの転送、記憶データの消去などが挙げられる。また、遠隔操作データとしては、所有者のみが知っている情報保全を行うためのキーワードも入力する。

【００１５】

この入力された遠隔操作データは、ステップＳ１０２で公衆および専用回線網を介して携帯端末装置の基地局に転送され、ステップＳ１０３で携帯端末装置の基地局から無線通信によって、紛失した携帯端末装置に送信される。

【００１６】

ステップＳ１０４で、その紛失した携帯端末装置が遠隔操作データを受信すると、ステップＳ１０５で遠隔操作データ内のキーワードが予め所有者によって記憶手段に記憶させておいたキーワードであるか否かを照合して識別する。ステップＳ１０５で不一致である場合（ＮＯ）には、その紛失した携帯端末装置はステップＳ１０４の次のデータ受信を待ち、情報保全処理システムを終了して通常のモードに戻す。また、キーワードが一致した場合（ＹＥＳ）には、ステップＳ１０６で情報保全処理システムを立ち上げ、装置のプロテクト機能を起動させる。

【００１７】

ステップＳ１０７でその紛失した携帯端末装置はその受信した遠隔操作データが所定の遠隔操作データであるか否かを識別する。ステップＳ１０７で遠隔操作データでない場合（ＮＯ）には、その紛失した携帯端末装置はステップＳ１０４の次のデータ受信を待ち、

情報保全処理システムを終了して通常のモードに戻す。また、その受信した遠隔操作データが所定の遠隔操作データである場合（ＹＥＳ）には、ステップＳ１０８で遠隔操作データの内容に沿った情報保全処理を実施する。

【００１８】

この従来技術によれば、偶然の携帯端末装置の盗難や紛失に対して、その所有者自身が遠隔操作を行うことにより、携帯端末装置の所有者が被害を被ることを排除する所定の情報保全手段を動作させて、紛失した携帯端末装置の所有者の財産または情報に関わるセキュリティを高めることができる。これにより、簡単に携帯端末装置の内部のデータを保護することができ、さらに、他人に、その紛失した携帯端末装置が勝手に使用されても、その使用料金を支払わされるという不具合を回避することができる。

【非特許文献１】ｈｔｔｐ：／／ｗｗｗ．ｄｏｃｏｍｏｋｙｕｓｙｕ．ｃｏ．ｊｐ／ｉｎｆｏ／ｗｅｅｋｌｙ／ｗｄ＿０４１００６＿５．ｈｔｍｌ２００５／０１／０６現在）

【特許文献１】特開平１０－１７７５２５号公報

【発明の開示】

【発明が解決しようとする課題】

【００１９】

上述した非特許文献１の遠隔ロック機能は、予め情報保全用として登録された電話番号から、その紛失した携帯端末装置に指定回数だけ着信させることによって情報保全処理を行って、第三者による情報の盗み見などを防ぐことができる。

【００２０】

しかしながら、この非特許文献１の手法では、その紛失した携帯端末装置の電話番号が予め登録された特定の機器からしかその情報保全処理を実施できず、その所有者が特定の機器に至るまでに時間がかかる場合には、盗難・紛失時から携帯端末装置内の情報を保全するまでに時間がかかる。例えば、出先で携帯端末装置を紛失した場合、自宅の電話装置に、その紛失した携帯端末装置の電話番号が情報保全用として登録されている場合には、その所有者が自宅まで戻らないと、その紛失した携帯端末装置を情報保全することができない。この間に、その携帯端末装置内のデータが第三者によって盗み見されてしまう虞がある。

【００２１】

また、この非特許文献１の情報保全手法では、第三者により誤って携帯端末装置の情報保全処理が実施されてしまうという可能性もある。例えば、公衆電話装置が予め情報保全用として登録されている場合、出先で携帯端末装置が紛失したときには有効である。しかしながら、第三者が公衆電話装置から所有者の携帯端末装置に発信して、所有者が応答できない状況である場合などに、第三者が何回も公衆電話装置から所有者の携帯端末装置に発信し直すことは、容易に想定することができる。この第三者による発信回数がその指定回数に達した場合には、その第三者が意図的でなくても、所有者の携帯端末装置による情報保全処理が実施されてしまい、その所有者が携帯端末装置を紛失していない場合にもその携帯端末装置を情報保全処理により使用不可能にしてしまうという虞もある。

【００２２】

さらに、この非特許文献１の情報保全手法では、その所有者は、盗難や紛失した携帯端末装置が情報保全されるまで、情報保全用として登録された特定の電話装置から、その紛失した携帯端末装置に対して発信を何回も行わなければならないという手間も必要である。例えば、紛失した携帯端末装置が電波の届かない場所にある場合、情報保全用として登録された特定の電話装置から、紛失した携帯端末装置に発信しても、その紛失した携帯端末装置側では受信が不可能である。所有者は、その紛失した携帯端末装置が受信し、かつ、情報保全処理の実施が確認されるまで、何回も発信し続ける必要がある。しかも、指定回数分、紛失した携帯端末装置が受信するまで、発信を行わなければならないという膨大な手間と時間を要してしまう。

【００２３】

一方、上述した特許文献１の携帯端末装置の情報保全システムでは、その所有者が直接

、公衆電話装置や携帯電話装置などの通信手段を利用して、キーワードを含む遠隔操作データを、紛失した携帯端末装置に送信することによって、盗難・紛失した携帯端末装置を情報保全処理することができる。この情報保全手法では、上記非特許文献１の遠隔ロック機能のような特定の電話装置以外（パーソナルコンピュータも含む）からも、携帯端末装置の情報保全を行うことができる。

【００２４】

しかしながら、この特許文献１の情報保全手法では、既存の通信手段から携帯端末装置の情報保全処理を簡易に行うことができるため、第三者による遠隔操作の悪用という危険性が極めて高くなる。例えば、悪意のある第三者がパーソナルコンピュータを用いてランダムにキーワードを生成し、「記憶データ消去」の情報保全内容を選択して遠隔操作データとして大量に携帯端末装置に送信した場合、任意のデータのいずれか一つがキーワードとして識別されて携帯端末装置の情報保全処理が勝手に実施されて、その所有者が気付かないうちに携帯端末装置内の貴重な記憶データが消去されてしまう虞がある。

【００２５】

また、この特許文献１の情報保全手法では、携帯端末装置の盗難や紛失時に、その所有者が情報保全処理を行うためのキーワードおよび遠隔操作データの送信方法の両方を把握していない可能性も高い。

【００２６】

さらに、この特許文献１の情報保全手法では、基地局からの遠隔操作データを携帯端末装置が受信できない場合について、明確にその対処方法について記載されていない。例えば、基地局が遠隔操作データを一回しか送信しない情報保全システムであれば、紛失した携帯端末装置が電波の届かない場所にある場合には、その時点で紛失した携帯端末装置は受信不可能になる。よって、その所有者は、紛失した携帯端末装置が受信し、かつ、情報保全処理の実施が確認されるまで、何回も遠隔操作データを作成して送信し続けるという手間と時間が必要になる。

【００２７】

本発明は、上記従来の問題を解決するもので、携帯端末装置の盗難、紛失時に、その所有者が情報保全処理を行うためのキーワードや遠隔操作データの送信方法を把握していなくても、少ない手間と時間で確実に、所有者が被害を被ることを排除できる携帯端末装置の情報保全システム、携帯端末装置の情報保全方法、この方法をコンピュータに実行させるための各処理手順が記述された制御プログラム、この制御プログラムが記述されたコンピュータ読み取り可能な可読記録媒体およびこの可読記録媒体から制御プログラムを読み取ってこの方法を実行可能な電子情報装置を提供することを目的とする。

【課題を解決するための手段】

【００２８】

本発明の携帯端末装置の情報保全システムは、遠隔操作情報に応じた所定の情報保全処理を実行可能とする携帯端末装置に対する情報保全要求時に、該携帯端末装置の所有者であるか否かを本人情報により識別する個人認証処理を行う認証装置と、

該認証装置による個人認証が該本人情報と一致した場合に、該携帯端末装置を情報保全処理するための該遠隔操作情報を生成し、該遠隔操作情報を該携帯端末装置に送信処理する管理装置とを有し、該携帯端末装置は、送信されてくる遠隔操作情報として、該携帯端末装置との間で予め定められた保全モード情報および保全処理情報を受信する受信手段と、　該管理装置との間で予め定められた保全モード情報および保全処理情報を記憶する第１記憶手段と、該受信手段で受信した、該携帯端末装置との間で予め定められた保全モード情報および保全処理情報を記憶する第２記憶手段と、該第２記憶手段の保全モード情報が該第１記憶手段の保全モード情報と一致するかどうかを識別する保全モード情報識別手段と、　該第２記憶手段の保全処理情報が該第１記憶手段の保全処理情報と一致するかどうかを識別する保全処理情報識別手段と、該保全モード情報識別手段および該保全処理情報識別手段による各識別結果に基づいて、該遠隔操作情報に応じた所定の情報保全処理を行う情報保全処理手段と、該情報保全処理手段によって情報保全処理が実行された後の

状態を記憶する第３記憶手段としての不揮発性記憶手段とを有し、そのことにより上記目的が達成される。

【００２９】
また、好ましくは、本発明の携帯端末装置の情報保全システムにおける認証装置は、連絡者側の通信手段と接続可能とする接続手段と、前記情報保全要求の該接続手段による接続時に、該連絡者が前記携帯端末装置の所有者であるか否かを前記本人情報により識別する個人認証を行う認証手段と、該個人認証が該本人情報と一致した場合に、情報保全処理命令を前記管理装置に出力する命令出力手段とを有する。

【００３０】
さらに、好ましくは、本発明の携帯端末装置の情報保全システムにおける認証手段は、前記連絡者側の通信手段と前記接続手段が接続した前記情報保全要求時に、生年月日および暗証番号のいずれかを該通信手段を介して該連絡者側にする質問に対して、該連絡者が該通信手段のキー番号で回答する本人情報と、予め記憶させている本人情報とを比較してそれらが一致するかどうかを識別する個人認証を行う。

