(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2006-148552
(P2006-148552A)
(43)公開日　平成18年6月8日(2006.6.8)

(51)Int.Cl.			F I			テーマコード（参考）
H04Q	7/38	(2006.01)	H04B	7/26	109S	5K027
H04M	1/67	(2006.01)	H04M	1/67		5K067

審査請求 未請求　請求項の数 23　ＯＬ　（全 34 頁）

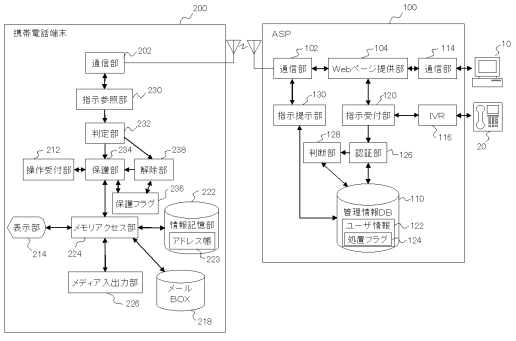
(21)出願番号　特願2004-336038 (P2004-336038)
(22)出願日　平成16年11月19日 (2004.11.19)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(71)出願人　000232254
日本電気通信システム株式会社
東京都港区三田１丁目４番２８号
(74)代理人　100110928
弁理士　速水　進治
(72)発明者　源田　隆博
東京都港区三田一丁目４番２８号　日本電気通信システム株式会社内
(72)発明者　高津戸　史朗
東京都港区三田一丁目４番２８号　日本電気通信システム株式会社内

最終頁に続く

(54)【発明の名称】セキュリティシステム

(57)【要約】
【課題】　携帯通信端末の盗難、紛失時に携帯通信端末内の情報を保護可能なセキュリティシステムを提供する。
【解決手段】　情報を記憶する情報記憶部２２２を備えた携帯電話端末２００の情報を保護するＡＳＰ１００を備えたセキュリティシステムであって、ＡＳＰ１００は、携帯電話端末２００のユーザからの情報を保護する保護指示および情報の保護を解除する解除指示を受け付ける指示受付部１２０と、携帯電話端末２００のユーザを認証する認証部１２６と、認証部１２６がユーザを認証したとき、保護指示および解除指示を携帯通信端末に通知する指示提示部１３０と、を含み、携帯電話端末２００は、ＡＳＰ１００から保護指示および解除指示を受信する指示参照部２３０と、保護指示に従って、情報を保護する処置を行う保護部２３４と、解除指示に従って、情報の保護を解除する処置を行う解除部２３８と、を含む。
【選択図】　図３



【特許請求の範囲】
【請求項１】
情報を記憶する情報記憶部を備えた携帯通信端末の前記情報を保護する制御装置を備えたセキュリティシステムであって、
前記制御装置は、
前記携帯通信端末のユーザからの前記情報を保護する保護指示および前記情報の保護を解除する解除指示を受け付けるユーザ指示受付部と、
前記携帯通信端末の前記ユーザを認証する認証部と、
前記認証部が前記ユーザを認証したとき、前記保護指示および前記解除指示を前記携帯通信端末に通知する指示通知部と、
前記携帯通信端末の前記情報を保護するセキュリティプログラムを提供する提供部と、
を含み、
前記携帯通信端末は、
前記制御装置から前記保護指示および前記解除指示を受信する受信部と、
前記受信部が受信した前記保護指示に従って、前記情報を保護する処置を行う情報保護部と、
前記受信部が受信した前記解除指示に従って、前記情報の保護を解除する処置を行う保護解除部と、
前記セキュリティプログラムを前記制御装置からインターネットを介してダウンロードするダウンロード部と、
前記ダウンロード部がダウンロードした前記セキュリティプログラムを記憶するプログラム記憶部と、
前記携帯通信端末が起動したとき、前記セキュリティプログラムを実行する実行部と、
を含むことを特徴とするセキュリティシステム。
【請求項２】
請求項１に記載のセキュリティシステムにおいて、
前記制御装置は、前記携帯通信端末の識別情報と、前記情報を保護する処置を施しているか否かを示す処置フラグとを対応付けて記憶するフラグ記憶部を備え、
前記制御装置の前記指示通知部は、前記携帯通信端末に前記保護指示および前記解除指示を通知したとき、前記フラグ記憶部の当該携帯通信端末の前記識別情報の前記処置フラグをセットおよびリセットし、
前記携帯通信端末は、
前記制御装置の前記フラグ記憶部に前記インターネットを経由してアクセスし、自識別情報に対応する前記処置フラグを参照する参照部と、
前記処置フラグがセットされているとき、前記情報保護部に前記情報を保護する処置をさせ、前記処置フラグがリセットされているとき、前記保護解除部に前記情報の保護を解除する処置をさせる制御部と、を含むことを特徴とするセキュリティシステム。
【請求項３】
請求項２に記載のセキュリティシステムにおいて、
前記制御装置は、
前記携帯通信端末から前記セキュリティプログラムの使用の申し込みを受け付ける申込受付部と、
前記申込受付部が申し込みを受け付けたとき、前記携帯通信端末の前記識別情報およびパスワードの登録を受け付ける登録受付部と、
前記登録受付部が受け付けた前記携帯通信端末の前記識別情報毎に前記パスワードを対応付けて記憶する登録端末記憶部と、
を含み、
前記制御装置において、
前記ユーザ指示受付部は、前記保護指示および前記解除指示とともに、当該携帯通信端末の前記識別情報および前記パスワードを受け付け、

前記認証部は、前記登録端末記憶部にアクセスして、前記ユーザ指示受付部が受け付けた前記携帯通信端末の前記識別情報および前記パスワードが一致するか否かを判定し、一致する場合、当該携帯通信端末の前記ユーザを認証することを特徴とするセキュリティシステム。

【請求項４】

請求項１乃至３いずれかにセキュリティシステムにおいて、

前記制御装置は、前記携帯通信端末に保護指示メールを送信する送信部を含み、

前記携帯通信端末は、前記保護指示メールを受信する受信部を含み、

前記携帯通信端末の前記情報保護部は、前記受信部が前記保護指示メールを受信したとき、前記情報を保護する処置を開始するとともに、その後、前記参照部が定期的に前記処置フラグを参照することを特徴とするセキュリティシステム。

【請求項５】

請求項１乃至４いずれかにセキュリティシステムにおいて、

前記制御装置は、前記携帯通信端末に解除指示メールを送信する送信部を含み、

前記携帯通信端末は、前記解除指示メールを受信する受信部を含み、

前記携帯通信端末の前記保護解除部は、前記受信部が前記解除指示メールを受信したとき、前記情報の保護を解除する処置を行うことを特徴とするセキュリティシステム。

【請求項６】

請求項４または５に記載のセキュリティシステムにおいて、

前記携帯通信端末は、

前記受信部が受信した前記保護指示メールまたは前記解除指示メールのタイトルまたは本文を参照し、当該メールが前記保護指示または前記解除指示を通知するメールか否かを判定する判定部を含み、

前記情報保護部は、前記判定部が前記保護指示を通知するメールであると判定したとき、前記情報を保護する処置を行い、

前記保護解除部は、前記判定部が前記解除指示を通知するメールであると判定したとき、前記情報の保護を解除する処置を行うことを特徴とするセキュリティシステム。

【請求項７】

請求項１乃至６いずれかに記載のセキュリティシステムにおいて、

前記ユーザ指示受付部は、前記携帯通信端末の前記ユーザからの電話を、公衆回線網を経由して受信し、音声自動応答する音声自動応答装置を含み、

前記音声自動応答装置が、前記携帯通信端末の前記保護指示および前記解除指示とともに、当該携帯通信端末の前記識別情報および前記パスワードを受け付けることを特徴とするセキュリティシステム。

【請求項８】

請求項１乃至７いずれかに記載のセキュリティシステムにおいて、

前記ユーザ指示部受付部は、前記携帯通信端末の前記ユーザから前記インターネットを経由して、前記携帯通信端末の前記保護指示および前記解除指示とともに、当該携帯通信端末の前記識別情報および前記パスワードの入力を受け付けることを特徴とするセキュリティシステム。

【請求項９】

請求項１乃至８いずれかに記載のセキュリティシステムにおいて、

前記携帯通信端末は、前記情報を操作する操作部を有し、

前記携帯通信端末の前記情報保護部は、当該携帯通信端末の前記操作部の操作を禁止する操作禁止部を有し、

前記携帯通信端末の前記保護解除部は、当該携帯通信端末の前記操作部の操作禁止を解除する禁止解除部を有することを特徴とするセキュリティシステム。

【請求項１０】

請求項１乃至９いずれかに記載のセキュリティシステムにおいて、

前記携帯通信端末は、当該携帯通信端末の電源を自動的に切断する切断部を有し、

前記携帯通信端末の前記情報保護部は、当該携帯通信端末の前記切断部に前記電源を自動的に切断させることを特徴とするセキュリティシステム。

【請求項１１】

請求項９または１０に記載のセキュリティシステムにおいて、

前記携帯電話端末の前記情報保護部が前記情報を保護する複数の保護処置を行い、

前記制御装置の前記ユーザ指示受付部は、前記複数の保護処置の中からいずれの保護処置を行うかを受け付け、

前記携帯電話端末の前記情報保護部は、前記制御部の前記ユーザ指示受付部が受け付けた前記保護処置を行うことを特徴とするセキュリティシステム。

【請求項１２】

請求項１乃至１１いずれかに記載のセキュリティシステムにおいて、

前記制御装置は、前記ユーザ指示受付部が前記保護指示を受け付けたとき、前記携帯通信端末に所定の電話番号から電話をかける発信部を含み、

前記携帯通信端末は、

前記所定の電話番号を記憶する番号記憶部と、

前記電話を着信する着信部と、

前記着信部で着信した電話番号を取得する取得部と、

前記番号記憶部にアクセスし、前記取得部で取得した電話番号が前記所定の電話番号であるか否かを判定する判定部と、を含み、

前記判定部が前記取得部で取得した電話番号が前記所定の電話番号であると判定したとき、前記携帯通信端末の前記情報保護部は前記情報を保護する処置を開始することを特徴とするセキュリティシステム。

【請求項１３】

請求項１乃至１２いずれかに記載のセキュリティシステムにおいて、

前記制御装置は、前記ユーザ指示受付部が前記解除指示を受け付けたとき、前記携帯通信端末に所定の電話番号から電話をかける発信部を含み、

前記携帯通信端末は、

前記所定の電話番号を記憶する番号記憶部と、

前記電話を着信する着信部と、

前記着信部で着信した電話番号を取得する取得部と、

前記取得部で取得した電話番号が前記所定の電話番号であるか否かを判定する判定部と、を含み、

前記判定部が前記取得部で取得した電話番号が前記所定の電話番号であると判定したとき、前記携帯通信端末の前記保護解除部は前記保護する処置を解除することを特徴とするセキュリティシステム。

