携帯型情報機器におけるセキュリティ機能

4L－13

赤外線鍵利用のアクセス制御方式/ファイル暗号化方式

古川 博† 大手 一郎† 壱岐 和男†† 鷲見浩明†††

(株)日立製作所 システム開発研究所†／オフィスシステム事業部†† 日立中部ソフトウェア(株)†††

1. はじめに

近年、ノートPCを中心とした携帯型情報機器の普及により、一般ユーザがこうした携帯型情報機器を使用する頻度が増え、活用範囲も広がってきている。こうした中、持ち運び可能な携帯型情報機器のセキュリティ機能は、重要な開発課題である。[1]

本稿では、携帯型情報機器の盗難・紛失による個人/機密情報の漏洩を防止するためのセキュリティ機能について提案する。

2. セキュリティ要件

携帯型情報機器に必要なセキュリティの内、今回特に以下の点について検討した。

（1）ユーザ認証

携帯型情報機器は小型であるため、他の情報機器と比べても、盗難・紛失に遭う可能性は高い。また不特定多数の外部の人間が存在する環境で使用することも多く、第三者にデータを盗まれる可能性は高い。このため現在、キーボードからのパスワード入力でユーザ認証を行うのが一般的である。

しかしパスワードは、正当な所有者以外でも入力することができ、パスワード入力を繰り返す内にセキュリティを破られる可能性を秘めている。

そこでパスワードに代わり、物理的なプロテクト可能な物理鍵によるユーザ認証の方式について検討した。その結果、機器本体には特別なハードウェア機構を設けずに上記問題を解決可能な、本赤外線鍵利用のアクセス制御方式を採用した。

（2）データの保護

所有者離席時などに機器が第三者によりアクセスされる場合を考え、機器上のデータであるファイルをユーザ単位で、機器本体のユーザ認証と共に二重に保護する必要がある。上記保護には暗号鍵を使ったファイル暗号を使用するのが一般的である。

しかし現在、携帯型情報機器に使用されているファイル暗号では、ファイル単位で暗号化を行い、暗号ファイルや暗号鍵の管理はユーザに任されているものが多く、ファイル暗号/復号操作がユーザにとって非常に煩雑になっている。

そこで、ユーザが指定する暗号鍵毎に、暗号化したファイルを一元管理するファイル暗号化方式で、これらの問題を解決する。

3. 赤外線鍵利用のアクセス制御方式

3.1 赤外線鍵の実現方式

本方式は、最近の携帯型情報機器に標準的に装備されることが増えた赤外線入出力装置を使用し、赤外線データを発信する物理鍵としてユーザ認証を実現する。この物理鍵を赤外線鍵と呼ぶ。

赤外線鍵は本体に付属して提供され、データ発信機構と各鍵毎に異なる赤外線データのみを持つ装置であり、比較的安価で容易に作成可能である。ユーザ側では鍵内のデータは変更出来ない。またデータ発信機構内には、他のデバイスから入力したデータで機能しないように、本赤外線鍵からの信号であることを識別するための特殊なデータ転送方法を設ける。

一方本体側（ここではPCを例にするが）では、従来のパスワードと同じく赤外線鍵のデータを、CMOSなど電池バックアップされている不揮発性記憶領域に、ハッシュ関数で変換をかけあらかじめ登録しておく。そして赤外線鍵から入力され

The function of security for portable computer system.