【００３１】
さらに、好ましくは、本発明の携帯端末装置の情報保全システムにおける管理装置は、
前記情報保全処理命令を受信可能とする接続手段と、該情報保全処理命令の受信時に、該携帯端末装置の情報保全処理を行うために遠隔操作情報を生成する遠隔操作情報生成手段と、該遠隔操作情報生成手段で生成した遠隔操作情報を該携帯端末装置に送信する遠隔操作情報送信手段とを有する。

【００３２】
さらに、好ましくは、本発明の携帯端末装置の情報保全システムにおける管理装置は、前記遠隔操作情報を中継基地局を介して該携帯端末装置に送信する。

【００３３】
さらに、好ましくは、本発明の携帯端末装置の情報保全システムにおける管理装置は、
前記携帯端末装置との通信状況を管理する管理手段と、該管理手段が管理する通信状況に基づいて、前記携帯端末装置が前記遠隔操作情報を受信したか否かを確認する確認手段とを有し、該確認手段が該携帯端末装置への前記遠隔操作情報の受信を確認できない場合に、該携帯端末装置への該遠隔操作情報の再送信を前記遠隔操作情報送信手段に実行させる。

【００３４】
さらに、好ましくは、本発明の携帯端末装置の情報保全システムにおいて、前記管理装置は、前記携帯端末装置と前記中継基地局との通信状況を管理する管理手段を有し、前記中継基地局は、該携帯端末装置が前記遠隔操作情報を受信したか否かを確認する確認手段を有し、該確認手段が該携帯端末装置への前記遠隔操作情報の受信を確認できない場合にこれを該中継基地局から該管理装置の管理手段に送信して、該管理手段が該携帯端末装置への該遠隔操作情報の再送信を前記遠隔操作情報送信手段に実行させる。

【００３５】
さらに、好ましくは、本発明の携帯端末装置の情報保全システムにおける管理装置は、
前記携帯端末装置との間で予め定められた保全モード情報と保全処理情報とを記憶する記憶手段を更に有し、前記遠隔操作情報生成手段は、前記遠隔操作情報を、該保全モード情報と該保全処理情報とに基づいて生成する。

【００４０】
さらに、好ましくは、本発明の携帯端末装置の情報保全システムにおける情報保全処理手段は、前記携帯端末装置の盗難または紛失時に、送信されてきた前記遠隔操作情報の識別結果に基づいて、該携帯端末装置の所有者が被害を被ることを排除する所定の情報保全処理を行う。

【００４１】
さらに、好ましくは、本発明の携帯端末装置の情報保全システムにおける情報保全処理

手段は、前記携帯端末装置の盗難または紛失時に、送信されてきた前記遠隔操作情報の識別結果に基づいて、該携帯端末装置の所有者への送信相手が被害を被ることを排除する所定の情報保全処理を行う。

【００４２】

さらに、好ましくは、本発明の携帯端末装置の情報保全システムにおける情報保全処理手段は、

（１）盗難または紛失した前記携帯端末装置の本来の機能を停止させて、所有者以外の他人が使用できないようにする「電源オフ」の情報保全処理、

（２）盗難または紛失した該携帯端末装置を所有者以外の他人が使用すると、視覚または聴覚に対してアラームを発生する「警告発生」の情報保全処理、

（３）盗難または紛失した該携帯端末装置を所有者以外の他人が使用すると、所有者が予め入力して前記記憶手段に記憶させた連絡先またはメッセージを所定の表示部に表示し、該携帯端末装置を回収するための「メッセージ表示」の情報保全処理、

（４）盗難または紛失した該携帯端末装置の本来の機能を停止させて、所有者が予め入力して該記憶手段に記憶させた連絡先にのみ交信処理する「所有者連絡発信」の情報保全処理、

（５）盗難または紛失した該携帯端末装置の本来の機能のうち、所有者が予め入力した機能を停止処理する「発信機能禁止」の情報保全処理、

（６）盗難または紛失した該携帯端末装置の記録手段からデータの出力を禁止する「データ出力禁止」の情報保全処理、

（７）盗難または紛失した該携帯端末装置の記録手段からデータを消去させ、他人に見られたり使用されないようにする「記憶データ消去」の情報保全処理、

（８）盗難または紛失した該携帯端末装置の通信回線番号を消滅させ、他人が使用できないようにする「通信回線番号消滅」の情報保全処理、

（９）盗難または紛失した該携帯端末装置の記録手段から記憶データを他の所定の電子装置に転送させ、該記憶データを回収するための「記憶データ転送」の情報保全処理、

（１０）前記識別手段により使用者を識別し、所有者以外の他人が該携帯端末装置を使用できないようにする「使用者識別」の情報保全処理のうち、少なくとも一つの情報保全処理を実行する。

【００４３】

さらに、好ましくは、本発明の携帯端末装置の情報保全システムにおける情報保全処理手段は、

（１）前記携帯端末装置に送信した相手に、所有者が受信できない事情にあるという所定の情報を送信する情報保全処理、

（２）該携帯端末装置に送信した相手からの受信情報を受信する機能を停止する情報保全処理、

（３）該携帯端末装置に送信した相手に、通話中または使用中のデータを送信する情報保全処理、

（４）該携帯端末装置に送信した相手に、送信情報を送信する機能を停止する情報保全処理、

（５）該携帯端末装置に送信した相手に、所有者が予め入力して前記記憶手段に記憶させた紛失メッセージを送信する情報保全処理、

（６）該携帯端末装置に送信した相手に、該携帯端末装置の情報保全システムの使用を防止する情報保全処理のうち、少なくとも一つの情報保全処理を実行する。

【００４４】

さらに、好ましくは、本発明の携帯端末装置の情報保全システムにおける通信手段は、携帯電話装置または公衆電話装置である。

【００４５】

本発明の携帯端末装置の情報保全方法は、請求項１に記載の携帯端末装置の情報保全システムを用いて情報保全処理を実行する携帯端末装置の情報保全方法であって、サーバが

、コンピュータ制御プログラムに基づいて、携帯端末装置の情報保全要求時に個人認証処理を行うステップと、該個人認証が本人情報と一致した場合に、該携帯端末装置との間で予め定められた保全モード情報と該保全処理情報とに基づいて遠隔操作情報を生成して中継基地局を介して該携帯端末装置に送信する管理ステップとを実行すると共に、該携帯端末装置が、コンピュータ制御プログラムに基づいて、送信されてくる遠隔操作情報として、該携帯端末装置との間で予め定められた保全モード情報および保全処理情報を受信する受信ステップと、該受信ステップで受信した保全モード情報が、該管理装置との間で予め定められ、記憶手段に記憶した保全モード情報と一致するかどうかを識別する保全モード情報識別ステップと、該受信ステップで受信した保全処理情報が、該管理装置との間で予め定められ、該記憶手段に記憶した保全処理情報と一致するかどうかを識別する保全処理情報識別ステップと、該保全モード情報識別ステップおよび該保全処理情報識別ステップによる各識別結果に基づいて、該遠隔操作情報に応じた所定の情報保全処理を行う情報保全処理ステップとを実行し、該情報保全処理後の状態を不揮発性記憶手段に記憶するものであり、そのことにより上記目的が達成される。

【００４６】

また、好ましくは、本発明の携帯端末装置の情報保全方法における認証ステップは、前記情報保全要求時に、連絡者が前記携帯端末装置の所有者であるか否かを前記本人情報により識別する個人認証を行うステップと、該個人認証が該本人情報と一致した場合に、情報保全処理命令を出力する命令出力ステップとを有する。

【００４７】

さらに、好ましくは、本発明の携帯端末装置の情報保全方法における管理ステップは、

前記情報保全処理命令の受信時に、前記携帯端末装置の情報保全処理を行うために遠隔操作情報を生成する遠隔操作情報生成ステップと、生成した該遠隔操作情報を該携帯端末装置に送信する遠隔操作情報送信ステップとを有する。

【００４８】

さらに、好ましくは、本発明の携帯端末装置の情報保全方法における管理ステップは、

前記携帯端末装置との通信状況を管理する管理ステップと、該通信状況に基づいて、該携帯端末装置が前記遠隔操作情報を受信したか否かを確認する確認ステップとを有し、該確認ステップで該携帯端末装置への該遠隔操作情報の受信を確認できない場合に、該携帯端末装置への該遠隔操作情報の再送信を実行させる。

【００５１】

本発明の制御プログラムは、本発明の上記携帯端末装置の情報保全方法の各ステップをコンピュータに実行させるためのものであり、そのことにより上記目的が達成される。

【００５２】

本発明の可読記録媒体は、本発明の上記制御プログラムが記録されたコンピュータ読み取り可能なものであり、そのことにより上記目的が達成される。

【００５３】

本発明の電子情報装置は、携帯端末装置の情報保全要求時に個人認証処理を行う認証手段と、該個人認証が本人情報と一致した場合に、遠隔操作情報を生成して該携帯端末装置に送信する手段とを有しており、そのことにより上記目的が達成される。

【００５４】

本発明の電子情報装置は、前記遠隔操作情報を受信し、この受信した該遠隔操作情報を識別する識別手段と、該識別手段による識別結果に基づいて、該遠隔操作情報に応じた所定の情報保全処理を実行する手段とを有しており、そのことにより上記目的が達成される。

【００５５】

上記構成により、以下に、本発明の作用について説明する。

【００５６】

本発明においては、携帯端末装置が盗難したり紛失したりしたときに、その所有者によ

って、認証装置に対して電話をかけて携帯端末装置の情報保全要求が行われる。認証装置では、所有者であるか否かを本人情報により識別するための個人認証処理が行われ、この個人認証処理によって本人情報と一致した場合にのみ、管理装置に対して情報保全命令が出される。

【００５７】

管理装置では、認証装置から情報保全命令を受けると、携帯端末装置を情報保全処理するための独自の遠隔操作情報（遠隔操作パケット）が生成され、これが中継基地局へ送信される。