【請求項１４】

請求項１乃至１３いずれかに記載のセキュリティシステムにおいて、

前記携帯通信端末は、Ｗｅｂブラウザ部を有し、

前記携帯通信端末は、前記Ｗｅｂブラウザ部経由で前記制御装置にアクセスすることを特徴とするセキュリティシステム。

【請求項１５】

請求項１乃至１４いずれかに記載のセキュリティシステムにおいて、

前記制御装置は、

前記ユーザ指示部が前記保護指示および前記解除指示を受け付けた日時の処置履歴を記録する保護処置履歴記録部と、

前記保護処置履歴記録部に記録された前記処置履歴をユーザの要求に応じて提示する履歴提示部と、を含むことを特徴とするセキュリティシステム。

【請求項１６】

請求項１５に記載のセキュリティシステムにおいて、

前記制御装置は、

前記保護処置履歴記録部に記録された前記処置履歴に基づいて、前記ユーザ毎に利用料金を課金する課金部を含むことを特徴とするセキュリティシステム。

【請求項１７】

請求項１乃至１６いずれかに記載のセキュリティシステムにおいて、

前記制御装置は、

前記登録受付部が受け付けた前記ユーザの前記セキュリティシステムの前記使用の申し込みの日時および前記使用を解約した日時の契約履歴を記録する契約履歴記録部と、

前記契約履歴記録部に記録された前記契約履歴に基づいて、前記ユーザ毎に利用料金を課金する課金部と、を含むことを特徴とするセキュリティシステム。

【請求項１８】

情報を記憶する情報記憶部を備えた携帯通信端末の前記情報を保護するセキュリティプログラムであって、前記携帯通信端末に、

前記携帯通信端末のユーザからの前記情報を保護する保護指示および前記情報の保護を解除する解除指示を通知する制御装置と通信する手順と、

前記通信する手順で前記制御装置から前記保護指示を受け付ける手順と、

前記通信する手順で前記制御装置から前記解除指示を受け付ける手順と、

前記保護指示に従って、前記情報を保護する処置を行う手順と、

前記解除指示に従って、前記情報の保護を解除する処置を行う手順と、

を実行させるためのプログラム。

【請求項１９】

請求項１８に記載のセキュリティプログラムにおいて、

前記制御装置は、前記携帯通信端末の識別情報と、前記情報を保護する処置を施しているか否かを示す処置フラグとを対応付けて記憶するフラグ記憶部を備え、

前記セキュリティプログラムは、前記携帯通信端末に、

前記制御装置の前記フラグ記憶部にアクセスし、自身の前記識別情報の前記処置フラグを参照する手順と、

前記処置フラグがセットされているとき、前記情報を保護する処置を行う手順と、

前記処置フラグがリセットされているとき、前記情報の保護を解除する処置を行う手順と、を実行させるためのセキュリティプログラム。

【請求項２０】

請求項１８または１９に記載のセキュリティプログラムにおいて、

前記制御装置は、前記携帯通信端末に保護指示メールを送信する送信部を含み、

前記セキュリティプログラムは、前記携帯通信端末に、

前記保護指示メールを受信する手順と、

前記受信する手順において前記保護指示メールを受信したとき、前記情報を保護する処置を開始する手順と、

前記開始する手順の後、定期的に前記処置フラグを参照する手順と、を実行させるためのセキュリティプログラム。

【請求項２１】

請求項１８乃至２０いずれかに記載のセキュリティプログラムにおいて、

前記制御装置は、前記携帯通信端末に解除指示メールを送信する送信部を含み、

前記セキュリティプログラムは、前記携帯通信端末に、

前記解除指示メールを受信する手順と、

前記受信する手順において前記解除指示メールを受信したとき、前記情報の保護を解除する処置を行う手順と、を実行させるためのセキュリティプログラム。

【請求項２２】

請求項１８乃至２１いずれかに記載のセキュリティプログラムにおいて、

前記制御装置は、前記保護指示を受け付ける手順で前記保護指示を受け付けたとき、前記携帯通信端末に所定の電話番号から電話をかける発信部を含み、

前記携帯電話端末は、前記所定の電話番号を記憶する番号記憶部を含み、

前記セキュリティプログラムは、前記携帯通信端末に、
前記電話を着信する手順と、
前記着信する手順で着信した電話番号を取得する手順と、
前記番号記憶部にアクセスし、前記取得する手順で取得した電話番号が前記所定の電話番号であるか否かを判定する手順と、
前記判定する手順で、前記取得する手順で取得した電話番号が前記所定の電話番号であると判定したとき、前記携帯通信端末の前記情報保護部は前記情報を保護する処置を開始する手順と、を実行させるためのセキュリティプログラム。

【請求項２３】

請求項１８乃至２２いずれかに記載のセキュリティプログラムにおいて、
前記制御装置は、前記ユーザ指示受付部が前記解除指示を受け付けたとき、前記携帯通信端末に所定の電話番号から電話をかける発信部を含み、
前記携帯通信端末は、前記所定の電話番号を記憶する番号記憶部を含み、
前記セキュリティプログラムは、前記携帯通信端末に、
前記電話を着信する手順と、
前記着信する手順で着信した電話番号を取得する手順と、
前記取得する手順で取得した電話番号が前記所定の電話番号であるか否かを判定する手順と
前記判定する手順で、前記取得する手順で取得した電話番号が前記所定の電話番号であると判定したとき、前記携帯通信端末の前記保護解除部は前記保護する処置を解除する手順と、を実行させるためのセキュリティプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、セキュリティシステムに関し、特に、携帯通信端末において盗難、紛失時のこの携帯通信端末内の情報保護に対するセキュリティシステムに関する。

【背景技術】

【０００２】

従来の携帯通信端末のセキュリティシステムとしては、例えば特許文献１に記載されたものがある。同文献に記載された携帯電話端末のセキュリティシステムは、パスワードを用いたものであり、ユーザが保護したいデータにパスワードをかけ、そのパスワードを入力した時のみデータにアクセスできるようにする。これにより、パスワードを決定した本来のユーザのみがデータにアクセスでき、端末を不当に入手したものはデータにアクセスできなくなる。

【特許文献１】特開平７－１９３８６５号公報

【発明の開示】

【発明が解決しようとする課題】

【０００３】

しかしながら、上記文献記載の従来技術は、以下の点で改善の余地を有していた。

【０００４】

第一に、パスワードはパスワードを設定したユーザが覚えていなければ使えないため、そのユーザに関係したものや、短く覚えやすいものであることが多い。このため、正当なユーザでない者がこの端末を入手したときに、試行錯誤することでパスワードを突き止めてしまう可能性がある。

【０００５】

第二に、そもそもユーザがパスワードを設定しなかった場合には、全くその効力を発揮しない。

【０００６】

本発明は上記事情に鑑みてなされたものであり、その目的とするところは、携帯通信端末の盗難、紛失時に携帯通信端末内の情報を保護可能なセキュリティシステムを提供する

ことにある。
【課題を解決するための手段】
【０００７】
本発明によれば、情報を記憶する情報記憶部を備えた携帯通信端末の前記情報を保護する制御装置を備えたセキュリティシステムであって、前記制御装置は、前記携帯通信端末のユーザからの前記情報を保護する保護指示および前記情報の保護を解除する解除指示を受け付けるユーザ指示受付部と、前記携帯通信端末の前記ユーザを認証する認証部と、前記認証部が前記ユーザを認証したとき、前記保護指示および前記解除指示を前記携帯通信端末に通知する指示通知部と、前記携帯通信端末の前記情報を保護するセキュリティプログラムを提供する提供部と、を含み、前記携帯通信端末は、前記制御装置から前記保護指示および前記解除指示を受信する受信部と、前記受信部が受信した前記保護指示に従って、前記情報を保護する処置を行う情報保護部と、前記受信部が受信した前記解除指示に従って、前記情報の保護を解除する処置を行う保護解除部と、前記セキュリティプログラムを前記制御装置からインターネットを介してダウンロードするダウンロード部と、前記ダウンロード部がダウンロードした前記セキュリティプログラムを記憶するプログラム記憶部と、前記携帯通信端末が起動したとき、前記セキュリティプログラムを実行する実行部と、を含むことを特徴とするセキュリティシステムが提供される。
【０００８】
ここで、携帯通信端末とは、たとえば、携帯電話、ＰＤＡ、ページャ、ノート型パソコンなど、無線通信が可能で持ち運びできる各種情報端末を含む。また、ユーザ指示受付部は、携帯通信端末のユーザからの盗難紛失届けおよび解除届けなどを電話およびパソコンなどの端末から受け付ける。ユーザから盗難紛失届けが出された場合、携帯通信端末の情報を保護する処置を行う保護指示を受け付ける。一方、ユーザの手元に携帯通信端末が戻り、ユーザから解除届けが出された場合、携帯通信端末の情報の保護を解除する処置を行う解除指示を受け付ける。
【０００９】
また、制御装置は、携帯通信端末とインターネットまたは無線または有線の電話回線を経由して通信することにより、保護指示および解除指示を通知することができる。また、提供部は、所謂ＡＳＰ（Application Service Provider）であり、携帯通信端末は、ＡＳＰからセキュリティプログラムをダウンロードして実行する。これにより、ＡＳＰとセキュリティプログラムとの連携によって、遠隔で携帯電話端末の情報保護処置を施すことができる。
【００１０】
この発明によれば、紛失または盗難時に携帯通信端末の情報を保護することが可能となる。
【００１１】
上記セキュリティシステムにおいて、前記制御装置は、前記携帯通信端末の識別情報と、前記情報を保護する処置を施しているか否かを示す処置フラグとを対応付けて記憶するフラグ記憶部を備えることができ、前記制御装置の前記指示通知部は、前記携帯通信端末に前記保護指示および前記解除指示を通知したとき、前記フラグ記憶部の当該携帯通信端末の前記識別情報の前記処置フラグをセットおよびリセットすることができ、前記携帯通信端末は、前記制御装置の前記フラグ記憶部に前記インターネットを経由してアクセスし、自識別情報に対応する前記処置フラグを参照する参照部と、前記処置フラグがセットされているとき、前記情報保護部に前記情報を保護する処置をさせ、前記処置フラグがリセットされているとき、前記保護解除部に前記情報の保護を解除する処置をさせる制御部と、を含むことができる。
【００１２】
ここで、携帯通信端末の識別情報とは、たとえば、携帯電話の電話番号などである。ＡＳＰが携帯通信端末のユーザからセキュリティプログラムの使用の申し込みを受け付け、ユーザ登録を行う。

【００１３】
この構成によれば、携帯電話端末からＡＳＰに定期的にアクセスして情報保護処置を行うか否かを判断できるので、遠隔で携帯電話端末の情報を保護することが可能となる。
【００１４】
上記セキュリティシステムにおいて、前記制御装置は、前記携帯通信端末から前記セキュリティプログラムの使用の申し込みを受け付ける申込受付部と、前記申込受付部が申し込みを受け付けたとき、前記携帯通信端末の前記識別情報およびパスワードの登録を受け付ける登録受付部と、前記登録受付部が受け付けた前記携帯通信端末の前記識別情報毎に前記パスワードを対応付けて記憶する登録端末記憶部と、を含むことができ、前記制御装置において、前記ユーザ指示受付部は、前記保護指示および前記解除指示とともに、当該携帯通信端末の前記識別情報および前記パスワードを受け付けることができ、前記認証部は、前記登録端末記憶部にアクセスして、前記ユーザ指示受付部が受け付けた前記携帯通信端末の前記識別情報および前記パスワードが一致するか否かを判定し、一致する場合、当該携帯通信端末の前記ユーザを認証することができる。
【００１５】
この構成によれば、ユーザ認証を行うことにより、不正に携帯電話端末の情報保護処置および保護処置の解除が行われることを防ぐことができ、本システムのセキュリティが向上する。
【００１６】
上記セキュリティシステムにおいて、前記制御装置は、前記携帯通信端末に保護指示メールを送信する送信部を含むことができ、前記携帯通信端末は、前記保護指示メールを受信する受信部を含むことができ、前記携帯通信端末の前記情報保護部は、前記受信部が前記保護指示メールを受信したとき、前記情報を保護する処置を開始するとともに、その後、前記参照部が定期的に前記処置フラグを参照することができる。
【００１７】
この構成によれば、通常の使用時に定期的に処置フラグをチェックするためにＡＳＰにアクセスする必要がなくなるので、ＡＳＰとの通信回数を大幅に低減することができる。また、携帯通信端末が保護指示メールを受信することにより、迅速に情報を保護する処置を開始できるので、システムの信頼性が増す。
【００１８】
上記セキュリティシステムにおいて、前記制御装置は、前記携帯通信端末に解除指示メールを送信する送信部を含むことができ、前記携帯通信端末は、前記解除指示メールを受信する受信部を含むことができ、前記携帯通信端末の前記保護解除部は、前記受信部が前記解除指示メールを受信したとき、前記情報の保護を解除する処置を行うことができる。
【００１９】
この構成によれば、保護処置後、定期的に処置フラグをチェックするためにＡＳＰにアクセスする必要がなく、ＡＳＰとの通信回数を大幅に低減することができる。
【００２０】
上記セキュリティシステムにおいて、前記携帯通信端末は、前記受信部が受信した前記保護指示メールまたは前記解除指示メールのタイトルまたは本文を参照し、当該メールが前記保護指示または前記解除指示を通知するメールか否かを判定する判定部を含むことができ、前記情報保護部は、前記判定部が前記保護指示を通知するメールであると判定したとき、前記情報を保護する処置を行い、前記保護解除部は、前記判定部が前記解除指示を通知するメールであると判定したとき、前記情報の保護を解除する処置を行うことができる。
【００２１】
この構成によれば、保護指示または解除指示メールによって携帯電話端末の情報の保護処置および保護解除を行うことができる。
【００２２】
上記セキュリティシステムにおいて、前記ユーザ指示受付部は、前記携帯通信端末の前

記ユーザからの電話を、公衆回線網を経由して受信し、音声自動応答する音声自動応答装置を含むことができ、前記音声自動応答装置が、前記携帯通信端末の前記保護指示および前記解除指示とともに、当該携帯通信端末の前記識別情報および前記パスワードを受け付けることができる。

【００２３】

ここで、音声自動応答装置とは、所謂ＩＶＲ（Ｉｎｔｒａｃｔｉｖｅ Ｖｏｉｃｅ Ｒｅｓｐｏｎｃｅ）であり、音声による自動応答を行うコンピュータシステムである。発信者のダイヤル操作に応じて、予め録音してある音声ガイダンスを発信者に自動的に再生する。あるいは、発信者側の発話を音声認識する音声認識部を有するものでもよく、音声認識された発話内容に応じて、再生を行うこともできる。

【００２４】

この構成によれば、電話回線を介してユーザからの盗難紛失届けや解除届けを受信することが可能となり、インターネットを介しての通信端末などからセキュリティシステムへの接続ができない場合であっても盗難紛失届けを受信することができることとなる。

【００２５】

上記セキュリティシステムにおいて、前記ユーザ指示部受付部は、前記携帯通信端末の前記ユーザから前記インターネットを経由して、前記携帯通信端末の前記保護指示および前記解除指示とともに、当該携帯通信端末の前記識別情報および前記パスワードの入力を受け付けることができる。

【００２６】

この構成によれば、インターネットを経由してユーザからの盗難紛失届けを受信することが可能となり、電話回線による接続ができない場合であっても盗難紛失届けを受信することができることとなる。