Hiroshi Furukawa† Ichiro Ote† Kazuo Iki†† Hiroaki Washimi†††

Systems Development Laboratory†, Office System Division††, Hitachi, Ltd. Hitachi Chubu Software, Ltd. †††

たデータは、PC起動処理プログラムBIOS上のユーザ認証部で前記登録データと判定でユーザ認証が実現される。

3.2 本方式での応用例

本方式の応用例を図1を用い説明する。通常の機器起動時は、鍵自体は本体と一緒に持ち歩かず、パスワードをキーボード入力し、上記入力をパスワード認証部で登録パスワードと判定しユーザ認証を行う。上記認証部では不正パスワードの入力回数をカウンタに記録しておき、特定回数以上の数値になると、不正パスワード回数チェック部によりパスワード無効フラグを立てる。パスワード無効フラグが立つと、機器起動時チェック部により何度機器の電源をONしようと機器の起動が行われないようになる。上記のパスワード無効状態を解除するには、あらかじめ機器内に登録してある赤外線データと同じデータの赤外線鍵を使用する。これで本体と鍵が同時に盗難に遭うこともなく、第三者によるデータ盗難を防ぐことが可能となる。

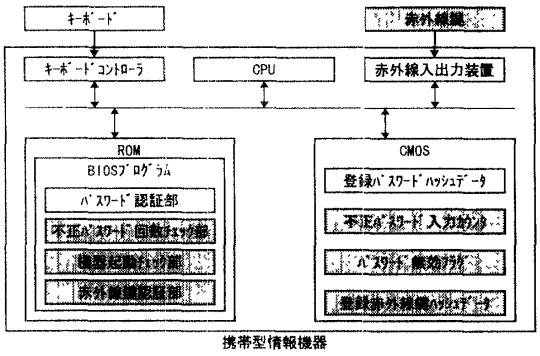

図1. 赤外線鍵によるパスワード無効状態解除構成

4. ファイル暗号化方式

本方式では、ユーザ毎に暗号情報を格納するためのディレクトリをディスク上に設ける。これらを暗号フォルダと呼ぶ。

暗号フォルダ下には、暗号化されたファイル、ハッシュ関数によって変換された認証パスワードを含むファイル、暗号ファイル/平文ファイル間の対応テーブルを含むファイルが、まとめて格納されており、これらはユーザから隠蔽されている。認証パスワードは暗号フォルダを作成するときにユーザによって設定され、暗号/復号操作の際に使用する暗号鍵を自動生成する。このためユーザは特に暗号鍵を意識する必要は無くなる。また、暗号フォルダには金庫をイメージしたアイコンが関連づけられている。

本方式での暗号化操作は、上記アイコンへのドラッグアンドドロップ操作と認証パスワードの入力により行われる。一方復号化操作は次の方法により実現する。上記アイコンをクリックし、ユーザにより正当な認証パスワードが入力されると、暗号ファイル/平文ファイル間対応テーブルを元に暗号化フォルダ下に存在する暗号ファイルを、平文ファイル名でリスト表示する。上記表示リストからファイルを選択し、復号操作を指示するとファイルが復号化する。

また、本方式では暗号フォルダ下に暗号/復号操作に必要な情報が存在するため、これらを1つのファイルに変換し、他機種に暗号ファイルをまとめて転送する機能も容易に実現可能である。

以上の暗号フォルダの構成を以下に示す。

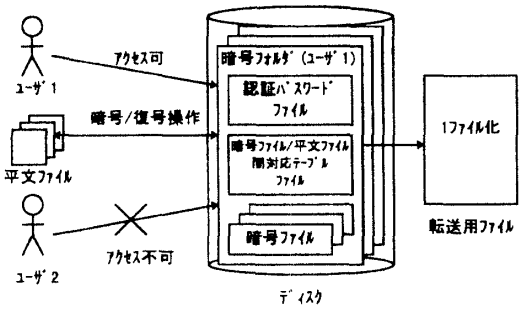

図2. 暗号フォルダの構成

5. おわりに

以上本稿では、携帯型情報機器に必要なセキュリティ機能とそのセキュリティを実現する二方式の概要についてを述べた。

今後は、本稿で述べた以外に必要なセキュリティ機能を検討し、研究開発を進めていく。

参考文献

[1]室伏　章郎,戦略的情報システム構築のための
インフォメーション・セキュリティ,
日経マグロウヒル社