【００５８】

中継基地局では、管理装置から遠隔操作パケットを受けると、例えば無線通信によりその遠隔操作パケットが紛失した携帯端末装置に送信される。

【００５９】

携帯端末装置では、その遠隔操作パケットが受信手段にて受信され、識別手段にて遠隔操作パケットが識別される。さらに、その識別結果が内部記憶情報と一致した場合にのみ、情報保全手段にて遠隔操作パケットの内容に沿った情報保全処理が実施されて、携帯端末装置の所有者が被害を被ることが排除される。

【発明の効果】

【００６０】

以上により、本発明によれば、携帯端末装置の盗難や紛失に対して、その所有者が遠隔操作情報により遠隔操作することにより、携帯端末装置の所有者が被害を被ることを排除する所定の情報保全処理が実施され、携帯端末装置の所有者の財産である情報に関わるセキュリティをいっそう高めることができる。

【００６１】

従来手法のような情報保全を行うためのキーワードや遠隔操作データの送信方法を所有者が把握していなくても、所有者が認証装置に対して電話を行って情報保全要求を行うだけで、即座に盗難や紛失した携帯端末装置の所有者が被害を被ることを排除することができる。なお、認証装置への連絡手段は一般的であり、所有者が盗難や紛失時にも把握していると考えられるため、従来手法のような盗難や紛失時から携帯端末装置の情報保全を行うまでのタイムラグが生じることなく、早急に携帯端末装置の情報保全を行うことができる。

【００６２】

また、認証装置にて所有者であるか否かの個人認証を行うことによって、所有者以外の第三者による情報保全処理の実施を防ぐことができる。

【００６３】

さらに、管理装置にて独自に生成される遠隔操作情報（遠隔操作パケット）を利用することによって、一般の携帯端末装置利用者からの遠隔操作パケットにより誤った情報保全処理が実施される危険性がない。

【００６４】

さらに、管理装置では、盗難や紛失した携帯端末装置と中継基地局との電波状況を把握することができるため、遠隔操作パケットが携帯端末装置に確実に受信されるまで、何回でも自動的にリトライすることができる。これにより、所有者自身が何回も遠隔操作パケットを送信する手間や時間が必要なくなる。

【００６５】

さらに、保全モード情報と保全処理情報とによって、ケースバイケースで最適の情報保全処理を選択して、最適の情報保全処理を適用することができる。

【００６６】

さらに、情報保全処理後の状態を記憶する記憶手段を設けることによって、情報保全処理を実行後に電源を再投入しても、その情報保全状態に戻ってそれを継続させることができる。

【発明を実施するための最良の形態】

【００６７】
以下に、本発明の携帯端末装置の情報保全システムの実施形態について、図面を参照しながら詳細に説明する。
【００６８】
図１は、本発明の実施形態に係る携帯端末装置の情報保全システムの要部構成例を示すブロック図である。
【００６９】
図１において、携帯端末装置の情報保全システム１は、携帯電話装置２や一般電話装置３からの連絡者が所有者であるか否かを識別する個人認証処理を行う認証装置４と、情報保全処理を行うための遠隔操作情報（遠隔操作パケット）を生成する管理装置５と、一つ以上の中継基地局６と、この中継基地局６と電波（無線）や有線を介して接続されているユーザ側の携帯端末装置７とを備えている。なお、図１では、これらの認証装置４と管理装置５は通信業者のサービスサーバ内に設けられている場合について示すが、これは一例であって、同様の役割を実現できるものであれば、他の実現方法であってもよい。また、図１では、中継基地局６を一つ示しているが、二つ以上の中継基地局６が含まれていてもよい。さらに、これらの携帯電話装置２、一般電話装置３、サービスサーバ、中継基地局６および携帯端末装置７は、電波通信回線や有線通信回線などの公衆回線網に接続されている場合について説明するが、衛星回線やその他の通信回線に接続されていてもよい。
【００７０】
携帯電話装置２としては、ＰＨＳデータ通信装置や携帯電話装置などであり、無線通信回線などの公衆回線網に接続されている。
【００７１】
一般電話装置３としては、有線通信回線などの公衆回線網などに接続されている。
【００７２】
認証装置４は、ユーザ（携帯電話装置２や一般電話装置３）と電波や有線を介して接続するための接続手段（受信手段）としての接続部４１と、接続部４１によって受信され、携帯端末装置７の情報保全要求が行われたときに連絡者が所有者（ユーザ）であるか否かを識別する個人認証処理を行う認証手段としての認証部４２と、認証部４２による個人認証が一致した場合に、管理装置５に対して情報保全処理の命令を出力する命令出力手段としての命令出力部４３とを有している。
【００７３】
管理装置５は、認証装置４の命令出力部４３と電波や有線を介して接続されて情報保全処理命令を受ける接続手段（命令受信手段）としての接続部５１と、携帯端末装置７との間で予め定められた保全モード情報と保全処理情報とを記憶する記憶手段としての記憶部５２と、接続部５１による情報保全処理命令の受信時に、携帯端末装置７を情報保全処理するために、記憶部５２内の保全モード情報と保全処理情報を用いて独自の遠隔操作パケットを生成する遠隔操作情報生成手段としてのパケット生成部５３と、この生成した遠隔操作パケットを中継基地局６に電波や有線を介して送信する遠隔操作情報送信手段としてのパケット送信部５４と、一つ以上の中継基地局６および携帯端末装置７との電波通信状況を管理・把握する管理手段としての管理部５５と、管理部５５による電波通信状況に基づいて携帯端末装置７側が遠隔操作パケットを受信したか否かを確認する確認手段としての確認部５６とを有している。
【００７４】
中継基地局６は、管理装置５からの遠隔操作パケットを受信する受信手段としての受信部６１と、この受信した遠隔操作パケットを携帯端末装置７に送信する送信手段としての送信部６２とを有している。
【００７５】
携帯端末装置７は、例えばＰＨＳ（Ｐｅｒｓｏｎａｌ　Ｈａｎｄｙ　Ｐｈｏｎｅ　Ｓｙｓｔｅｍ）データ通信装置や携帯電話装置であって、中継基地局６から例えば電波を伝送媒体とし送信されてくる遠隔操作パケットを受信する受信手段としての受信部７１と、こ

の受信部７１で受信した遠隔操作パケットを識別する識別手段としての識別部７２と、この識別部７２による識別結果に基づいて携帯端末装置７の所有者が被害を被ることを排除するために遠隔操作パケットに応じた所定の情報保全処理を行う情報保全処理手段としての保全部７３と、管理装置５との間で予め定められ、識別部７２で用いる識別用の保全モード情報と保全処理情報を記憶したり、電波や有線を介して受信部７１により受信した遠隔操作パケットを記憶したり、保全部７３による情報保全処理が実行された後の状態を記憶したりする記憶手段としての記憶部７４とを有している。

【００７６】

識別部７２は、記憶部７４に記憶した保全モード情報が遠隔操作パケットの保全モード情報と一致するかどうかを識別する保全モード情報識別手段と、記憶部７４に記憶した保全処理情報が遠隔操作パケットの保全処理情報と一致するかどうかを識別する保全処理情報識別手段とを有している。

【００７７】

上記構成により、以下に、本実施形態の携帯端末装置の情報保全システム１を用いた携帯端末装置の情報保全方法について説明する。

【００７８】

本実施形態の携帯端末装置の情報保全システム１では、携帯端末装置７に対する情報保全要求が行われたときに、認証装置４によって個人認証処理を行い、この個人認証処理で認証が一致した場合に、管理装置５のパケット生成部５３によって遠隔操作パケットを生成して、これをパケット送信部５４から中継基地局６を介して携帯端末装置７に送信し、携帯端末装置７に所定の情報保全処理を行わせて、携帯端末装置７の所有者が被害を被るのを排除する。これを図２を用いて説明する。

【００７９】

図２は、本実施形態の携帯端末装置の情報保全システム１による携帯端末装置７の情報保全方法の各処理手順を説明するためのフローチャートである。

【００８０】

図２に示すように、まず、ステップＳ１で市内や市外の例えば一般電話装置３から公衆回線網を介して、または例えば携帯電話装置２から無線通信回線を介して通信業者のサービスサーバに情報保全要求が行われると、ステップＳ２で認証装置４によってその連絡者が携帯端末装置７の所有者であるか否かの個人認証処理が行われる。

【００８１】

次に、ステップＳ２で認証部４２による認証が本人情報と一致しない場合（不一致）には、ステップＳ３でその連絡者からの情報保全要求が拒否されて本実施形態の情報保全処理が終了する。一方、ステップＳ２で認証部４２による認証の一致が確認された場合（本人情報と一致）には、ステップＳ４で管理装置５のパケット生成部５３によって、予め携帯端末装置７との間で予め定められた保全モード情報と所有者によって選択された保全処理情報とから、遠隔操作パケットが生成される。

【００８２】

ステップＳ５で管理装置５のパケット送信部５４によって電波などを介して中継基地局６に対して、生成された遠隔操作パケットが送信される。

【００８３】

ステップＳ６では、その送信された遠隔操作パケットが中継基地局６で受信されると、中継基地局６から携帯端末装置７に対してその受信遠隔操作パケットが送信される。

【００８４】

ステップＳ７で携帯端末装置７の受信部７１によってその遠隔操作パケットが受信されると、ステップＳ８で識別部７２によってその受信した遠隔操作パケットが予め記憶された所定の保全モード情報と一致するか否かが判別される。

【００８５】

識別部７２による識別結果の一致が確認された場合（ＹＥＳ）にのみ、ステップＳ９で保全部７３によって情報保全システム１が立ち上げられる。さらに、ステップＳ１０で保

全処理情報が識別され、ステップＳ１１で携帯端末装置７の所有者が被害を被ることを排除するために保全処理情報に応じた所定の情報保全処理が実施される。

【００８６】

次に、本実施形態の携帯端末装置の情報保全システム１における各構成部の処理についてそれぞれ詳細に説明する。

【００８７】

まず、図１の認証装置４による処理動作（図２のステップＳ１～Ｓ３）について図３を用いて詳細に説明する。

【００８８】

図３は、図１の携帯端末装置の情報保全システム１における認証装置４の処理動作（図２のステップＳ１～Ｓ３）について、その処理手順をさらに詳細に説明するためのフローチャートである。