【００２７】

上記セキュリティシステムにおいて、前記携帯通信端末は、前記情報を操作する操作部を有し、前記携帯通信端末の前記情報保護部は、当該携帯通信端末の前記操作部の操作を禁止する操作禁止部を有することができ、前記携帯通信端末の前記保護解除部は、当該携帯通信端末の前記操作部の操作禁止を解除する禁止解除部を有することができる。

【００２８】

上記セキュリティシステムにおいて、前記携帯通信端末は、当該携帯通信端末の電源を自動的に切断する切断部を有することができ、前記携帯通信端末の前記情報保護部は、当該携帯通信端末の前記切断部に前記電源を自動的に切断させることができる。

【００２９】

上記セキュリティシステムにおいて、前記携帯電話端末の前記情報保護部が前記情報を保護する複数の保護処置を行い、前記制御装置の前記ユーザ指示受付部は、前記複数の保護処置の中からいずれの保護処置を行うかを受け付け、前記携帯電話端末の前記情報保護部は、前記制御部の前記ユーザ指示受付部が受け付けた前記保護処置を行うことができる。

【００３０】

上記セキュリティシステムにおいて、前記制御装置は、前記ユーザ指示受付部が前記保護指示を受け付けたとき、前記携帯通信端末に所定の電話番号から電話をかける発信部を含むことができ、前記携帯通信端末は、前記所定の電話番号を記憶する番号記憶部と、前記電話を着信する着信部と、前記着信部で着信した電話番号を取得する取得部と、前記番号記憶部にアクセスし、前記取得部で取得した電話番号が前記所定の電話番号であるか否かを判定する判定部と、を含むことができ、前記判定部が前記取得部で取得した電話番号が前記所定の電話番号であると判定したとき、前記携帯通信端末の前記情報保護部は前記情報を保護する処置を開始することができる。

【００３１】

この構成によれば、予め登録されている所定の電話番号からの着信をトリガとして、携帯通信端末の情報を保護する処置を施すことが可能となる。したがって、携帯通信端末が

インターネットに接続できない状況であっても電話が繋がれば情報を保護することが可能となる。

【００３２】

上記セキュリティシステムにおいて、前記制御装置は、前記ユーザ指示受付部が前記解除指示を受け付けたとき、前記携帯通信端末に所定の電話番号から電話をかける発信部を含むことができ、前記携帯通信端末は、前記所定の電話番号を記憶する番号記憶部と、前記電話を着信する着信部と、前記着信部で着信した電話番号を取得する取得部と、前記取得部で取得した電話番号が前記所定の電話番号であるか否かを判定する判定部と、を含むことができ、前記判定部が前記取得部で取得した電話番号が前記所定の電話番号であると判定したとき、前記携帯通信端末の前記保護解除部は前記保護する処置を解除することができる。

【００３３】

この構成によれば、所定の電話番号からの着信をトリガとして、携帯通信端末の情報を保護する処置を解除することが可能となる。したがって、携帯通信端末がインターネットに接続できない状況であっても電話が繋がれば情報の保護を解除することが可能となる。

【００３４】

上記セキュリティシステムにおいて、前記携帯通信端末は、Ｗｅｂブラウザ部を有することができ、前記携帯通信端末は、前記Ｗｅｂブラウザ部経由で前記制御装置にアクセスすることができる。

【００３５】

上記セキュリティシステムにおいて、前記制御装置は、前記ユーザ指示部が前記保護指示および前記解除指示を受け付けた日時の処置履歴を記録する保護処置履歴記録部と、前記保護処置履歴記録部に記録された前記処置履歴をユーザの要求に応じて提示する履歴提示部と、を含むことができる。

【００３６】

この構成によれば、ユーザの要求に応じて、携帯電話端末の情報が保護されていることを示す保護処置履歴を提示することができるので、手元に携帯電話端末がなく不安なユーザを安心させることができる。

【００３７】

上記セキュリティシステムにおいて、前記制御装置は、前記保護処置履歴記録部に記録された前記処置履歴に基づいて、前記ユーザ毎に利用料金を課金する課金部を含むことができる。

【００３８】

この構成によれば、保護処置サービスの利用に応じて利用料金を課金することができる。

【００３９】

上記セキュリティシステムにおいて、前記制御装置は、前記登録受付部が受け付けた前記ユーザの前記セキュリティシステムの前記使用の申し込みの日時および前記使用を解約した日時の契約履歴を記録する契約履歴記録部と、前記契約履歴記録部に記録された前記契約履歴に基づいて、前記ユーザ毎に利用料金を課金する課金部と、を含むことができる。

【００４０】

この構成によれば、契約期間に応じてサービス利用料金を課金することができる。

【００４１】

なお、以上の構成要素の任意の組合せ、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。

【発明の効果】

【００４２】

本発明によれば、携帯通信端末の盗難、紛失時に携帯通信端末内の情報を保護可能なセ

キュリティシステムが提供される。
【発明を実施するための最良の形態】
【００４３】
以下、本発明の実施の形態について、図面を用いて説明する。尚、すべての図面において、同様な構成要素には同様の符号を付し、適宜説明を省略する。
（第一の実施の形態）
図１は、本発明の実施の形態に係るセキュリティシステムの構成を示すブロック図である。なお、セキュリティシステムの各構成要素は、任意のコンピュータのＣＰＵ、メモリ、メモリにロードされた本図の構成要素を実現するプログラム、そのプログラムを格納するハードディスクなどの記憶ユニット、ネットワーク接続用インタフェースを中心にハードウェアとソフトウェアの任意の組合せによって実現される。そして、その実現方法、装置にはいろいろな変形例があることは、当業者には理解されるところである。以下説明する各図は、ハードウェア単位の構成ではなく、機能単位のブロックを示している。また、以下の図において、本発明の本質に関わらない部分の構成については省略してある。
【００４４】
本実施形態のセキュリティシステムは、紛失や盗難時に携帯電話端末２００の情報を保護するものであり、ＡＳＰ１００を備えている。
【００４５】
ＡＳＰ１００は、たとえば、Ｗｅｂブラウザ機能を有する携帯電話端末２００に、ＡＳＰ１００が保有する各種アプリケーションソフトを提供する。携帯電話端末２００は、ＡＳＰ１００にブラウザを介してアクセスし、ＡＳＰ１００が保有するアプリケーションソフトを起動し、実行させることができる。また、ＡＳＰ１００は、通信端末装置１０および電話機２０と接続可能であり、ユーザ３０からの問い合わせや連絡を受け付ける。なお、携帯電話端末２００の詳細については後述する。
【００４６】
ＡＳＰ１００は、通信部１０２と、Ｗｅｂページ提供部１０４と、プログラム記憶部１０６と、セキュリティプログラム１０８と、管理情報データベース（図中、「管理情報ＤＢ」と示す）１１０と、メール送受信部１１２と、通信部１１４と、ＩＶＲ１１６と、制御部１１８と、を含む。
【００４７】
通信部１０２は、携帯電話端末２００と無線通信を行う。Ｗｅｂページ提供部１０４は、ブラウザ機能を有する端末、ここでは、携帯電話端末２００および通信端末装置１０が参照するＷｅｂページを提供する。プログラム記憶部１０６は、ＡＳＰ１００が保有する各種のアプリケーションソフトを格納する。本実施形態において、セキュリティプログラム１０８がプログラム記憶部１０６に格納される。セキュリティプログラム１０８は、携帯電話端末２００にダウンロードされ、携帯電話端末２００の情報をＡＳＰ１００との連携により保護する機能を有するプログラムである。
【００４８】
管理情報データベース１１０は、本セキュリティシステムを利用するユーザの各種情報が格納されたデータベースである。メール送受信部１１２は、所謂メーラーであり、ＡＳＰ１００から各携帯電話端末２００にメールを作成し、送信するとともに、各携帯電話端末２００から送信されたメールを受信する。通信部１１４は、通信端末装置１０とインターネットなどのネットワークを介して通信を行う。通信部１１４により、インターネットを経由してユーザ３０からの盗難紛失届けを受信することが可能となり、電話回線による接続ができない場合であっても盗難紛失届けを受信することができることとなる。
【００４９】
ＩＶＲ１１６は、音声自動応答装置であり、音声による自動応答を行うコンピュータシステムである。ユーザ３０である発信者のダイヤル操作に応じて、予め録音してある音声ガイダンスを自動的に再生する。あるいは、発信者側の発話を音声認識する音声認識部を有するものでもよく、音声認識された発話内容に応じて、再生を行うこともできる。ＩＶ

Ｒ１１６により、インターネットを介しての通信端末装置１０などからＡＳＰ１００への接続ができない場合であっても盗難紛失届けを受信することができることとなる。制御部１１８は、ＡＳＰ１００の各要素とともに装置全体を制御する。なお、図１において、制御部１１８からの制御ラインは省略してある。

【００５０】

図２は、図１のセキュリティシステムによって内部の情報が保護される携帯電話端末２００の構成を示すブロック図である。

【００５１】

携帯電話端末２００は、通信部２０２と、ブラウザ部２０４と、プログラム記憶部２０６と、実行部２１０と、操作受付部２１２と、表示部２１４と、メール送受信部２１６と、メールボックス２１８（図中、「メールＢＯＸ」と示す）と、情報記憶部２２２と、メモリアクセス部２２４と、メディア入出力部２２６と、制御部２２８と、を含む。

【００５２】

携帯電話端末２００は、インターネットに接続可能でブラウザ機能を有する一般的な携帯電話であり、アドレス情報やメールなど個人に関する各種情報を保有する。あるいは、携帯電話端末２００は、電子マネー決済機能、あるいは個人認証機能などを有してもよい。なお、以下の説明において、本セキュリティシステムによる携帯電話端末２００の情報の保護とは、アドレス情報やメールなど個人に関する各種情報記憶部へのアクセスや参照を防止することや、電子マネー決済機能や個人認証機能などの不正利用を防止することなどを含む。また、本実施形態において、セキュリティシステムの対象となる携帯通信端末として、携帯電話端末２００を例として説明するが、これに限定されない。携帯通信端末は、たとえば、携帯電話、ＰＤＡ、ページャ、ノート型パソコンなど、無線通信が可能で持ち運びできる各種情報端末を含む。

【００５３】

通信部２０２は、ＡＳＰ１００と無線通信する。ブラウザ部２０４は、通信部２０２を介してＡＳＰ１００に接続し、ＡＳＰ１００が提供するＷｅｂページにアクセスする。プログラム記憶部２０６は、ＡＳＰ１００から通信部２０２を介してダウンロードされたアプリケーションソフトを格納する。本実施形態において、携帯電話端末２００は、ＡＳＰ１００からセキュリティプログラム１０８をダウンロードし、格納する。

【００５４】

実行部２１０は、プログラム記憶部２０６に格納されたプログラムを実行する。操作受付部２１２は、図示されない携帯電話端末２００の操作キーなどの操作を受け付ける。表示部２１４は、液晶表示パネルなどであり、文字情報、画像、動画像を表示する。メール送受信部２１６は、通信部２０２を介してメールを送受信する。メールボックス２１８は、メール送受信部２１６が送受信したメールを保存する。

【００５５】

情報記憶部２２２は、アドレス帳２２３を含む各種情報を記憶する。メモリアクセス部２２４は、メールボックス２１８および情報記憶部２２２にアクセスし、メールボックス２１８および情報記憶部２２２に格納されたメールおよび情報を読み出し、表示部２１４に表示したり、メディア入出力部２２６を介して外部に出力したりする。メディア入出力部２２６は、各種メディアや外部出力端子を介して、各種メディアや外部記憶装置と、データの入出力を行う。たとえば、メールボックス２１８や情報記憶部２２２に格納されているメールや情報をメディアに出力したり、メディアからデータを入力し、情報記憶部２２２に格納したりする。

【００５６】

図３は、上記のように構成されたセキュリティシステムの概略機能ブロック図である。

【００５７】

本実施形態のＡＳＰ１００は、指示受付部１２０と、認証部１２６と、判断部１２８と、指示提示部１３０と、を含む。

【００５８】

指示受付部１２０は、通信部１１４を介してＷｅｂページ提供部１０４にアクセスした通信端末装置１０からの指示を受け付けるとともに、ＩＶＲ１１６を介して電話機２０からの指示を受け付ける。あるいは、通信部１０２を介してＷｅｂページ提供部１０４にアクセスした携帯電話端末２００からの指示を受け付ける。

【００５９】

本実施形態において、指示受付部１２０は、携帯電話端末２００のユーザ３０が本セキュリティシステムのサービス利用の申し込みをＷｅｂページ提供部１０４を介して受け付ける。Ｗｅｂページ提供部１０４は、サービス利用の申し込みフォーム（不図示）を提示して、ユーザ３０からの申し込みを受け付ける。申し込み内容には、ユーザＩＤとして携帯電話端末２００の電話番号と、パスワードと、が含まれる。本実施形態において、ユーザＩＤとして携帯電話端末２００の電話番号を用いたが、これに限定されない。ＡＳＰ１００によって付与される固有の管理用ＩＤであってもよい。さらに、指示受付部１２０は、ユーザ３０からの盗難紛失などの紛失届けと、紛失届けを解除する解除届けと、を通信端末装置１０または電話機２０から受け付ける。紛失届けおよび解除届けには、ユーザ３０のユーザＩＤ、たとえば、携帯電話端末２００の電話番号、およびパスワードが含まれる。

【００６０】

本実施形態において、管理情報データベース１１０は、ユーザ情報テーブル（図中、「ユーザ情報」と示す）１２２を有する。ユーザ情報テーブル１２２は、図４に示すように、ユーザＩＤと、パスワードと、処置フラグ１２４と、が関連付けられて記憶される。処置フラグ１２４は、該当するユーザＩＤの携帯電話端末２００が現在、情報保護処置中であるか否かを示す。「１」の場合、情報保護処置中であり、「０」の場合、保護処置は解除中であることを示す。

【００６１】

図３に戻り、認証部１２６は、管理情報データベース１１０にアクセスし、ユーザ情報テーブル１２２を参照し、紛失届けおよび解除届けに含まれるユーザＩＤおよびパスワードに基づいて、ユーザ３０の認証を行う。すなわち、紛失届けおよび解除届けに含まれるユーザＩＤおよびパスワードがユーザ情報テーブル１２２のユーザＩＤおよびパスワードと一致した場合、ユーザ３０を認証する。

【００６２】

判断部１２８は、認証部１２６がユーザ３０を認証したとき、ユーザ情報テーブル１２２を参照し、指示受付部１２０が紛失届けを受け付けた場合は当該ユーザ３０の処置フラグ１２４に「１」をセットし、指示受付部１２０が解除届けを受け付けた場合は当該ユーザ３０の処置フラグ１２４を「０」にリセットする。また、認証部１２６は、指示受付部１２０が携帯電話端末２００からのサービス利用の申し込みで受け付けたユーザＩＤとパスワードをユーザ情報テーブル１２２に登録する。

【００６３】

指示提示部１３０は、管理情報データベース１１０にアクセスし、ユーザ情報テーブル１２２を参照し、処置フラグ１２４の状態を携帯電話端末２００に通信部１０２を介して提示する。

【００６４】

また、携帯電話端末２００は、指示参照部２３０と、判定部２３２と、保護部２３４と、保護フラグ２３６と、解除部２３８と、を含む。

【００６５】

指示参照部２３０は、ＡＳＰ１００に通信部２０２を介してアクセスし、ＡＳＰ１００が保有する処置フラグ１２４の提示を要求し、処置フラグ１２４を参照する。判定部２３２は、指示参照部２３０が取得した処置フラグ１２４に基づいて、処置フラグ１２４がオン（本実施形態では「１」）かオフ（本実施形態では「０」）かを判定する。処置フラグ１２４がオンの場合、判定部２３２は保護部２３４に情報を保護する処置を行うよう指示する。処置フラグ１２４がオフの場合、判定部２３２は解除部２３８に情報保護処置を解

除する指示を行う。

【００６６】

保護部２３４は、判定部２３２からの指示にしたがい、携帯電話端末２００の各種情報を保護する処置を行う。保護される情報とは、たとえば、メールボックス２１８のメールや情報記憶部２２２のアドレス帳２２３などである。また、電子決済機能や個人認証機能を有する携帯電話端末２００の場合、電子決済機能や個人認証機能に関する情報を保護する。また、保護部２３４は、情報保護処置を行った場合、保護フラグ２３６を「１」にセットする。

【００６７】

情報保護処置の例として、下記のものが考えられる。

（１）携帯電話端末２００の操作キーをロックし、操作不能とする。たとえば、操作キーの押下を全て無視するように構成する。ただし、例外的に携帯電話端末２００への着信があった場合に、通話キーの操作は可能とすることもできる。

（２）携帯電話端末２００の電源を自動的にオフさせる。

【００６８】

これらの処置は、本セキュリティシステムの利用契約時にユーザ３０毎に予め設定してもよいし、該当する処置を行うセキュリティプログラムを提供するようにしてもよいし、あるいは、紛失届け時に利用する処置を選択できるようにしてもよい。

【００６９】

以下、紛失届け時に利用する処置を選択する場合の例を説明する。ＡＳＰ１００の管理情報データベース１１０は、図５に示すようなユーザ情報テーブル１３２を有し、ユーザ情報テーブル１３２にはユーザＩＤと、パスワードと、レベル１処置フラグ１３４と、レベル２処置フラグ１３５と、が関連付けられて記憶される。指示受付部１２０は、ユーザ３０のユーザＩＤとパスワードに加え、利用したい処置のレベルを含む紛失届けを受け付ける。認証部１２６は、ユーザ３０を認証した後、受け付けた処置レベルに対応するレベル１処置フラグ１３４またはレベル２処置フラグ１３５に「１」をセットする。

【００７０】

携帯電話端末２００では、指示参照部２３０が、このレベル１処置フラグ１３４およびレベル２処置フラグ１３５の提示をＡＳＰ１００に要求して参照する。判定部２３２は、指示参照部２３０が取得した処置フラグに基づいて、どの処置フラグがオンかオフかによって、携帯電話端末２００で情報を保護するのか保護処置を解除するのか、情報を保護する場合、レベル１およびレベル２のどちらのレベルの処置を行うのかを判定する。そして、判定部２３２は保護部２３４にレベル１の処置とレベル２の処置のどちらの処置を行うかを指示する。

【００７１】

このようにして、携帯電話端末２００への保護処置のレベルを選択することができるので、状況に応じた適切な処置を施すことが可能となり、利便性が増す。たとえば、「個人ユーザが友人宅に携帯電話端末を忘れた」程度であれば、「キーをロックする」処置を施し、データを友人に見せないようにして後で返してもらうようにすることができる。また「重要な顧客情報の入った会社の携帯電話端末が盗難にあった」というときは、すぐに「電源を落として立ち上がらないようにする」処置を施してデータを守ることができる。

【００７２】

図３に戻り、解除部２３８は、判定部２３２が処置フラグ１２４がオフであると判定した場合に、保護部２３４による情報保護処置を解除させ、保護フラグ２３６をオフ（本実施形態では「０」）にリセットする。

【００７３】

また、図６に示すように携帯電話端末２００は、自動起動部２３９を含む。自動起動部２３９は、携帯電話端末２００の電源がオンされたとき、自動的にセキュリティプログラム１０８を起動させる。これにより、本セキュリティシステムを利用しているユーザ３０の携帯電話端末２００は、電源がオンしている間、常にセキュリティプログラム１０８が

動作している状態とすることができる。

【００７４】

図７は、本実施形態の携帯電話端末２００の動作の一例を示すフローチャートである。

【００７５】

まず、携帯電話端末２００の電源が投入されると（ステップＳ１１）、セキュリティプログラム１０８を実行部２１０が自動的に起動し実行する（ステップＳ１３）。つづいて、指示参照部２３０が通信部２０２を介してＡＳＰ１００にアクセスし、ＡＳＰ１００に処置フラグ１２４の提示を要求し、処置フラグ１２４を参照する（ステップＳ１５）。このとき、ＡＳＰ１００では、指示提示部１３０が通信部１０２を介して携帯電話端末２００からの処置フラグ１２４の提示要求を受け付け、管理情報データベース１１０にアクセスし、ユーザ情報テーブル１２２を参照し、携帯電話端末２００のユーザＩＤに対応する処置フラグ１２４を携帯電話端末２００に提示する。なお、ステップＳ１５の処置フラグ１２４のチェックは、常時、または定期的に実行されるものとする。

【００７６】

つづいて、指示参照部２３０は、処置フラグ１２４の参照時、通信エラーなどのエラーがなかった否かを判定する（ステップＳ１７）。エラーがなかった場合（ステップＳ１７のＹＥＳ）、判定部２３２が処置フラグ１２４がオンであるか否かを判定する（ステップＳ１９）。処置フラグ１２４がオンの場合（ステップＳ１９のＹＥＳ）、保護部２３４が情報保護処置を行い、保護フラグ２３６に「１」をセットする（ステップＳ２１）。ここでは、たとえば、携帯電話端末２００の電源が自動的にオフされる。

【００７７】

一方、処置フラグ１２４がオフの場合（ステップＳ１９のＮＯ）、解除部２３８が保護フラグ２３６がオンか否か、すなわち情報保護処置中であるか否かを判定する（ステップＳ２５）。情報保護処置中である場合（ステップＳ２５のＹＥＳ）、解除部２３８は、保護処置を解除し、保護フラグ２３６を「０」にリセットする（ステップＳ２７）。また、情報保護処置中でない場合（ステップＳ２５のＮＯ）、ステップＳ１５に戻り、処置フラグ１２４のチェックを行う。

【００７８】

また、ステップＳ１５における処置フラグ１２４の参照時に通信エラーなどが発生し、処置フラグ１２４が得られなかった場合（ステップＳ１７のＮＯ）、保護部２３４が保護フラグ２３６がオンか否か、すなわち情報保護処置中であるか否かを判定する（ステップＳ２３）。情報保護処置中である場合（ステップＳ２３のＹＥＳ）、ステップＳ２１に進み、保護部２３４が情報保護処置を行い、保護フラグ２３６に「１」をセットする。情報保護処置中でない場合（ステップＳ２３のＮＯ）、ステップＳ１５に戻る。

【００７９】

このステップＳ１７により、たとえば、セキュリティプログラム１０８によって、情報保護処置がなされた携帯電話端末２００の電源が一旦オフした後に、再度立ち上げられた場合、圏外などでＡＳＰ１００との通信が行えない場合であっても、保護フラグ２３６を参照することにより、自動的に情報保護処置を行うことができる。

【００８０】

以上のように構成された本実施形態のセキュリティシステムのシステム全体の動作について、図を用いて説明する。図８は、本実施形態のセキュリティシステムの動作の一例を示すフローチャートである。

【００８１】

まず、携帯電話端末２００のユーザ３０は、本セキュリティシステムの申し込みを行う（ステップＡ１１）。ユーザ３０は、携帯電話端末２００を操作して、ブラウザ部２０４を介してＡＳＰ１００にアクセスし、セキュリティシステムの申し込みページを参照し、申し込みフォーム（不図示）にて申し込むことができる。あるいは、ユーザ３０は、通信端末装置１０を介してＡＳＰ１００にアクセスし、セキュリティシステムの申し込みページを参照し、申し込みフォームにて申し込んでもよいし、電話機２０を介してＡＳＰ１０

０に電話をかけ、ＩＶＲ１１６の音声ガイダンスに応じて入力することにより申し込んでもよい。なお、本実施形態において、申し込みフォームにおいて、携帯電話端末２００の電話番号をユーザＩＤとし、ユーザＩＤとパスワードを登録する。

【００８２】

ＡＳＰ１００の指示受付部１２０が携帯電話端末２００からのサービス利用の申し込みを受け付け、認証部１２６により管理情報データベース１１０のユーザ情報テーブル１２２にユーザＩＤとパスワードを登録する（ステップＡ１３）。

【００８３】

つづいて、携帯電話端末２００に、ＡＳＰ１００からセキュリティプログラム１０８がダウンロードされる（ステップＡ１５）。具体的には、ユーザ登録後またはユーザ認証された携帯電話端末２００が、ブラウザ部２０４を介してセキュリティプログラム１０８のダウンロードページ（不図示）にアクセスし、セキュリティプログラム１０８を通信部２０２を介してダウンロードし、プログラム記憶部２０６に保存する。そして、実行部２１０がセキュリティプログラム１０８を実行する（ステップＡ１７）。

【００８４】

その後、ユーザ３０が携帯電話端末２００を紛失してしまったとする。ユーザ３０は、通信端末装置１０または電話機２０を介してＡＳＰ１００に紛失届けを提出する（ステップＡ１９）。ここでは、通信端末装置１０を介して紛失届けを提出した場合について説明する。通信端末装置１０はＡＳＰ１００のＷｅｂページ提供部１０４が提供する紛失届けページ（不図示）にアクセスし、紛失届けに必要な、ユーザＩＤとパスワードを入力する。

【００８５】

ＡＳＰ１００において、指示受付部１２０がＷｅｂページ提供部１０４を介して入力されたユーザＩＤとパスワードを受け付ける。認証部１２６が、管理情報データベース１１０にアクセスし、ユーザ情報テーブル１２２を参照し、受け付けたユーザＩＤとパスワードに基づいて、ユーザの認証を行う（ステップＡ２１）。認証された場合、判断部１２８は、管理情報データベース１１０にアクセスして、ユーザ情報テーブル１２２の処置フラグ１２４を「１」にセットする（ステップＡ２２）。

【００８６】

一方、携帯電話端末２００では、起動中のセキュリティプログラム１０８により、指示参照部２３０が通信部２０２を介してＡＳＰ１００にアクセスし、ＡＳＰ１００に処置フラグ１２４の提示を要求し、処置フラグ１２４を参照する（ステップＡ２３）。ＡＳＰ１００では、指示提示部１３０が通信部１０２を介して携帯電話端末２００からの処置フラグ１２４の提示要求を受け付け、管理情報データベース１１０にアクセスし、ユーザ情報テーブル１２２を参照し、携帯電話端末２００のユーザＩＤに対応する処置フラグ１２４を携帯電話端末２００に提示する。

【００８７】

携帯電話端末２００において、判定部２３２がＡＳＰ１００から受け取った処置フラグ１２４がオンであるか否かを判定する。判定部２３２が処置フラグ１２４がオンであると判定した場合、保護部２３４が情報保護処置を行う（ステップＡ２５）。情報保護処置は、上述したように、たとえば、携帯電話端末２００の電源を自動的にオフする。