【００８９】

図３に示すように、所有者が携帯端末装置７を紛失した場合、その所有者は、前述したように、まず、ステップＳ１で携帯電話装置２または一般電話装置３からサービスサーバの認証装置４に電話をかけて連絡して、紛失した携帯端末装置７の情報保全要求を行う。

【００９０】

次に、この情報保全要求を受けてステップＳ２で個人認証処理を行う。これについて詳細に説明する。まず、ステップＳ２１で携帯端末装置７に対する情報保全要求が認証装置４の接続部４１で受信されると、ステップＳ２２で認証装置４の認証部４２によって、例えば生年月日や住所または暗証番号を自動的に音声質問するなど（例えば定型の音声質問に対して電話器のキー番号で暗証番号などを回答するなどの方法）、何らかの方法を用いて、連絡者が紛失した携帯端末装置７の所有者（本人）であるか否かを、本人情報として記憶されているデータと比較することにより識別する個人認証処理が行われる。

【００９１】

ステップＳ２２でこの個人認証が一致しない場合（ＮＯ）、ステップＳ３で連絡者の情報保全要求が拒否されて情報保全処理自体が終了する。一方、ステップＳ２２で個人認証の一致が確認された場合（ＹＥＳ）には、ステップＳ２３で認証装置４の命令出力部４３によって、連絡者が要求する情報保全項目として、例えば記憶データ出力禁止や記憶データ転送、記憶データ消去などが、管理装置５に対して情報保全処理の命令として出力される。

【００９２】

図３のフローチャートからも分かるように、認証装置４を介することによって、

（１）認証装置４への連絡手段は一般的であるため、所有者が携帯端末装置７の盗難や紛失時をも把握していると考えられ、早急に携帯端末装置７の情報保全要求を行うことが可能であり、

（２）個人認証を行うことによって、所有者以外の第三者による情報保全処理の実施を防ぐことが可能であるという効果がある。

【００９３】

次に、図１の管理装置５および中継基地局６による処理動作（図２のステップＳ４～Ｓ６）について図４を用いて詳細に説明する。

【００９４】

図４は、図１の携帯端末装置の情報保全システム１における管理装置５および中継基地局６の処理動作（図２のステップＳ４～Ｓ６）について、その処理手順をさらに詳細に説明するためのフローチャートである。

【００９５】

ステップＳ４１で、認証装置４からの情報保全処理命令が管理装置５の接続部（命令受信部）５１で受信されると、ステップＳ４２でパケット生成部５２によって、この情報保全処理命令に応じた遠隔操作パケットが生成される。

【００９６】

この遠隔操作パケットは、例えば図５に示すように、ヘッダ部に予め携帯端末装置７との間で定められた情報保全処理を行うためのヘッダ情報である保全モード情報が含まれ、その後に続くデータ部には保全処理情報が含まれている。ここで、この保全処理情報とは、認証装置４に対して所有者が選択した情報保全項目を示しており、情報保全項目として例えば図６Ａおよび図６Ｂにて後述するが、例えば「警告発生」、「メッセージ表示」および「発信機能禁止」などがある。このヘッダ部とデータ部とが一つの遠隔操作パケットとして生成される。これらの保全モード情報と保全処理情報とは、記憶部５３に記憶されている。なお、この図５の遠隔操作パケットの構成は一例であり、同様の機能を実現できるものであれば、他の実現方法であってもよい。

【００９７】

この遠隔操作パケットの生成後、前述したようにステップＳ５１で管理装置５のパケット送信部５４によって、その遠隔操作パケットが中継基地局６に送信される。さらに、ステップＳ６で中継基地局６の送信部６２から、紛失した携帯端末装置７に対して、無線通信によりその遠隔操作パケットが送信される。

【００９８】

管理装置５では、管理部５５によって、盗難・紛失した携帯端末装置７と中継基地局６との電波状況（通信状況）を管理・把握することができるため、ステップＳ５２において、その遠隔操作パケットが携帯端末装置７に受信されたか否かが確認され、受信が確認されるまで何回でもパケット送信部５４により再送することが可能である。なお、この再送方法は一例であり、同様の目的を果たすことができるものであれば、他の実現方法であってもよい。

【００９９】

この図４のフローチャートからも分かるように、管理装置５によって独自に生成される遠隔操作パケットを利用することによって、

（１）従来のように一般の携帯端末装置利用者からのパケットによる誤った情報保全処理の実施の危険性がなく、

（２）遠隔操作パケットを携帯端末装置７が確実に受信するまで何回でもリトライが可能となり、

（３）所有者自身が何回も遠隔操作パケットを再送する手間や時間が必要ないという効果が得られる。

【０１００】

次に、紛失した携帯端末装置７による情報保全処理（図２のステップＳ７～Ｓ１１）について図６Ａおよび図６Ｂを用いて詳細に説明する。

【０１０１】

図６Ａおよび図６Ｂは、図１の携帯端末装置の情報保全システム１における携帯端末装置７の各処理動作（図２のステップＳ７～Ｓ１１）について、その処理手順をさらに詳細に説明するためのフローチャートである。

【０１０２】

図６Ａに示すように、前述したように、ステップＳ７で管理装置５から中継基地局６を介して所有者の携帯端末装置７に送信された遠隔操作パケットが、紛失した携帯端末装置７の受信部７１で受信されると、ステップＳ８で識別部７２によって、その遠隔操作パケットの保全モード情報が携帯端末装置７内の記憶部７４に記憶されている保全モード情報と一致するか否かが識別される。

【０１０３】

ステップＳ８でその識別結果が不一致である場合（ＮＯ）には、保全モード情報の識別待ちとなって、情報保全処理システム１の情報保全処理が終了して、通常のモードに戻る。一方、ステップＳ８でその識別結果が所定の保全モード情報と確認（一致）された場合（ＹＥＳ）には、ステップＳ９で情報保全処理システム１が立ち上げられ、保全部７３による情報保全処理機能が起動される。

【０１０４】

ステップＳ１０で識別部７２によって、遠隔操作パケットの保全処理情報が、携帯端末装置７内の記憶部７４に記憶されている保全処理情報と一致するか否かが識別される。

【０１０５】

ステップＳ１０でその識別結果が不一致である場合（ＮＯ）には、保全処理情報の識別待ちとなって、情報保全処理システム１が終了して、通常のモードに戻る。一方、ステップＳ１０でその識別結果が所定の保全処理情報と確認（一致）された場合（ＹＥＳ）には、ステップＳ１１１で保全処理情報の情報保全内容が解析される。

【０１０６】

この保全処理情報は、各情報保全処理に対してコードが予め定められており（保全モード情報や保全処理情報はコードの一致により確認される）、例えば「警告発生」、「メッセージ表示」、「発信機能禁止」、「所有者連絡発信」、「記憶データ消去」、「データ出力禁止」、「通信回線番号消滅」、「記憶データ転送」、「使用者の識別」および「電源オフ」など、所定のコードにより分岐されて、個々の情報保全処理ルーチンに移行する。

【０１０７】

例えばステップＳ１１２で保全処理情報の内容が「警告発生」コードと一致すると識別された場合（ＹＥＳ）にはステップＳ１１３の処理に進み、保全部７３によって、視覚または聴覚に対してアラームを発生する「警告発生」の情報保全処理が実行される。また、ステップＳ１１２で不一致の場合（ＮＯ）には、次の処理コードに対するステップＳ１１４の処理に進み、次々と一致するコードを検索しながら各処理を進める。その他の保全処理情報の内容についても同様であり、コードが一致した場合（ＹＥＳ）に該当する情報保全処理が実行される。予め定められた処理コードに該当しない場合には、情報保全処理システム１による情報保全処理が終了するか、または固定の情報保全処理が行われる。

【０１０８】

ステップＳ１１４では、保全処理情報の内容が「メッセージ表示」コードと一致するか否か識別され、これと一致した場合（ＹＥＳ）には、ステップＳ１１５の処理に移行して、所有者が予め入力して記憶部７４に記憶させた連絡先および／またはメッセージを表示する「メッセージ表示」の情報保全処理が実行される。また、ステップＳ１１４で不一致の場合（ＮＯ）には、次の処理コードに対するステップＳ１１６の処理に移行する。

【０１０９】

ステップＳ１１６では、保全処理情報の内容が「発信機能禁止」コードと一致するか否かが識別され、これと一致した場合（ＹＥＳ）には、ステップＳ１１７の処理に移行して、所有者が予め入力した機能を停止する「発信機能禁止」の情報保全処理が実行される。ステップＳ１１６で不一致の場合（ＮＯ）には、次の処理コードに対するステップＳ１１８の処理に移行する。

【０１１０】

次に、図６Ｂに示すように、ステップＳ１１８では、保全処理情報の内容が「所有者連絡発信」コードと一致するか否かが識別され、これと一致した場合（ＹＥＳ）にステップＳ１１９の処理に移行して、所有者が予め入力して記憶部７４に記憶させた連絡先に発信する「所有者連絡発信」の情報保全処理が実行される。また、ステップＳ１１８で不一致の場合（ＮＯ）には、次の処理コードに対するステップＳ１２０の処理に移行する。

【０１１１】

ステップＳ１２０では、保全処理情報の内容が「記憶データ消去」コードと一致するか否かが識別され、これと一致した場合（ＹＥＳ）には、ステップＳ１２１の処理に移行して、記録部７４のデータを消去して、記録部７４のデータを他人に見られたり使用されないようにする「記憶データ消去」の情報保全処理が実行される。また、ステップＳ１２０で不一致の場合（ＮＯ）には、次の処理コードに対するステップＳ１２２の処理に移行する。