【００８８】

この状態で、携帯電話端末２００の電源が投入されると（ステップＡ４０）、セキュリティプログラム１０８が再起動する（ステップＡ１７）。指示参照部２３０が通信部２０２を介してＡＳＰ１００にアクセスし、ＡＳＰ１００に処置フラグ１２４の提示を要求し、処置フラグ１２４を参照する（ステップＡ２３）。処置フラグ１２４は「１」であるので、判定部２３２が処置フラグ１２４はオンであると判定し、保護部２３４が情報保護処置を行い、たとえば、携帯電話端末２００の電源を自動的にオフする（ステップＡ２５）。

【００８９】

このように、紛失した携帯電話端末２００に対し、遠隔からＡＳＰ１００を経由して携帯電話端末２００の情報保護処置を施すことができる。

【００９０】

その後、ユーザ３０の手元に携帯電話端末２００が戻って来たとき、ユーザ３０は、通信端末装置１０または電話機２０を介してＡＳＰ１００に解除届けを提出する（ステップＡ２７）。ここでは、電話機２０を介して解除届けを提出した場合について説明する。ユーザ３０が電話機２０を使用してＡＳＰ１００に電話をかけ、ＡＳＰ１００のＩＶＲ１１６から音声ガイダンスにしたがって、解除届けに必要なユーザＩＤとパスワードを入力する。

【００９１】

ＡＳＰ１００において、指示受付部１２０がＩＶＲ１１６を介して電話機２０から入力されたユーザＩＤとパスワードを受け付ける。認証部１２６が、管理情報データベース１１０にアクセスし、ユーザ情報テーブル１２２を参照し、受け付けたユーザＩＤとパスワードに基づいて、ユーザの認証を行う（ステップＡ２９）。認証された場合、判断部１２８は、管理情報データベース１１０にアクセスして、ユーザ情報テーブル１２２の処置フラグ１２４を「０」にリセットする（ステップＡ３１）。

【００９２】

この状態で、携帯電話端末２００の電源が再投入されると、セキュリティプログラム１０８が起動し、指示参照部２３０が通信部２０２を介してＡＳＰ１００にアクセスし、ＡＳＰ１００に処置フラグ１２４の提示を要求し、処置フラグ１２４を参照する（ステップＡ３３）。携帯電話端末２００において、判定部２３２がＡＳＰ１００から受け取った処置フラグ１２４がオンであるか否かを判定する。判定部２３２が処置フラグ１２４がオフであると判定した場合、解除部２３８が情報保護処置を解除する（ステップＡ３５）。

【００９３】

このようにして、ユーザ３０の手元に携帯電話端末２００が戻ってきたとき、情報保護処置を解除させることができる。

【００９４】

以上説明したように、本実施形態のセキュリティシステムによれば、携帯電話端末２００からＡＳＰ１００に定期的にアクセスして情報保護処置を行うか否かを判断できるので、紛失または盗難時に遠隔で携帯電話端末２００の情報を保護することが可能となる。

【００９５】

また、ユーザ認証を行うことにより、不正に携帯電話端末の情報保護処置および保護処置の解除が行われることを防ぐことができ、本システムのセキュリティが向上する。

（第二の実施の形態）

図９は、本発明の実施の形態に係るセキュリティシステムの構成を示すブロック図である。本実施形態のセキュリティシステムは、図３に示した上記実施の形態とは、ＡＳＰ１００からメール送信により携帯電話端末２００に情報保護通知を行い、携帯電話端末２００が情報保護処置を開始する点で相違する。

【００９６】

ＡＳＰ１００は、上記実施の形態のＡＳＰ１００の構成要素に加え、通知部１４０と、メール送受信部１４２と、を含む。

【００９７】

ここで、判断部１２８は、指示受付部１２０が紛失届けを受け付けたとき、管理情報データベース１１０にアクセスし、ユーザ情報テーブル１２２を参照し、認証部１２６が認証したユーザ３０の処置フラグ１２４を「１」にセットするとともに、通知部１４０に当該ユーザ３０の携帯電話端末２００に情報保護指示を通知するよう指示する。

【００９８】

通知部１４０は、この指示にしたがって、当該携帯電話端末２００宛に情報保護指示メールを送信するようメール送受信部１４２に指示する。メール送受信部１４２は、この指示にしたがって、情報保護指示メールを作成し、通信部１０２を介して当該携帯電話端末

２００宛に送信する。ここで、情報保護指示メールは、たとえば、タイトルまたは本文に情報保護指示を示す単語を記載して送信する。あるいは、所定のメールアドレスから送信する。

【００９９】

携帯電話端末２００は、上記実施の形態の構成要素に加えて、解読部２４０と、判定部２４２と、を含む。

【０１００】

ここで、メール送受信部２１６は、通信部２０２を介してＡＳＰ１００から情報保護指示メールを受信し、解読部２４０に受け渡す。解読部２４０は、メール送受信部２１６から受け取ったメールを解読し、情報保護指示メールであるか否かを判定する。たとえば、受け取ったメールのタイトルや本文に情報保護指示を含むか否かを調べる。または、送信元のメールアドレスが所定のアドレスであるか否かを調べる。解読部２４０が、情報保護指示メールであると判定したとき、判定部２４２に情報保護指示メールを受信したことを通知する。

【０１０１】

判定部２４２は、解読部２４０から情報保護指示メールを受信したことが通知されたとき、保護部２３４に情報を保護する処置を行うよう指示する。情報保護指示メールを受信し、情報保護処置がなされた後、判定部２４２は、指示参照部２３０が取得した処置フラグ１２４に基づいて、処置フラグ１２４がオン（本実施形態では「１」）かオフ（本実施形態では「０」）かを判定するようになる。上記実施の形態と異なる点は、指示参照部２３０による処置フラグ１２４の参照が、情報保護指示メールを受信した後から開始されることである。この構成によれば、通常の使用時に定期的に処置フラグ１２４をチェックするためにＡＳＰ１００にアクセスする必要がなくなるので、ＡＳＰ１００との通信回数を大幅に低減することができる。また、携帯電話端末２００が保護指示メールを受信することにより、迅速に情報を保護する処置を開始できるので、システムの信頼性が増す。

【０１０２】

以上のように構成された本実施形態のセキュリティシステムのシステム全体の動作について、図を用いて説明する。図１０は、本実施形態のセキュリティシステムの動作の一例を示すフローチャートである。なお、図８の上記実施の形態のセキュリティシステムのフローチャートとは、ステップＡ１１～ステップＡ２２およびステップＡ２５～ステップＡ３５は同じであるので同じ符号を付して詳細な説明は省略する。

【０１０３】

携帯電話端末２００において、セキュリティプログラム１０８が起動（ステップＡ１７）した後、ＡＳＰ１００において、ユーザ３０により紛失届けが提出され（ステップＡ１９）、ユーザ３０が認証されると（ステップＡ２１）、判断部１２８は、管理情報データベース１１０にアクセスして、ユーザ情報テーブル１２２の処置フラグ１２４を「１」にセットする（ステップＡ２２）。同時に、判断部１２８が通知部１４０に当該ユーザ３０の携帯電話端末２００に情報保護指示を通知するよう指示する。この指示にしたがって、通知部１４０が当該ユーザ３０の携帯電話端末２００宛に情報保護指示メールを送信するようメール送受信部１４２に指示する。この指示にしたがって、メール送受信部１４２が情報保護指示メールを作成し、通信部１０２を介して当該携帯電話端末２００宛に送信する（ステップＢ１１）。

【０１０４】

携帯電話端末２００において、携帯電話端末２００の電源がオンであり、かつ通話圏内にあるとき、メール送受信部２１６が通信部２０２を介してＡＳＰ１００から情報保護指示メールを受信する。そして解読部２４０に受け渡し、解読部２４０がメールを解読し、情報保護指示メールであるか否かを判定する（ステップＢ１３）。解読部２４０が情報保護指示メールであると判定し、判定部２４２に通知する。判定部２４２から保護部２３４に情報を保護する処置を行うよう指示がなされ、指示にしたがって保護部２３４が情報を保護する処置を行う（ステップＡ２５）。また、保護部２３４は、保護フラグ２３６を「

１」にセットする。上述したように情報保護処置により、たとえば、携帯電話端末２００の電源が自動的にオフされる。

【０１０５】

なお、判定部２４２は、以後、携帯電話端末２００の電源が再投入された場合、セキュリティプログラム１０８が自動的に起動され、指示参照部２３０が定期的にＡＳＰ１００にアクセスして取得した処置フラグ１２４に基づいて、処置フラグ１２４がオン（本実施形態では「１」）かオフ（本実施形態では「０」）かを判定するようになる（ステップＢ１５）。ユーザ３０から解除届けが提出されるまでは、処置フラグ１２４はオンであるので、保護部２３４による情報保護処置が続行される（ステップＢ１７）。

【０１０６】

このように、紛失した携帯電話端末２００に対し、遠隔からＡＳＰ１００を経由して携帯電話端末２００の情報保護処置を施すことができる。

【０１０７】

その後、携帯電話端末２００がユーザ３０の手元に戻り、ＡＳＰ１００において、ユーザ３０により解除届けが提出され（ステップＡ２７）、ユーザ３０が認証されると（ステップＡ２９）、判断部１２８が管理情報データベース１１０にアクセスして、ユーザ情報テーブル１２２の処置フラグ１２４を「０」にリセットする（ステップＡ３１）。

【０１０８】

この状態で、携帯電話端末２００の電源が再投入されると、セキュリティプログラム１０８が起動し、指示参照部２３０が処置フラグ１２４を参照する（ステップＡ３３）。判定部２４２が処置フラグ１２４がオフであると判定し、解除部２３８が情報保護処置を解除する（ステップＡ３５）。

【０１０９】

このようにして、ユーザ３０の手元に携帯電話端末２００が戻ってきたとき、情報保護処置を解除させることができる。

【０１１０】

以上説明したように、本実施形態のセキュリティシステムによれば、紛失または盗難時に携帯通信端末の情報を保護することが可能となる。

（第三の実施の形態）

図１１は、本発明の実施の形態に係るセキュリティシステムの構成を示すブロック図である。本実施形態のセキュリティシステムは、図９に示した上記実施の形態とは、ＡＳＰ１００から情報保護通知を携帯電話端末２００にメールで送信するだけでなく、ＡＳＰ１００から保護解除通知も携帯電話端末２００にメールで送信し、情報保護処置および保護解除処置を行う点で相違する。

【０１１１】

ＡＳＰ１００は、図３の上記実施の形態のＡＳＰ１００の構成から指示提示部１３０に替えて通知部１４４を含む。また、図３の管理情報データベース１１０のユーザ情報テーブル１２２の処置フラグ１２４は不要となる。ただし、ＡＳＰ１００の管理用として、各携帯電話端末２００の保護処置状況を記憶してもよい。

【０１１２】

通知部１４４は、判断部１２８からの指示にしたがって、当該携帯電話端末２００宛に情報保護指示メールを送信するようメール送受信部１１２に指示する。また、判断部１２８は、指示受付部１２０が解除届けを受け付けたとき、管理情報データベース１１０にアクセスし、メール送受信部１１２を参照し、通知部１４４に当該ユーザ３０の携帯電話端末２００に保護解除指示を通知するよう指示する。通知部１４４は、この指示にしたがって、当該携帯電話端末２００宛に保護解除指示メールを送信するようメール送受信部１１２に指示する。

【０１１３】

メール送受信部１１２は、通知部１４４からの指示にしたがって、情報保護指示メールまたは保護解除指示メールを作成し、通信部１０２を介して当該携帯電話端末２００宛に

送信する。ここで、情報保護指示メールおよび保護解除指示メールは、たとえば、タイトルまたは本文に情報保護指示および保護解除指示を示す単語を記載して送信する。あるいは、指示毎に異なる所定のメールアドレスから送信する。

【０１１４】

携帯電話端末２００は、図３の上記実施の形態の構成の指示参照部２３０および判定部２３２に替えて解読部２４４および判定部２４６を含む。

【０１１５】

ここで、メール送受信部２１６は、メールを通信部２０２を介して受信し、解読部２４４に受け渡す。解読部２４４は、メール送受信部２１６から受け取ったメールを解読し、情報保護指示メールまたは保護解除指示メールであるか否かを判定する。たとえば、受け取ったメールのタイトルや本文に情報保護指示または保護解除指示を含むか否かを調べる。または、送信元のメールアドレスが、各指示に対応する所定のアドレスであるか否かを調べる。解読部２４４は、判定した結果を判定部２４６に通知する。また、解読部２４４は、着信メールが情報保護指示メールや保護解除指示メールではないと判定した場合、メールボックス２１８にメールを保存し、再び、メール送受信部２１６によるメールチェックを行うよう指示する。

【０１１６】

判定部２４６は、解読部２４４から情報保護指示メールを受信したことが通知されたとき、保護部２３４に情報を保護する処置を行うよう指示する。また、判定部２４６は、解読部２４４から保護解除指示メールを受信したことが通知されたとき、解除部２３８に保護を解除するよう指示する。