【０１１２】

ステップＳ１２２では、保全処理情報の内容が「データ出力禁止」コードと一致するか

否かが識別され、これと一致した場合（ＹＥＳ）には、ステップＳ１２３の処理に移行して、記録部７４からのデータ出力を禁止する「データ出力禁止」の情報保全処理が実行される。また、ステップＳ１２２で不一致の場合（ＮＯ）には、次の処理コードに対するステップＳ１２４の処理に移行する。

【０１１３】

ステップＳ１２４では、保全処理情報の内容が「通信回線番号消滅」コードと一致するか否かが識別され、これと一致した場合（ＹＥＳ）には、ステップＳ１２５の処理に移行して、通信回線番号を消滅させて他人がその通信回線番号を使用できないようにする「通信回線番号消滅」の情報保全処理が実行される。また、ステップＳ１２４で不一致の場合（ＮＯ）には、次の処理コードに対するステップＳ１２６の処理に移行する。

【０１１４】

ステップＳ１２６では、保全処理情報の内容が「記憶データ転送」コードと一致するか否かが識別され、これと一致した場合（ＹＥＳ）には、ステップＳ１２７の処理に移行して、記録部７４内のデータをデータ移動して記録部７４内にそのデータを残さないようにデータ回収する「記憶データ転送」の情報保全処理が実行される。また、ステップＳ１２６で不一致の場合（ＮＯ）には、次の処理コードに対するステップＳ１２８の処理に移行する。

【０１１５】

ステップＳ１２８では、保全処理情報の内容が「使用者の識別」コードと一致するか否かが識別され、これと一致した場合（ＹＥＳ）には、ステップＳ１２９の処理に移行して、識別部７２を用いて使用者を識別し、所有者以外の他人が携帯端末装置７の使用ができないようにする「使用者の識別」の保全処理が実行される。ステップＳ６２で不一致の場合には次の処理コードに対するステップＳ１３０の処理に移行する。

【０１１６】

ステップＳ１３０では、保全処理情報の内容が「電源オフ」コードと一致するか否かが識別され、これと一致した場合（ＹＥＳ）には、ステップＳ１３１の処理に移行して、携帯端末装置７を使用できないようにする「電源オフ」の情報保全処理が実行される。また、ステップＳ１３０で不一致の場合（ＮＯ）には、次の処理コードに対するステップＳ１３２の処理に移行する。

【０１１７】

ステップＳ１３２でどのコードにも該当しないコードであれば（ＹＥＳ）、情報保全処理システム１の情報保全処理を終了する。また、ステップＳ１３２でどのコードにも該当しないコードでない場合（ＮＯ）には、ステップＳ１３３の処理に移行して固定の情報保全処理として例えば「電源オフ」の情報保全処理が実行されて、情報保全処理システム１の情報保全処理を終了する。

【０１１８】

以上のように、紛失した携帯端末装置７では、この携帯端末装置７と管理装置５との間で予め定められた保全モード情報と保全処理情報とが記憶部７４に記憶され、例えば電波を伝送媒体として遠隔操作パケットが送信されて携帯端末装置７で受信されると、その識別結果の保全処理情報が記憶部７４に記憶される。記憶手段に予め記憶された保全モード情報および保全処理情報と遠隔操作パケットの保全モード情報および保全処理情報との一致が確認されて、図６に示すような情報保全処理の少なくともいずれかがが実行される。さらに、その情報保全処理後の状態が、記憶部７４に設けられた不揮発性メモリなどのような不揮発性記憶手段に記憶されている。

【０１１９】

このようにすることで、

（１）紛失した携帯端末装置７の情報保全処理が実現可能となり、

（２）ケースバイケースで最適な情報保全処理を選択して適用することが可能となり、

（３）情報保全処理実行後に携帯端末装置７の電源を再投入しても情報保全状態を継続することが可能となるという効果を有する。

【０１２０】
なお、紛失した携帯端末装置７の保全部７３による情報保全処理について、上記図６Ａおよび図６Ｂに示した事例は一例であり、保全部７３は、携帯端末装置７が盗難または紛失したときに、通信手段を介して送信されてきた遠隔操作パケットの識別結果により、携帯端末装置７の所有者が被害を被ることを排除するために、
（１）盗難または紛失した携帯端末装置７の本来の機能を停止させて、使用者以外の他人が使用できないようにする「電源オフ」の情報保全処理（図６Ｂのステップ Ｓ１３１，Ｓ１３３）、
（２）盗難または紛失した携帯端末装置７を所有者以外の他人が使用すると、視覚または聴覚に対してアラームを発生する「警告発生」の情報保全処理（図６Ａのステップ Ｓ１１３）、
（３）盗難または紛失した携帯端末装置７を所有者以外の他人が使用すると、所有者が予め入力して記憶部７４に記憶させた連絡先および／またはメッセージを表示し、携帯端末装置７の拾得者が使用することを防止したり所有者に返還を呼びかけて携帯端末装置７を回収する「メッセージ表示」の情報保全処理、
（４）盗難または紛失した携帯端末装置７の本来の機能を停止させて、所有者が予め入力して記憶部７４に記憶させた連絡先にのみ交信する「所有者連絡発信」の情報保全処理、
（５）盗難または紛失した携帯端末装置７の本来の機能のうち、所有者が予め入力した機能を停止する「発信機能禁止」の情報保全処理、
（６）盗難または紛失した携帯端末装置７の記録部７４からのデータ出力を禁止する「データ出力禁止」の情報保全処理、
（７）盗難または紛失した携帯端末装置７の記録部７４からデータを消去させ、その記録部７４内のデータを他人に見られたり使用されないようにする「記憶データ消去」の情報保全処理、
（８）盗難または紛失した携帯端末装置７の通信回線番号を消滅させて、他人がその通信回線番号を使用できないようにする「通信回線番号消滅」の情報保全処理、
（９）盗難または紛失した携帯端末装置７の記録部７４からデータを他の所定の電子装置に転送（データ移動）させて記録部７４内にそのデータを残さないようにし、その記憶データを回収する「記憶データ転送」の情報保全処理、
（１０）識別部７２を用いて使用者を識別し、所有者以外の他人が携帯端末装置７の使用ができないようにする「使用者識別」の情報保全処理のうち、一つまたは二つ以上の処理を行うことができる。

【０１２１】
また、保全部７３は、携帯端末装置７の盗難または紛失が発生したときに、通信手段を介して送信されてきた遠隔操作パケットの識別部７２による識別結果により、携帯端末装置７の所有者への送信相手または相手情報が被害を被ることを排除するために、
（１）携帯端末装置７に送信した相手に、所有者が受信できない事情にあるという所定の情報を送信する情報保全処理、
（２）携帯端末装置７に送信した相手からの受信情報を受信する機能を停止する情報保全処理、
（３）携帯端末装置７に送信した相手に、通話中または使用中のデータを送信する情報保全処理、
（４）携帯端末装置７に送信した相手に、例えば通信手続き動作においてアクセス信号を送信しないことなどによって、送信情報を送信する機能を停止する情報保全処理、
（５）携帯端末装置７に送信した相手に、所有者が予め入力して記憶部７４に記憶させた紛失メッセージを送信する情報保全処理、
（６）携帯端末装置７に送信した相手に対して、携帯端末装置７の情報保全システムの他人による使用を防止する情報保全処理のうち、一つまたは二つ以上の処理を行うことができる。

【０１２２】
ここで、図１の携帯端末装置７の具体的構成例について図７を用いて説明する。
【０１２３】
図７は、図１の携帯端末装置７の詳細な構成例を示すブロック図である。
【０１２４】
図７において、電子情報装置としての携帯端末装置７は、前述したが、遠隔操作パケットを受信する受信部７１と、この受信部７１で受信された遠隔操作パケット内の保全モード情報を識別する保全モード情報識別部７２ａと、この遠隔操作パケット内の保全処理情報を識別する保全処理情報識別部７２ｂと、この保全処理情報識別部７２ｂで識別された情報に対応する情報保全処理を選択する保全処理選択部７３ａと、この保全処理選択部７３ａにて選択された情報保全処理に応じた信号を発生する保全処理信号発生部７３ｂと、この保全処理信号発生部７３ｂからの信号を受けてこの信号に応じた情報保全処理を実行する情報保全処理実行部７３ｃと、予め管理装置５との間で定められた保全モード情報および保全処理情報を記憶している第１記憶手段としての第１記憶部７４ａと、管理装置５から中継基地局６を介して所有者の携帯端末装置７へ送信された遠隔操作パケットを記憶する第２記憶手段としての第２記憶部７４ｂと、保全部７３ｃによる保全処理実行後の状態を記憶する不揮発性の第３記憶手段としての第３記憶部７４ｃと、制御プログラムおよびそのデータを記憶するＲＯＭ７４ｄと、ワークメモリとして作用するＲＡＭ７４ｅと、ＲＡＭ７４ｅ内に読み出された制御プログラムに基づいて、各部に接続されて各部の機能を実行する制御部（ＣＰＵ；中央得演算処理装置）７ａとを有している。
【０１２５】
なお、図１の識別部７２は、保全モード情報識別部７２ａ、保全処理情報識別部７２ｂおよび制御部７ａを有する。また、保全部７３は、保全処理選択部７３ａ、保全処理信号発生部７３ｂ、情報保全処理実行部７３ｃおよび制御部７ａを有する。さらに、可読記録媒体としての記憶部７４は、第１記憶部７４ａ、第２記憶部７４ｂ、第３記憶部７４ｃ、ＲＯＭ７４ｄおよびＲＡＭ７４ｅを有する。ＲＯＭ７４ｄおよびＲＡＭ７４ｅは、制御プログラムが記録されたコンピュータ読み取り可能な可読記録媒体である。この可読記録媒体としては、ハードディスク、光ディスク、磁気ディスク、ＩＣメモリなどの各種メモリ装置で構成されていてもよい。
【０１２６】
上記構成により、以下に、携帯端末装置７の各処理動作について説明する。
【０１２７】
まず、管理装置５から中継基地局６を介して所有者の携帯端末装置７へ送信された遠隔操作パケット（遠隔操作情報）が受信部７１によって受信されると、制御部７ａによってその遠隔操作パケットがデコードされて第２記憶部７４ｂに送られる。第２記憶部７４ｂでは、送られてきたデータが記憶される。
【０１２８】
次に、保全モード情報識別部７２ａによって、第１記憶部７４ａに記憶されている保全モード情報と第２記憶部７４ｂに記憶されている保全モード情報とが互いに一致するか否かが識別される。保全モード情報が一致した場合には、保全処理情報識別部７２ｂによって、第１記憶部７４ａに記憶されている保全処理情報が第２記憶部７４ｂに記憶されている保全処理情報であるか否かが識別される。
【０１２９】
同じ保全処理情報で一致した場合には、保全処理選択部７３ａによって第２記憶部７４ｂに記憶されている保全処理情報に応じた情報保全処理が選択される。情報保全処理の選択後、情報保全処理信号発生部７３ｂによって選択された情報保全処理に応じた信号が発生され、情報保全処理実行部７４ｃに信号が送られる。
【０１３０】
情報保全処理実行部７４ｃでは、信号が受信されると、受信された信号に応じた情報保全処理が実行される。情報保全処理の実行後、第３記憶部７４ｃによって、電源再投入時

に元の状態に継続して戻るようにするべく情報保全処理後の現在の状態が記憶される。

【０１３１】

以上の回路ブロック構成によって、盗難や紛失した携帯端末装置の所有者情報や相手情報を保全することが可能となる。なお、この回路ブロック構成はその一例であり、同様の機能を実現することができるものであれば、他の実現方法であってもよい。

【０１３２】

図８は、図７の携帯端末装置における識別部および保全部による処理データの流れを説明するためのフロー図である。

【０１３３】

図８に示すように、まず、管理装置５から中継基地局６を介して所有者の携帯端末装置７へ送信された遠隔操作パケットが受信されると、受信完了信号が保全モード識別部７２ａに届く。この保全モード識別部７２ａでは、その送信された遠隔操作パケットの保全モード情報と第１記憶部７４ａ内の保全モード情報とが一致しているかどうかが識別される。これらの各保全モード情報が互いに一致している場合には、保全モード情報識別部７２ａによって一致データが次の保全処理情報識別部７２ｂに送られる。

【０１３４】

次に、保全処理情報識別部７２ｂでは、保全モード識別部７２ａからの一致データを受け取ると、その遠隔操作パケット内の保全処理情報と第１記憶部７４ａの保全処理情報とが一致しているかどうかが識別される。これらの各保全処理情報が一致していると識別されると、保全処理情報識別部７２ｂから、保全処理情報データが保全処理選択部７３ａに送られる。

【０１３５】

保全処理選択部７３ａでは、その保全処理情報データから、該当する情報保全処理が選択されて、その選択された選択データが情報保全処理信号発生部７３ｂに送られる。

【０１３６】

情報保全処理信号発生部７３ｂでは、その選択データを元に情報保全処理信号が発生されて、情報保全処理実行部７３ｃに送られる。

【０１３７】

情報保全処理実行部７３ｃでは、受け取った情報保全処理信号に応じた情報保全処理が実行される。この情報保全処理の実行後、情報保全処理実行部７３ｃから、情報保全処理終了信号が保全モード識別部７２ａに送られる。

【０１３８】

なお、このデータフローは一例であって、同様の処理を実現することができるものであれば、他の方法であってもよい。

【０１３９】

以上により、本実施形態によれば、携帯端末装置の情報保全システム１は、携帯端末装置７との間に電波通信手段を介して接続されている一つ以上の中継基地局６と、所有者であるか否かを識別するための個人認証処理を行う認証装置４と、携帯端末装置７を情報保全処理するための遠隔操作パケットを生成する管理装置５とを備え、携帯端末装置７に対する情報保全要求が行われたときに、認証装置４によって個人認証処理を行い、この個人認証が一致した場合に、管理装置５によって遠隔操作パケットを生成して中継基地局６から携帯端末装置７に送信し、遠隔操作パケットを携帯端末装置７で受信してこれに応じた所定の情報保全処理を行わせる。これによって、携帯端末装置７の盗難や紛失に対して、少ない手間と時間で確実に、所有者が被害を被ることを排除できる携帯端末装置の情報保全システム１を得ることができる。

【０１４０】

なお、上記実施形態では、管理装置５は、中継基地局６および携帯端末装置７との通信状況を管理する管理部５５と、この管理部５５が管理する通信状況に基づいて、携帯端末装置７が遠隔操作パケットを受信したか否かを確認する確認部５６とを有し、この確認部５６が携帯端末装置７への遠隔操作パケットの受信を確認できない場合に、携帯端末装置

７への遠隔操作パケットの再送信をパケット送信部５４に実行（リトライ）させるように構成したが、これに限らず、管理装置５は、携帯端末装置７と中継基地局６との通信状況を管理する管理部５５を有し、中継基地局６は、携帯端末装置７が遠隔操作パケットを受信したか否かを確認する確認部を更に有し、この確認部が携帯端末装置７への遠隔操作パケットの受信を確認できない場合にこれを中継基地局６から管理装置５の管理部５５に送信して、この管理部５５が携帯端末装置７への遠隔操作パケットの再送信をパケット送信部５４に実行（リトライ）させるように構成してもよい。

また、本発明の制御プログラム（携帯端末装置７の情報保全処理プログラム）は、本発明の携帯端末装置７の情報保全方法をコンピュータによって読み取って実行させるための各処理手順が記述されており、コンピュータ読み取り可能な可読記録媒体に格納させることができる。これにより、本発明の携帯端末装置７の情報保全方法をコンピュータによって制御して、これを実行させることができる。また、この可読記録媒体と、可読記録媒体から制御プログラムを読み取って実行可能なコンピュータを、電子情報装置として、本発明の携帯端末装置７と、認証装置４および管理装置５を持つサービスサーバとにそれぞれ搭載することによって、本発明の携帯端末装置７の情報保全システムを構成することができる。

【０１４１】

以上のように、本発明の好ましい実施形態を用いて本発明を例示してきたが、本発明は、この実施形態に限定して解釈されるべきものではない。本発明は、特許請求の範囲によってのみその範囲が解釈されるべきであることが理解される。当業者は、本発明の具体的な好ましい実施形態の記載から、本発明の記載および技術常識に基づいて等価な範囲を実施することができることが理解される。本明細書において引用した特許、特許出願および文献は、その内容自体が具体的に本明細書に記載されているのと同様にその内容が本明細書に対する参考として援用されるべきであることが理解される。

【産業上の利用可能性】

【０１４２】

本発明は、ＰＨＳ（Ｐｅｒｓｏｎａｌ　Ｈａｎｄｙ　Ｐｈｏｎｅ　Ｓｙｓｔｅｍ）、携帯電話装置などを含む通信手段を有するデータ処理端末装置である携帯端末装置に、これが盗難や紛失したときに、その携帯端末装置内の情報に関するセキュリティを高める情報保全処理機能を持たせた携帯端末装置の情報保全システム、携帯端末装置の情報保全方法、この方法をコンピュータに実行させるための各処理手順が記述された制御プログラム、その制御プログラムが記述されたコンピュータ読み取り可能な可読記録媒体およびこの可読記録媒体から制御プログラムを読み取ってこの方法を実行可能なコンピュータを備えた電子情報装置の分野において、携帯端末装置の盗難や紛失に対して、その所有者が遠隔操作することにより、携帯端末装置の所有者が被害を被ることを排除する所定の情報保全処理が実施され、携帯端末装置の所有者の財産または情報に関わるセキュリティを高めることができる。

【図面の簡単な説明】

【０１４３】

【図１】本発明の実施形態に係る携帯端末装置の情報保全システムの要部構成例を示すブロック図である。

【図２】図１の携帯端末装置の情報保全システムによる携帯端末装置の情報保全方法の各処理手順を説明するためのフローチャートである。

【図３】図２の携帯端末装置の情報保全システムにおける認証装置の処理について、その各処理手順を説明するためのフローチャートである。

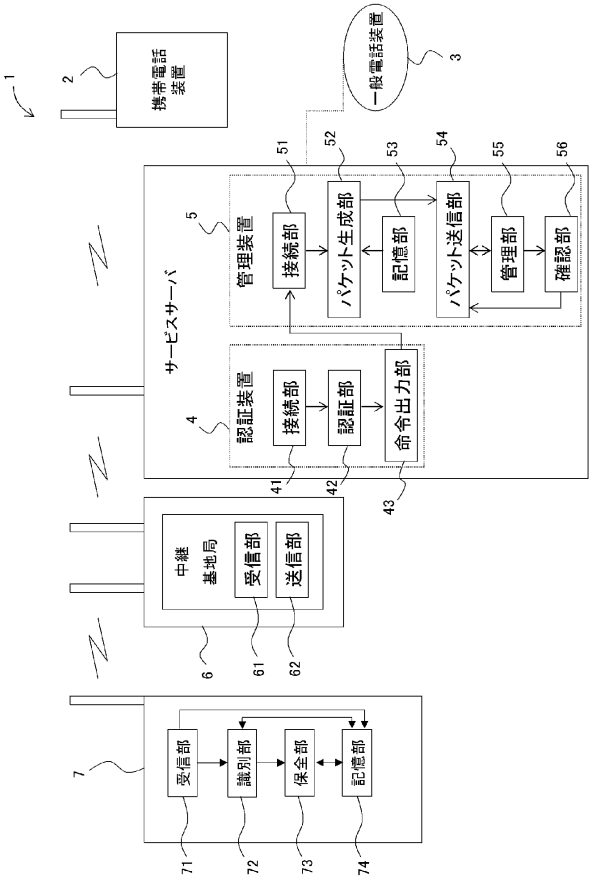
【図４】図２の携帯端末装置の情報保全システムにおける管理装置および中継基地局の各処理について、その各処理手順を説明するためのフローチャートである。