【０１１７】

図１２は、本実施形態の携帯電話端末２００の動作の一例を示すフローチャートである。なお、図７の上記実施形態の携帯電話端末２００の動作のフローチャートとは、フラグチェックのステップＳ１５に替えてメールチェックのステップＳ３１、通信エラー判定のステップＳ１７に替えてメールの有無および通信エラー判定のステップＳ３３、フラグ判定のステップＳ１９に替えてメール判定のステップＳ３５を設けた点で相違する。

【０１１８】

まず、携帯電話端末２００の電源が投入されると（ステップＳ１１）、セキュリティプログラム１０８を実行部２１０が自動的に起動し実行する（ステップＳ１３）。つづいて、メール送受信部２１６が通信部２０２を介してメールサーバ（不図示）にアクセスし、メールチェックを行う（ステップＳ３１）。つづいて、解読部２４０は、メールチェック時、受信メールがあるかないか、また通信エラーなどのエラーがなかったか否かを判定する（ステップＳ３３）。

【０１１９】

着信メールがあり、かつ通信エラーがなかった場合（ステップＳ３３のＹＥＳ）、解読部２４４がメール送受信部２１６から受け取ったメールを解読し、情報保護指示メールまたは保護解除指示メールであるか否かを判定する（ステップＳ３５）。解読部２４４が情報保護指示メールであると判定した場合（ステップＳ３５の保護）、判定部２４６に判定結果を通知し、判定部２４６は保護部２３４に情報保護処置の指示を行う。保護部２３４が情報保護処置を行い、保護フラグ２３６に「１」をセットする（ステップＳ２１）。ここでは、たとえば、携帯電話端末２００の電源が自動的にオフされる。

【０１２０】

一方、解読部２４４が保護解除指示メールであると判定した場合（ステップＳ３５の解除）、判定部２４６に判定結果を通知し、判定部２４６は解除部２３８に保護処置解除の指示を行う。解除部２３８が保護処置を解除し、保護フラグ２３６を「０」にリセットする（ステップＳ２７）。また、解読部２４４がその他のメールであると判定した場合（ステップＳ３５のその他）、メールボックス２１８にメールを保存し、ステップＳ３１に戻る。ステップＳ３１のメールチェックは、予め決められた時刻に行ってもよいし、定期的に行ってもよい。あるいは、メールチェックは行わず、メールサーバからのメールを単に

受信するだけであってもよいが、通知を取得し迅速な処置を施すためには、定期的にメールチェックを行った方が好ましい。

【０１２１】

以上のように構成された本実施形態のセキュリティシステムのシステム全体の動作について、図を用いて説明する。図１３は、本実施形態のセキュリティシステムの動作の一例を示すフローチャートである。なお、図１０の上記実施の形態のセキュリティシステムのフローチャートとは、ステップＡ１１～ステップＡ２１、ステップＡ２５～ステップＡ２９、およびステップＡ３５は同じであるので同じ符号を付して詳細な説明は省略する。

【０１２２】

携帯電話端末２００において、セキュリティプログラム１０８が起動（ステップＡ１７）された後、ＡＳＰ１００において、ユーザ３０により紛失届けが提出され（ステップＡ１９）、ユーザ３０が認証されると（ステップＡ２１）、判断部１２８が通知部１４４に当該ユーザ３０の携帯電話端末２００に情報保護指示を通知するよう指示する。この指示にしたがって、通知部１４４が認証部１２６で認証されたユーザ３０の携帯電話端末２００宛に情報保護指示メールを送信するようメール送受信部１１２に指示する。この指示にしたがって、メール送受信部１１２が情報保護指示メールを作成し、通信部１０２を介して当該携帯電話端末２００宛に送信する（ステップＣ１１）。

【０１２３】

携帯電話端末２００において、メール送受信部２１６が通信部２０２を介してＡＳＰ１００から情報保護指示メールを受信し、解読部２４４に受け渡し、解読部２４４がメールを解読し、情報保護指示メールまたは保護解除指示メールであるか否かを判定する（ステップＣ１３）。解読部２４４が情報保護指示メールであると判定し、判定部２４６に通知する。判定部２４６から保護部２３４に情報を保護する処置を行うよう指示がなされ、指示にしたがって保護部２３４が情報を保護する処置を行う（ステップＡ２５）。また、保護部２３４は、保護フラグ２３６を「１」にセットする。情報保護処置は、上述したように、たとえば、携帯電話端末２００の電源が自動的にオフされる。

【０１２４】

このように、紛失した携帯電話端末２００に対し、遠隔からＡＳＰ１００を経由して携帯電話端末２００の情報保護処置を施すことができる。

【０１２５】

その後、ＡＳＰ１００において、ユーザ３０により解除届けが提出され（ステップＡ２７）、ユーザ３０が認証されると（ステップＡ２９）、判断部１２８が通知部１４４に当該ユーザ３０の携帯電話端末２００に保護解除指示を通知するよう指示する。この指示にしたがって、通知部１４４が認証部１２６で認証されたユーザ３０の携帯電話端末２００宛に保護解除指示メールを送信するようメール送受信部１１２に指示する。この指示にしたがって、メール送受信部１１２が保護解除指示メールを作成し、通信部１０２を介して当該携帯電話端末２００宛に送信する（ステップＣ１５）。

【０１２６】

この状態で、携帯電話端末２００において、電源が投入されると、メール送受信部２１６は通信部２０２を介してメールサーバ（不図示）にアクセスし、メールを受信する。メール送受信部２１６が通信部２０２を介してＡＳＰ１００からの保護解除指示メールを受信し、解読部２４４に受け渡し、解読部２４４がメールを解読し、情報保護指示メールまたは保護解除指示メールであるか否かを判定する（ステップＣ１７）。なお、メールを受信しなかった場合、および保護解除指示メールでなかった場合は、そのまま情報保護処置を行う。すなわち、電源をオフする（不図示）。

【０１２７】

解読部２４４が保護解除指示メールであると判定し、判定部２４６に通知する。判定部２４６から解除部２３８に保護処置を解除するよう指示がなされ、指示にしたがって解除部２３８が保護処置を解除する（ステップＡ３５）。

【０１２８】

このようにして、ユーザ３０の手元に携帯電話端末２００が戻ってきたとき、情報保護処置を解除させることができる。

【０１２９】

以上説明したように、本実施形態のセキュリティシステムによれば、紛失または盗難時に携帯通信端末の情報を保護することが可能となる。また、保護処置後、定期的に処置フラグ１２４をチェックするためにＡＳＰ１００にアクセスする必要がなく、ＡＳＰ１００との通信回数を大幅に低減することができる。

（第四の実施の形態）

図１４は、本発明の実施の形態に係るセキュリティシステムの構成を示すブロック図である。本実施形態のセキュリティシステムは、図３に示した上記実施の形態とは、ＡＳＰ１００から所定の電話番号で発信された情報保護通知および保護解除通知を携帯電話端末２００が着信し、その着信をトリガとして情報保護処置および保護処置解除を行う点で相違する。

【０１３０】

ＡＳＰ１００は、上記実施の形態のＡＳＰ１００の構成要素に加え、指示提示部１３０に替えて通知部１５０と、発信部１５２と、番号記憶部１５４と、を含む。また、図３の管理情報データベース１１０のユーザ情報テーブル１２２の処置フラグ１２４は不要となる。ただし、ＡＳＰ１００の管理用として、各携帯電話端末２００の保護処置状況を記憶してもよい。

【０１３１】

ここで、判断部１２８は、指示受付部１２０が紛失届けまたは解除届けを受け付けたとき、管理情報データベース１１０にアクセスし、ユーザ情報テーブル１２２を参照し、通知部１５０に当該ユーザ３０の携帯電話端末２００に情報保護指示を通知するよう指示する。

【０１３２】

通知部１５０は、この指示にしたがって、番号記憶部１５４にアクセスし、図１５（ａ）に示す発信番号テーブル１５６を参照し、情報保護指示に該当する電話番号を取得し、取得した電話番号から携帯電話端末２００宛に電話をかけるよう発信部１５２に指示する。図１５（ａ）に示すように発信番号テーブル１５６は、情報保護通知用および保護解除通知用の発信電話番号をそれぞれ有する。発信部１５２は、通知部１５０からの指示にしたがって、当該携帯電話端末２００に対して通信部１０２を介して所定の発信電話番号から電話をかける。

【０１３３】

携帯電話端末２００は、上記実施の形態の構成要素に加えて、指示参照部２３０および判定部２３２に替えて、着信部２５０と、番号記憶部２５２と、判定部２５４と、を含む。

【０１３４】

着信部２５０は、通信部２０２を介してＡＳＰ１００からの電話を着信し、着信電話番号を取得する。判定部２５４は、番号記憶部２５２にアクセスし、図１５（ｂ）に示される着信番号テーブル２５６を参照し、着信部２５０で着信した着信電話番号が情報保護通知および保護解除通知のいずれの通知であるかを判定する。判定部２５４が情報保護通知であると判定したとき、保護部２３４に情報を保護する処置を行うよう指示する。一方、判定部２５４が保護解除通知であると判定したとき、解除部２３８に保護処置を解除するよう指示する。

【０１３５】

以上のように構成された本実施形態のセキュリティシステムのシステム全体の動作について、図を用いて説明する。図１６は、本実施形態のセキュリティシステムの動作の一例を示すフローチャートである。なお、図８の上記実施の形態のセキュリティシステムのフローチャートとは、ステップＡ１１～ステップＡ２１およびステップＳ２５～ステップＳ２９、ステップＳ３５は同じであるので同じ符号を付して詳細な説明は省略する。

【０１３６】
携帯電話端末２００において、セキュリティプログラム１０８が起動（ステップＡ１７）した後、ＡＳＰ１００において、ユーザ３０により紛失届けが提出され（ステップＡ１９）、ユーザ３０が認証されると（ステップＡ２１）、判断部１２８が通知部１５０に当該ユーザ３０の携帯電話端末２００に情報保護指示を通知するよう指示する。
【０１３７】
この指示にしたがって、通知部１５０は番号記憶部１５４にアクセスし、発信番号テーブル１５６を参照して情報保護指示通知用の発信電話番号（×××－×××－１１１１）を取得し、発信部１５２に発信を指示する。この指示にしたがって、発信部１５２が通信部１０２を介して当該携帯電話端末２００に上記の発信電話番号から電話をかける（ステップＤ１１）。
【０１３８】
携帯電話端末２００において、着信部２５０が通信部２０２を介してＡＳＰ１００からの電話を着信し、着信電話番号を判定部２５４に受け渡す（ステップＤ１３）。ここでは、着信電話番号は「×××－×××－１１１１」である。判定部２５４は、番号記憶部２５２にアクセスし、着信番号テーブル２５６を参照して、着信電話番号に対応する通知を判定し、情報保護通知であると判定する。
【０１３９】
判定部２５４は、保護部２３４に情報を保護する処置を行うよう指示し、指示にしたがって保護部２３４が情報を保護する処置を行う（ステップＡ２５）。また、保護部２３４は、保護フラグ２３６を「１」にセットする。上述したように情報保護処置により、たとえば携帯電話端末２００の電源が自動的にオフされる。
【０１４０】
なお、判定部２５４は、以後、携帯電話端末２００の電源が投入された場合、保護フラグ２３６を参照し、現在情報保護処置中であるか否かを判定し、情報保護処置中である場合は、携帯電話端末２００の電源を自動的にオフする（不図示）。
【０１４１】
このように、紛失した携帯電話端末２００に対し、遠隔からＡＳＰ１００を経由して携帯電話端末２００の情報保護処置を施すことができる。
【０１４２】
その後、ＡＳＰ１００において、ユーザ３０により解除届けが提出され（ステップＡ２７）、ユーザ３０が認証されると（ステップＡ２９）、判断部１２８が通知部１５０に当該ユーザ３０の携帯電話端末２００に保護解除指示を通知するよう指示する。
【０１４３】
この指示にしたがって、通知部１５０は番号記憶部１５４にアクセスし、発信番号テーブル１５６を参照して保護解除示通知用の発信電話番号（×××－×××－９９９９）を取得し、発信部１５２に発信を指示する。この指示にしたがって、発信部１５２が通信部１０２を介して当該携帯電話端末２００に上記の発信電話番号から電話をかける（ステップＤ１５）。
【０１４４】
携帯電話端末２００において、着信部２５０が通信部２０２を介してＡＳＰ１００からの電話を着信し、着信電話番号を判定部２５４に受け渡す（ステップＤ１７）。ここでは、着信電話番号は「×××－×××－９９９９」である。判定部２５４は、番号記憶部２５２にアクセスし、着信番号テーブル２５６を参照して、着信電話番号に対応する通知を判定し、保護解除通知であると判定する。
【０１４５】
判定部２５４は、解除部２３８に保護処置を解除するよう指示し、指示にしたがって解除部２３８が保護処置を解除する（ステップＡ３５）。
【０１４６】
このようにして、ユーザ３０の手元に携帯電話端末２００が戻ってきたとき、情報保護

処置を解除させることができる。

【０１４７】

以上説明したように、本実施形態のセキュリティシステムによれば、予め登録されている所定の電話番号からの着信をトリガとして、携帯電話端末２００の情報保護処置または保護処置の解除ができるので、携帯電話端末２００がインターネットに接続できない状況であっても電話が繋がれば情報を保護または保護を解除することが可能となる。このようにして、本実施形態のセキュリティシステムにより、紛失または盗難時に携帯通信端末の情報を保護することが可能となる。