【図５】図４の遠隔操作パケットの構成例を示す図である。

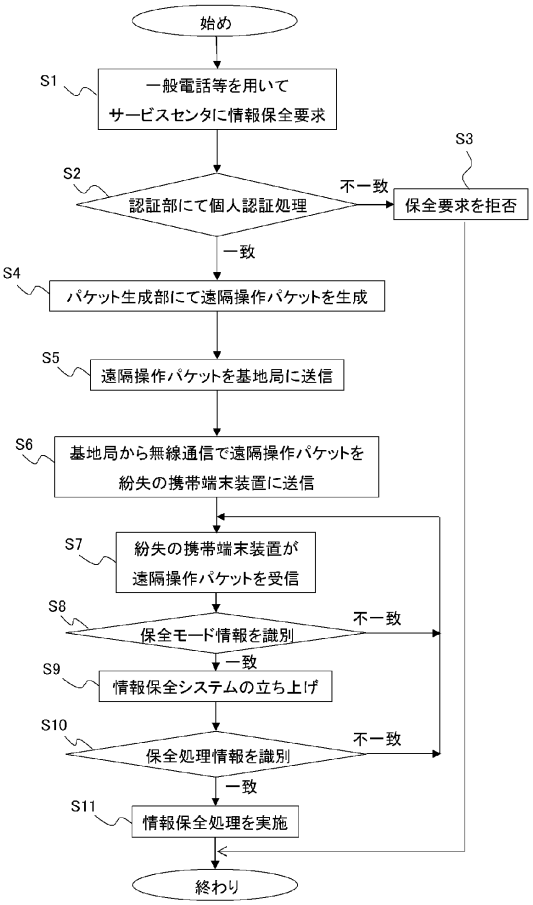
【図６Ａ】図２の携帯端末装置の情報保全システムにおける携帯端末装置の処理について、その各処理手順（その１）を説明するためのフローチャートである。

【図６Ｂ】図２の携帯端末装置の情報保全システムにおける携帯端末装置の処理について、その各処理手順（その２）を説明するためのフローチャートである。
【図７】図１の携帯端末装置の詳細構成例を示すブロック図である。
【図８】図１の携帯端末装置における識別部と保全部による処理データの流れを説明するためのフロー図である。
【図９】非特許文献１の遠隔ロック機能の各処理手順を説明するためのフローチャートである。
【図１０】特許文献１の携帯端末装置の情報保全システムによる各処理手順を説明するためのフローチャートである。
【符号の説明】
【０１４４】
１　携帯端末装置の情報保全システム
２　携帯電話装置
３　一般電話装置
４　認証装置
４１　接続部
４２　認証部
４３　命令出力部
５　管理装置
５１　接続部（命令受信部）
５２ パケット生成部
５３ 記憶部（可読記録媒体）
５４ パケット送信部
５５ 管理部
５６　確認部
６　中継基地局
７　携帯端末装置
７１ 受信部
７２ 識別部
７２ａ 保全モード情報識別部
７２ｂ　保全処理情報識別部
７３　保全部
７３ａ 保全処理選択部
７３ｂ 保全処理信号発生部
７３ｃ 保全処理実行部
７４　記憶部
７４ａ　第１記憶部（可読記録媒体）
７４ｂ　第２記憶部（可読記録媒体）
７４ｃ　第３記憶部（可読記録媒体）
７４ｄ　ＲＯＭ（記憶部；可読記録媒体）
７４ｅ　ＲＡＭ（記憶部；可読記録媒体）
７５　制御部（ＣＰＵ）

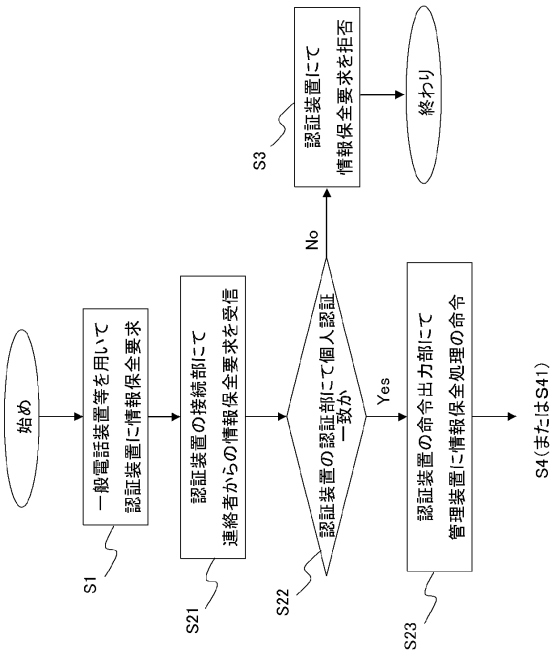
【図１】


1
2
携帯電話装置
一般電話装置
3
サービスサーバ
5
管理装置
51
接続部
52
パケット生成部
53
記憶部
54
パケット送信部
55
管理部
56
確認部
4
認証装置
接続部
認証部
命令出力部
41
42
43
中継基地局
6
受信部
送信部
61
62
7
受信部
識別部
保全部
記憶部
71
72
73
74

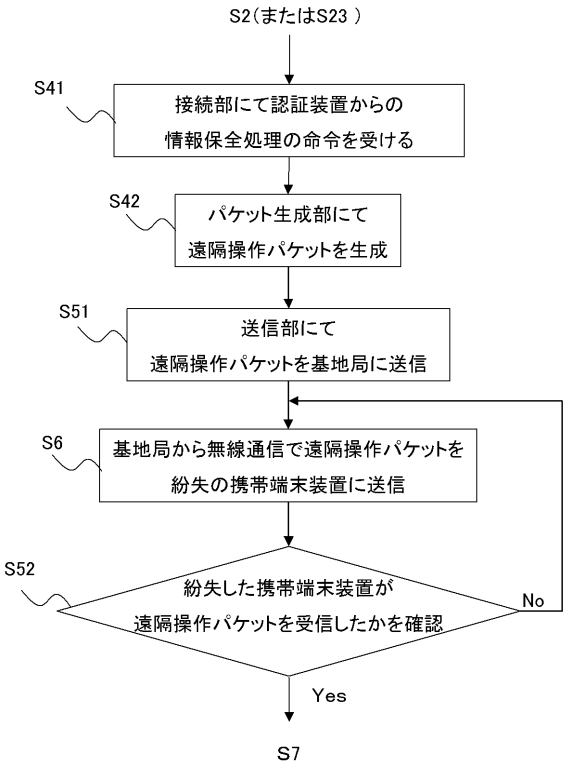
【図２】


始め
S1
一般電話等を用いてサービスセンタに情報保全要求
S2
認証部にて個人認証処理
不一致
S3
保全要求を拒否
一致
S4
パケット生成部にて遠隔操作パケットを生成
S5
遠隔操作パケットを基地局に送信
S6
基地局から無線通信で遠隔操作パケットを紛失の携帯端末装置に送信
S7
紛失の携帯端末装置が遠隔操作パケットを受信
S8
保全モード情報を識別
不一致
一致
S9
情報保全システムの立ち上げ
S10
保全処理情報を識別
不一致
一致
S11
情報保全処理を実施
終わり

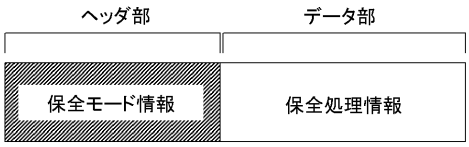
【図３】


始め
一般電話装置等を用いて認証装置に情報保全要求
S1
認証装置の接続部にて連絡者からの情報保全要求を受信
S21
認証装置の認証部にて個人認証一致か
S22
No
Yes
S3
認証装置にて情報保全要求を拒否
終わり
認証装置の命令出力部にて管理装置に情報保全処理の命令
S23
S4(またはS41)

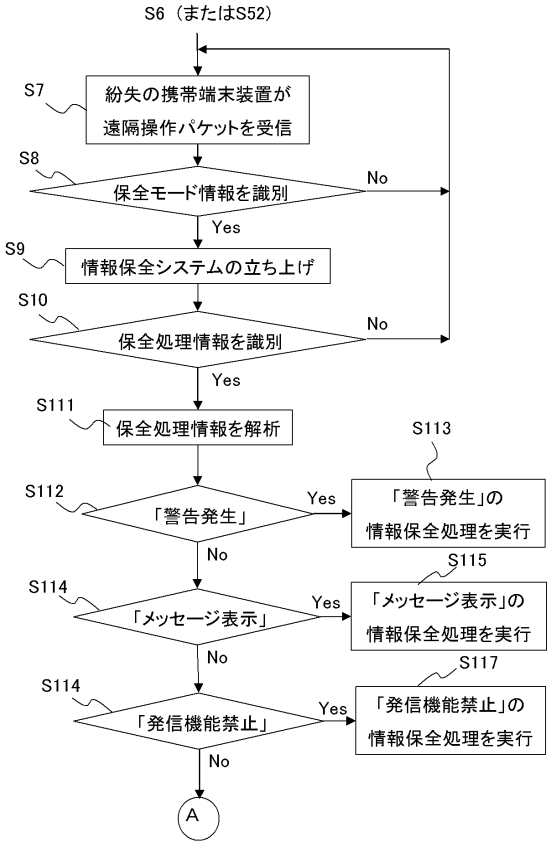
【図４】


S2(またはS23)
S41
接続部にて認証装置からの情報保全処理の命令を受ける
S42
パケット生成部にて遠隔操作パケットを生成
S51
送信部にて遠隔操作パケットを基地局に送信
S6
基地局から無線通信で遠隔操作パケットを紛失の携帯端末装置に送信
S52
紛失した携帯端末装置が遠隔操作パケットを受信したかを確認
No
Yes
S7

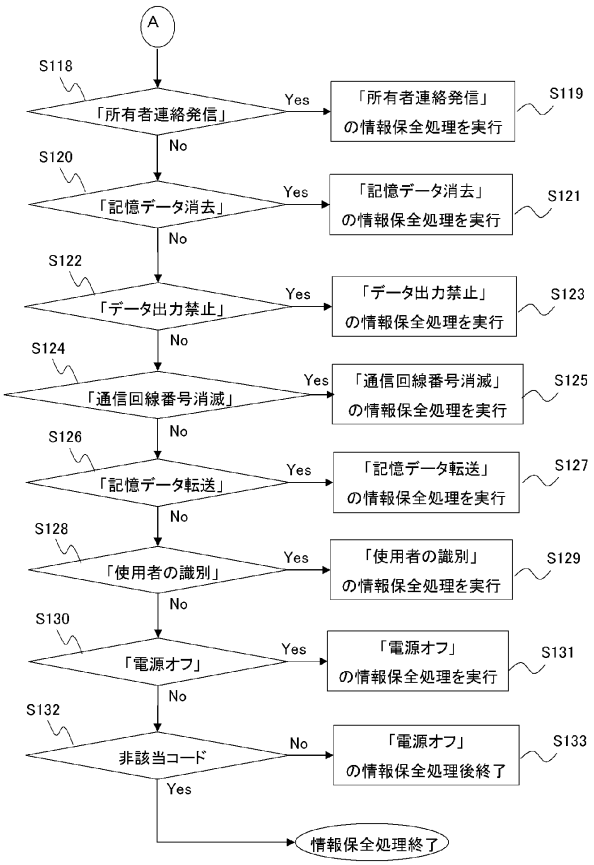
【図５】


ヘッダ部
データ部
保全モード情報
保全処理情報

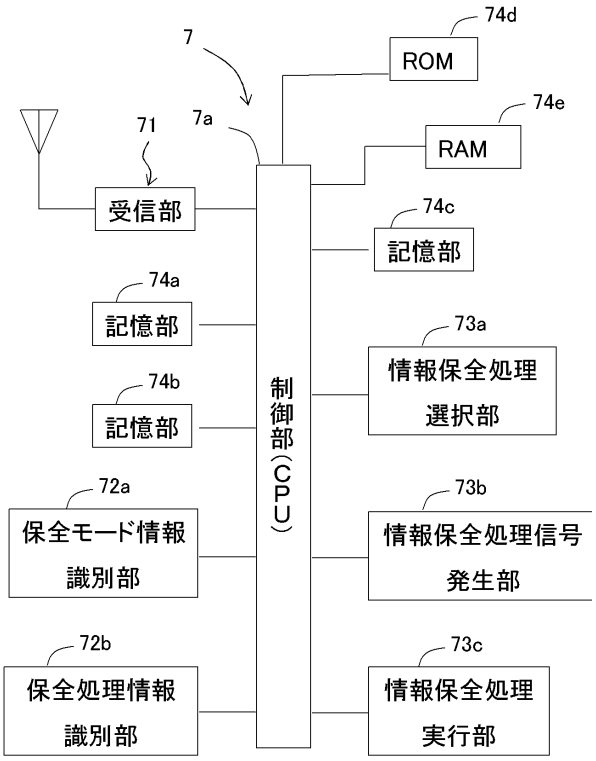
【図６Ａ】


S6（またはS52）
S7
紛失の携帯端末装置が
遠隔操作パケットを受信
S8
保全モード情報を識別
No
Yes
S9
情報保全システムの立ち上げ
S10
保全処理情報を識別
No
Yes
S111
保全処理情報を解析
S113
S112
「警告発生」
Yes
「警告発生」の
情報保全処理を実行
No
S115
S114
「メッセージ表示」
Yes
「メッセージ表示」の
情報保全処理を実行
No
S117
S114
「発信機能禁止」
Yes
「発信機能禁止」の
情報保全処理を実行
No
A

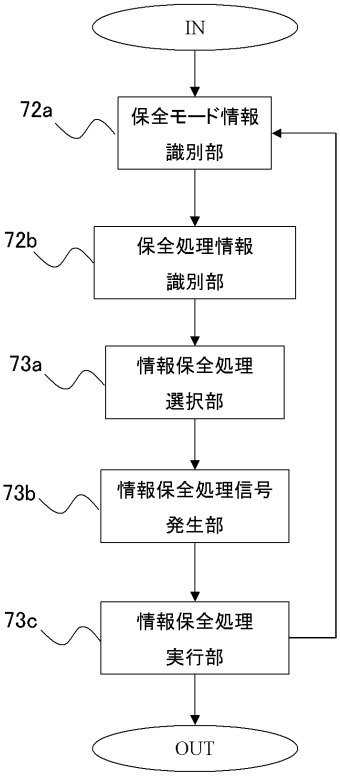
【図６Ｂ】


A
S118
「所有者連絡発信」
Yes
「所有者連絡発信」
の情報保全処理を実行
S119
No
S120
「記憶データ消去」
Yes
「記憶データ消去」
の情報保全処理を実行
S121
No
S122
「データ出力禁止」
Yes
「データ出力禁止」
の情報保全処理を実行
S123
No
S124
「通信回線番号消滅」
Yes
「通信回線番号消滅」
の情報保全処理を実行
S125
No
S126
「記憶データ転送」
Yes
「記憶データ転送」
の情報保全処理を実行
S127
No
S128
「使用者の識別」
Yes
「使用者の識別」
の情報保全処理を実行
S129
No
S130
「電源オフ」
Yes
「電源オフ」
の情報保全処理を実行
S131
No
S132
非該当コード
No
「電源オフ」
の情報保全処理後終了
S133
Yes
情報保全処理終了

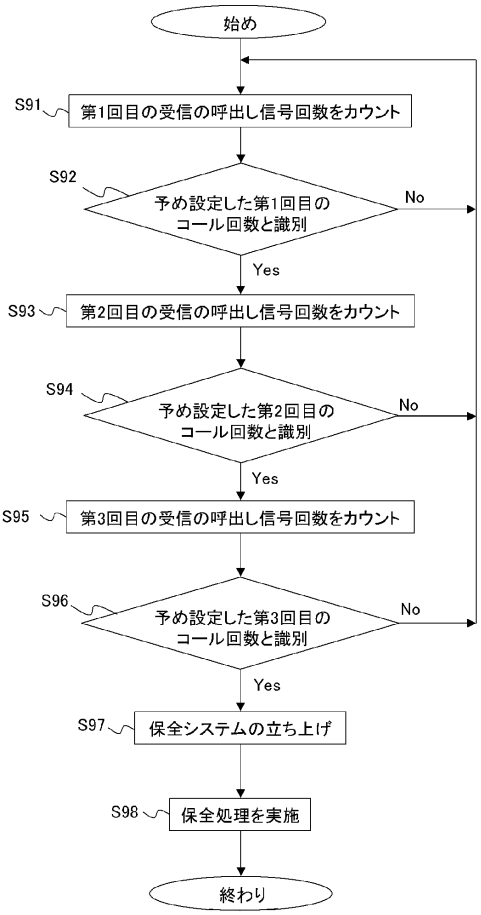
【図７】


7
74d
ROM
74e
RAM
71
7a
受信部
74c
記憶部
74a
記憶部
73a
情報保全処理
選択部
74b
記憶部
制御部（CPU）
72a
保全モード情報
識別部
73b
情報保全処理信号
発生部
72b
保全処理情報
識別部
73c
情報保全処理
実行部

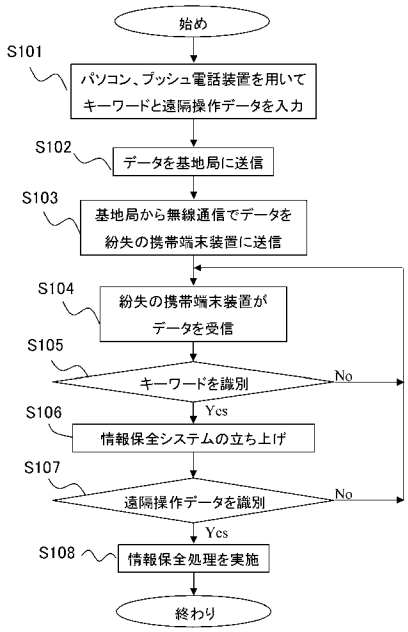
【図８】


IN
72a
保全モード情報
識別部
72b
保全処理情報
識別部
73a
情報保全処理
選択部
73b
情報保全処理信号
発生部
73c
情報保全処理
実行部
OUT

【図９】


始め
S91
第1回目の受信の呼出し信号回数をカウント
S92
予め設定した第1回目の
コール回数と識別
No
Yes
S93
第2回目の受信の呼出し信号回数をカウント
S94
予め設定した第2回目の
コール回数と識別
No
Yes
S95
第3回目の受信の呼出し信号回数をカウント
S96
予め設定した第3回目の
コール回数と識別
No
Yes
S97
保全システムの立ち上げ
S98
保全処理を実施
終わり

【図１０】


始め
S101
パソコン、プッシュ電話装置を用いて
キーワードと遠隔操作データを入力
S102
データを基地局に送信
S103
基地局から無線通信でデータを
紛失の携帯端末装置に送信
S104
紛失の携帯端末装置が
データを受信
S105
キーワードを識別
No
Yes
S106
情報保全システムの立ち上げ
S107
遠隔操作データを識別
No
Yes
S108
情報保全処理を実施
終わり

フロントページの続き

審査官　戸次　一夫

(56)参考文献　特開２００１－３５９１５７（ＪＰ，Ａ）
特開平０８－２５１６６０（ＪＰ，Ａ）
特開２００５－０３９５８７（ＪＰ，Ａ）
特開平１０－１７７５２５（ＪＰ，Ａ）
特開２００３－２２９８１２（ＪＰ，Ａ）
特開２００４－２９５１６２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　７／２４－　７／２６、
Ｈ０４Ｍ　１／００、　１／２４－　１／２５３、
１／５８－　１／６２、　１／６６－　３／００、
３／１６－　３／２０、　３／３８－　３／５８、
７／００－　７／１６、１１／００－１１／１０、９９／００、
Ｈ０４Ｑ　７／００－　７／３８