（第五の実施の形態）

図１７は、本発明の実施の形態に係るセキュリティシステムの構成を示すブロック図である。本実施形態のセキュリティシステムは、上記実施の形態とは、ＡＳＰ１００において、本セキュリティシステムの利用履歴情報を保有し、携帯電話端末２００のユーザ３０に提供する点で相違する。

【０１４８】

ＡＳＰ１００は、上記実施の形態のＡＳＰ１００の構成要素に加え、管理情報データベース１１０に替えて管理情報データベース１６０と、記録部１６６と、履歴提示部１６８と、を含む。

【０１４９】

管理情報データベース１６０は、ユーザ履歴情報記憶部（図中、「ユーザ履歴情報」と示す）１６２を含む。ユーザ履歴情報記憶部１６２には、サービス契約履歴１６４および保護処置履歴１６５が記録部１６６によって記録される。

【０１５０】

サービス契約履歴１６４には、本セキュリティシステムの利用の申し込み日時、解約日時などが記録される。保護処置履歴１６５には、ユーザ３０からの紛失届けおよび解除届けに応じて施された情報保護処置および保護解除の日時などが記録される。

【０１５１】

履歴提示部１６８は、通信端末装置１０を介してユーザ３０がサービス契約履歴１６４または保護処置履歴１６５の参照を要求したとき、各履歴を提示する。具体的には、ユーザ３０が通信端末装置１０を介してＡＳＰ１００にアクセスしたとき、Ｗｅｂページ提供部１０４を介して履歴提示部１６８がサービス契約履歴１６４または保護処置履歴１６５の参照ページ（不図示）を提示する。Ｗｅｂページ提供部１０４がユーザ３０のユーザＩＤを受け付けたとき、履歴提示部１６８が、管理情報データベース１６０のユーザ履歴情報記憶部１６２にアクセスし、受け付けたユーザＩＤに該当するサービス契約履歴１６４または保護処置履歴１６５を取得する。

【０１５２】

あるいは、履歴提示部１６８は、ＩＶＲ１１６を介して、ユーザ３０からサービス契約履歴１６４または保護処置履歴１６５の参照要求を受け付け、音声にてユーザ３０に伝達する。

【０１５３】

このように構成された本実施形態のセキュリティシステムによれば、ユーザ３０の要求に応じて、携帯電話端末２００の情報が保護されていることを示す保護処置履歴を提示することができるので、手元に携帯電話端末２００がなく不安なユーザ３０を安心させることができる。

（第六の実施の形態）

図１８は、本発明の実施の形態に係るセキュリティシステムの構成を示すブロック図である。本実施形態のセキュリティシステムは、図１７の上記実施の形態とは、ＡＳＰ１００において、本セキュリティシステムの利用履歴情報に基づいてサービス料金を課金する点で相違する。

【０１５４】

ＡＳＰ１００は、図１７の上記実施形態のＡＳＰ１００の構成要素に加え、契約期間集

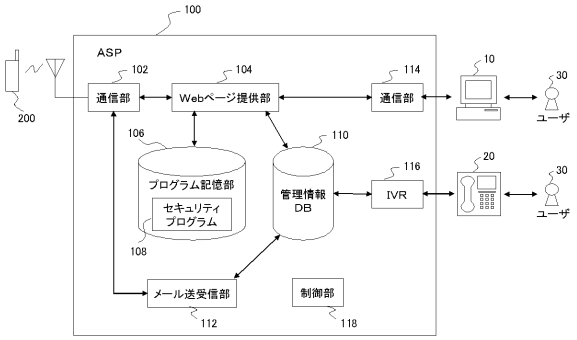
計部１７０と、処置期間集計部１７２と、課金部１７４と、を含む。
【０１５５】
契約期間集計部１７０は、管理情報データベース１６０のユーザ履歴情報記憶部１６２にアクセスし、サービス契約履歴１６４から各ユーザ３０のサービス申し込みから現時点までの課金対象期間の集計を行う。
【０１５６】
処置期間集計部１７２は、管理情報データベース１６０のユーザ履歴情報記憶部１６２にアクセスし、保護処置履歴１６５から各ユーザ３０の情報保護処置を行った期間の集計を行う。
【０１５７】
課金部１７４は、契約期間集計部１７０および処置期間集計部１７２で集計された期間に応じて、各ユーザ３０にサービス利用料金の課金を行う。
【０１５８】
このように構成された本実施形態のセキュリティシステムによれば、保護処置サービスの利用や契約期間に応じてサービス利用料金を課金することができる。
【０１５９】
以上、図面を参照して本発明の実施形態について述べたが、これらは本発明の例示であり、上記以外の様々な構成を採用することもできる。
【０１６０】
たとえば、図１５に示した発信番号テーブル１５６および着信番号テーブル２５６は、たとえば、図１９に示すように、複数の保護処置に対応して発信電話番号および着信電話番号を登録した発信番号テーブル１８０および着信番号テーブル２６０とすることもできる。これにより、紛失届け時にユーザ３０が携帯電話端末２００に施す処置を複数の中から選択して指示できることとなる。
【０１６１】
また、携帯電話端末２００に対する保護処置の解除方法として、上記実施の形態では、ＡＳＰ１００を介して解除指示をユーザ３０が行っていたが、その他に以下のようなものが考えられる。
【０１６２】
ＡＳＰ１００において、指示受付部１２０は、紛失届けとして、特定の操作キーパターンの登録を受け付ける。ＡＳＰ１００から携帯電話端末２００に保護処置通知を行う際、一緒にこの操作キーパターンを送信する。携帯電話端末２００では、保護処置を行うとともに、この操作キーパターンを受け付けて記憶する。ユーザ３０の手元に携帯電話端末２００が戻って来たとき、ユーザ３０が携帯電話端末２００の電源を立ち上げるとき、この操作キーパターンでキーを押下すると、保護処置が解除されるようにしてもよい。
【０１６３】
携帯電話端末２００では、電源が投入されたとき、セキュリティプログラム１０８を起動し、この操作キーパターンのキー操作を受け付けて判定する判定部を含み、判定部で操作キーパターンの操作を受け付けたことが確認されたときに、解除部２３８に保護処置を解除させる。また、この時、携帯電話端末２００からＡＳＰ１００に対し、保護処置が解除されたことを通知する解除通知メールを送信し、ＡＳＰ１００では、解除通知メールを受信し、ユーザ情報テーブル１２２の当該携帯電話端末２００の処置フラグ１２４をオフする。
【０１６４】
この構成によれば、手元に戻ってきた携帯電話端末２００を、ＡＳＰ１００にアクセスしなくとも、即刻使用可能とすることができるので、使い勝手が向上する。
【０１６５】
また、上記実施の形態において、携帯電話端末２００に保護指示および解除指示をＡＳＰ１００から行う方法は、処置フラグ１２４、指示メール、電話などによってそれぞれ行われたが、これらは組み合わせることが可能であり、状況に応じて選択して用いることも

できる。
【図面の簡単な説明】
【０１６６】
【図１】本発明の実施の形態に係るセキュリティシステムの構成を示すブロック図である。
【図２】図１のセキュリティシステムにおける携帯電話端末の構成を示すブロック図である。
【図３】図１のセキュリティシステムの概略機能ブロック図である。
【図４】図３のセキュリティシステムのＡＳＰの管理情報データベースのユーザ情報テーブルの構造の一例を示す図である。
【図５】図３のセキュリティシステムのＡＳＰの管理情報データベースのユーザ情報テーブルの構造の他の一例を示す図である。
【図６】図３のセキュリティシステムの携帯電話端末の部分ブロック図である。
【図７】図３のセキュリティシステムの携帯電話端末の動作の一例を示すフローチャートである。
【図８】図３のセキュリティシステムの動作の一例を示すフローチャートである。
【図９】本発明の実施の形態に係るセキュリティシステムの構成を示すブロック図である。
【図１０】図９のセキュリティシステムの動作の一例を示すフローチャートである。
【図１１】本発明の実施の形態に係るセキュリティシステムの構成を示すブロック図である。
【図１２】図１１のセキュリティシステムの携帯電話端末の動作の一例を示すフローチャートである。
【図１３】図１１のセキュリティシステムの動作の一例を示すフローチャートである。
【図１４】本発明の実施の形態に係るセキュリティシステムの構成を示すブロック図である。
【図１５】図１４のセキュリティシステムのＡＳＰおよび携帯電話端末の番号記憶部の構造の一例を示す図である。
【図１６】図１４のセキュリティシステムの動作の一例を示すフローチャートである。
【図１７】本発明の実施の形態に係るセキュリティシステムのＡＳＰの構成を示すブロック図である。
【図１８】本発明の実施の形態に係るセキュリティシステムのＡＳＰの構成を示すブロック図である。
【図１９】本発明のセキュリティシステムのＡＳＰおよび携帯電話端末の番号記憶部の構造の他の例を示す図である。
【符号の説明】
【０１６７】
１０　通信端末装置
２０　電話機
３０　ユーザ
１００　ＡＳＰ
１０２　通信部
１０４　Ｗｅｂページ提供部
１０６　プログラム記憶部
１０８　セキュリティプログラム
１１０　管理情報データベース
１１２　メール送受信部
１１４　通信部
１１６　ＩＶＲ
１１８　制御部

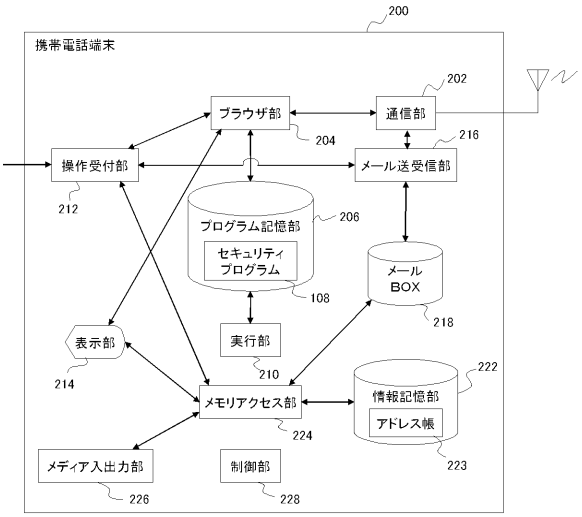
１２０　指示受付部
１２２　ユーザ情報テーブル
１２４　処置フラグ
１２６　認証部
１２８　判断部
１３０　指示提示部
１３２　ユーザ情報テーブル
１３４　処置フラグ
１３５　処置フラグ
１４０　通知部
１４２　メール送受信部
１４４　通知部
１５０　通知部
１５２　発信部
１５４　番号記憶部
１５６　発信番号テーブル
１６０　管理情報データベース
１６２　ユーザ履歴情報記憶部
１６４　サービス契約履歴
１６５　保護処置履歴
１６６　記録部
１６８　履歴提示部
１７０　契約期間集計部
１７２　処置期間集計部
１７４　課金部
１８０　発信番号テーブル
２００　携帯電話端末
２０２　通信部
２０４　ブラウザ部
２０６　プログラム記憶部
２１０　実行部
２１２　操作受付部
２１４　表示部
２１６　メール送受信部
２１８　メールボックス
２２２　情報記憶部
２２３　アドレス帳
２２４　メモリアクセス部
２２６　メディア入出力部
２２８　制御部
２３０　指示参照部
２３２　判定部
２３４　保護部
２３６　保護フラグ
２３８　解除部
２３９　自動起動部
２４０　解読部
２４２　判定部
２４４　解読部
２４６　判定部

２５０　着信部
２５２　番号記憶部
２５４　判定部
２５６　着信番号テーブル
２６０　着信番号テーブル

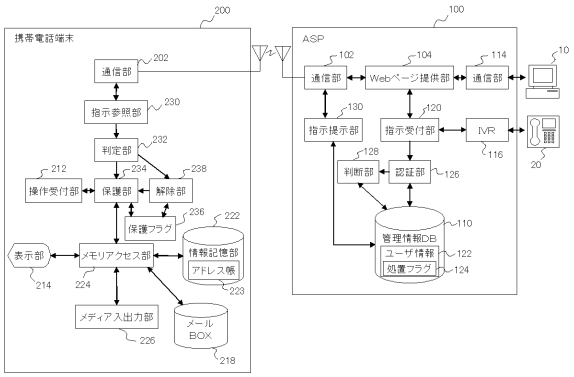
【図１】



【図２】



【図３】



【図４】

122 ユーザ情報テーブル　　124

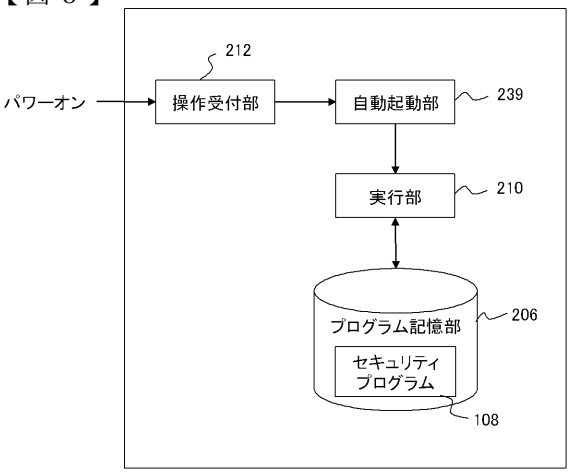
ユーザID	パスワード	処置フラグ
090－××××－××××	＊＊＊＊＊＊	1
080－××××－××××	＊＊＊＊＊＊	0
090－××××－××××	＊＊＊＊＊＊	0
⋮	⋮	⋮

【図５】

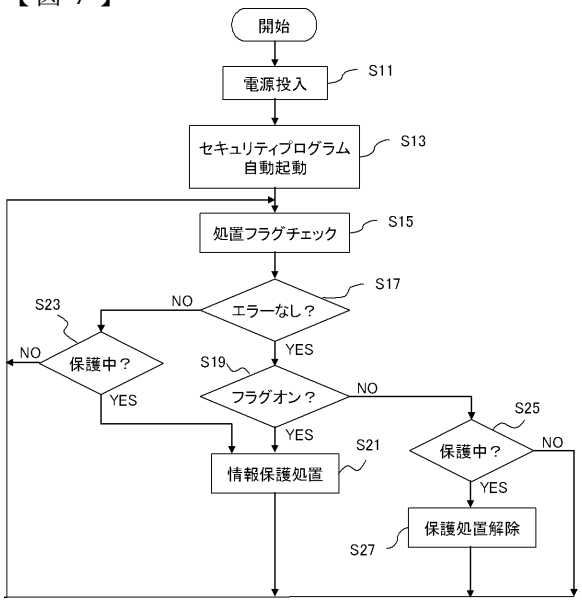
132 ユーザ情報テーブル　　134　　135

ユーザID	パスワード	レベル1 処置フラグ	レベル2 処置フラグ
090－××××－××××	＊＊＊＊＊＊	1	0
080－××××－××××	＊＊＊＊＊＊	0	1
090－××××－××××	＊＊＊＊＊＊	0	0
⋮	⋮	⋮	

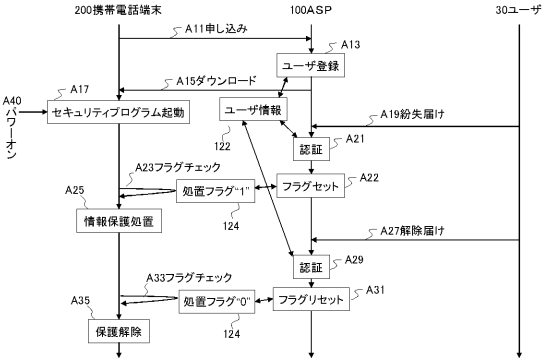
【図６】



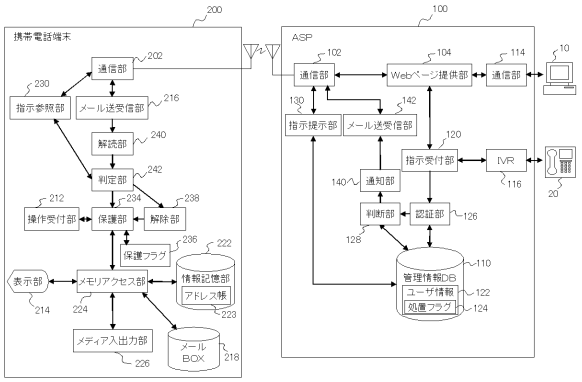
【図７】


開始
電源投入
S11
セキュリティプログラム
自動起動
S13
処置フラグチェック
S15
エラーなし？
S17
NO
YES
S23
保護中？
NO
YES
S19
フラグオン？
NO
YES
S25
保護中？
NO
YES
S21
情報保護処置
保護処置解除
S27

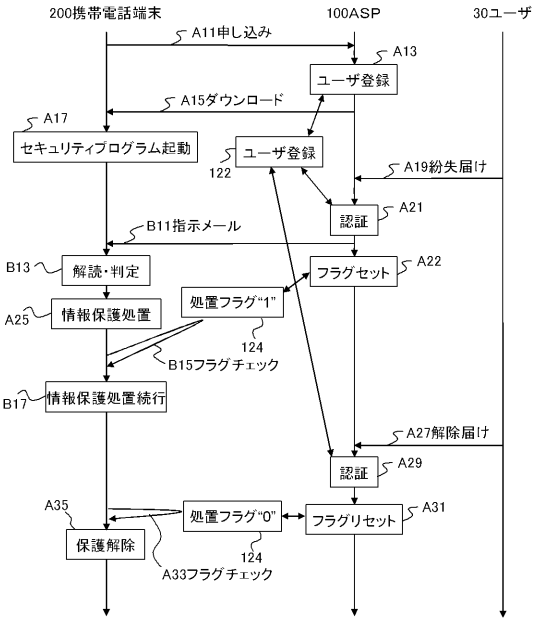
【図８】


200携帯電話端末
100ASP
30ユーザ
A11申し込み
A13
ユーザ登録
A15ダウンロード
A17
セキュリティプログラム起動
ユーザ情報
A19紛失届け
A40
パワーオン
122
認証
A21
A23フラグチェック
処置フラグ"1"
フラグセット
A22
A25
情報保護処置
124
A27解除届け
認証
A29
A33フラグチェック
処置フラグ"0"
フラグリセット
A31
A35
保護解除
124

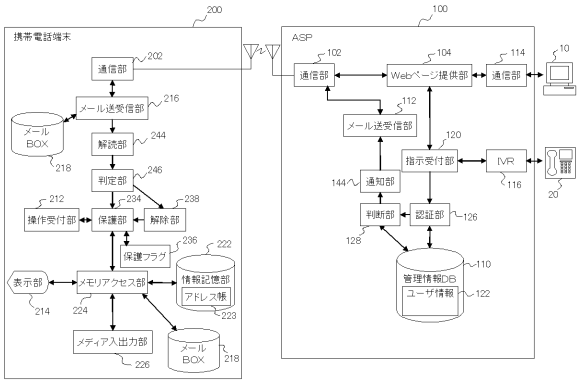
【図９】


200
携帯電話端末
通信部
202
指示参照部
230
メール送受信部
216
解読部
240
判定部
242
操作受付部
212
保護部
234
解除部
238
保護フラグ
236
222
表示部
214
メモリアクセス部
224
情報記憶部
アドレス帳
223
メディア入出力部
226
メール
BOX
218
100
ASP
通信部
102
Webページ提供部
104
通信部
114
10
130
指示提示部
メール送受信部
142
120
指示受付部
IVR
116
20
140
通知部
判断部
128
認証部
126
管理情報DB
110
ユーザ情報
122
処置フラグ
124

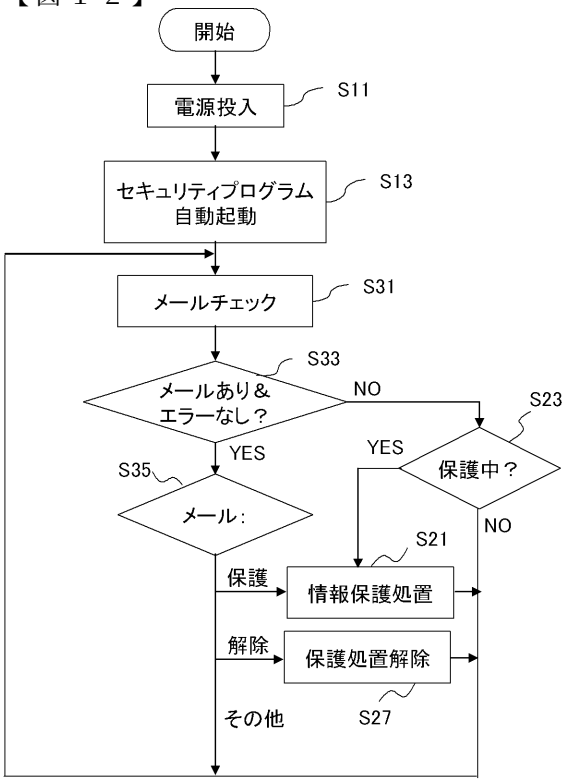
【図１０】


200携帯電話端末
100ASP
30ユーザ
A11申し込み
A13
ユーザ登録
A15ダウンロード
A17
セキュリティプログラム起動
ユーザ登録
122
A19紛失届け
認証
A21
B11指示メール
B13
解読・判定
フラグセット
A22
A25
情報保護処置
処置フラグ"1"
124
B15フラグチェック
B17
情報保護処置続行
A27解除届け
認証
A29
A35
処置フラグ"0"
フラグリセット
A31
保護解除
124
A33フラグチェック

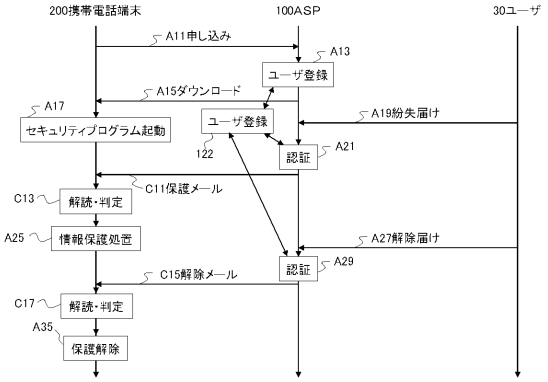
【図１１】



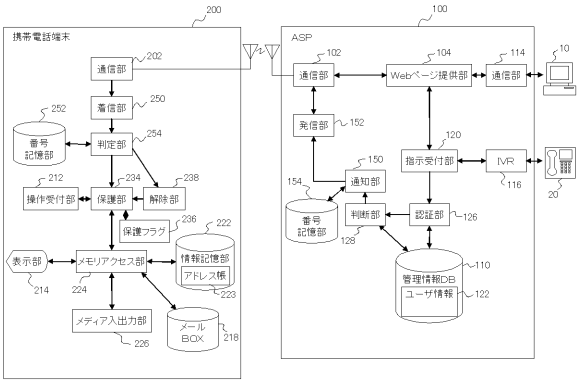
【図１２】



【図１３】



【図１４】



【図１５】

(a)

156発信番号テーブル

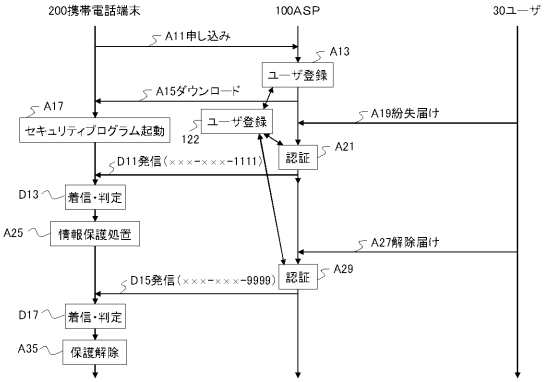
通知	発信電話番号
保護	×××－×××－1111
解除	×××－×××－9999

(b)

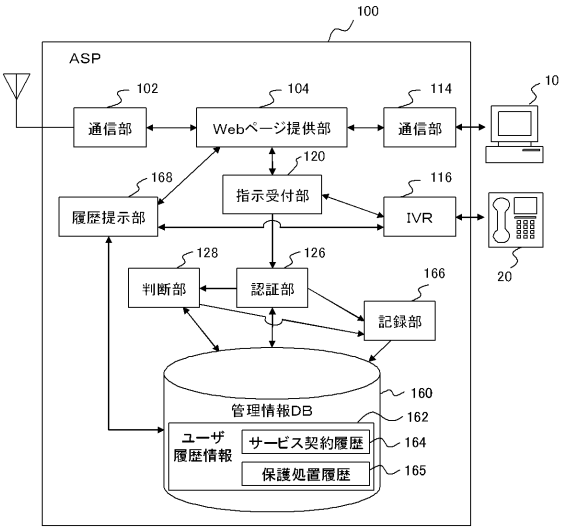
256着信番号テーブル

着信電話番号	通知
×××－×××－1111	保護
×××－×××－9999	解除

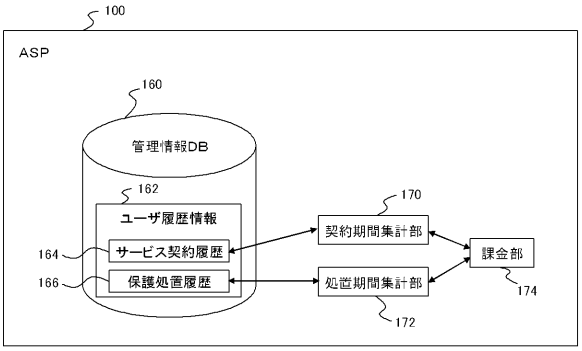
【図１６】



【図１７】



【図１８】



【図１９】

（a）

180発信番号テーブル

通知	発信電話番号
保護レベル1	×××－×××－1111
保護レベル2	×××－×××－2222
解除	×××－×××－9999

（b）

260着信番号テーブル

着信電話番号	通知
×××－×××－1111	保護レベル1
×××－×××－2222	保護レベル2
×××－×××－9999	解除

フロントページの続き

(72)発明者　中橋　修
東京都港区三田一丁目４番２８号　日本電気通信システム株式会社内
(72)発明者　上野　公雄
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考) 5K027 AA11 BB09
5K067 AA30 BB04 BB21 DD17 DD27 DD51 EE02 EE10 EE16 FF04
FF05 HH21