(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4936967号
(P4936967)

(45)発行日　平成24年5月23日(2012.5.23)　(24)登録日　平成24年3月2日(2012.3.2)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601C
H04L	9/32	(2006.01)	H04L	9/00	601E
G06K	17/00	(2006.01)	H04L	9/00	673A
			G06K	17/00	T

請求項の数 14　(全 23 頁)

(21)出願番号　特願2007-106395 (P2007-106395)
(22)出願日　平成19年4月13日 (2007.4.13)
(65)公開番号　特開2008-263548 (P2008-263548A)
(43)公開日　平成20年10月30日 (2008.10.30)
審査請求日　平成22年1月20日 (2010.1.20)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100084618
弁理士　村松　貞男

最終頁に続く

(54)【発明の名称】通信端末装置、情報管理システムおよび情報管理方法

(57)【特許請求の範囲】
【請求項１】
第１の電子装置および第２の電子装置における情報を管理する情報管理システムであって、
前記第１の電子装置は、
外部からのアクセスが禁止されている記憶手段と、
前記第２の電子装置にも着脱可能な記憶媒体が着脱される第１のインターフェースと、
この第１のインターフェースによりアクセス可能な記憶媒体に、前記記憶手段に記憶されている復号化鍵に対応する暗号化鍵で暗号化されている暗号化データを書込む書込手段と、
前記書込手段により前記記憶媒体に書込んだ暗号化データを復号化するための前記記憶手段に記憶されている復号化鍵に基づいてパスワードを生成する第１の生成手段と、
この第１の生成手段により生成したパスワードを報知する報知手段と、を有し、
前記第２の電子装置は、
前記記憶媒体が着脱される第２のインターフェースと、
前記第１の電子装置の前記報知手段により報知されたパスワードが入力された場合、入力されたパスワードから前記記憶媒体に記憶されている暗号化データを復号化するための復号化鍵を生成する第２の生成手段と、
この第２の生成手段により生成された復号化鍵を用いて前記記憶媒体に記憶されている暗号化データを復号化する復号化手段と、を有する、

ことを特徴とする情報管理システム。
【請求項２】
前記第１の電子装置の前記第１の生成手段は、前記復号化鍵を元に発生させる乱数によりワンタイムパスワードを生成し、
前記前記第２の電子装置の前記第２の生成手段は、前記第１の生成手段により生成されたワンタイムパスワードに基づいて前記復号化鍵を生成する、
ことを特徴とする前記請求項１に記載の情報管理システム。
【請求項３】
前記第１の電子装置の前記書込手段は、コンテンツ鍵により暗号化されたコンテンツと、前記暗号化鍵により暗号化されたコンテンツ鍵と前記記憶媒体に書込み、
前記第２の電子装置は、
さらに、前記パスワードを解析する解析手段を有し、
前記第２の生成手段は、前記解析手段による入力されたパスワードの解析結果と前記記憶媒体に記憶されている暗号化されたコンテンツ鍵とに基づいて、暗号化されたコンテンツを復号化するためのコンテンツ鍵を生成し、
前記復号化手段は、前記第２の生成手段により生成されたコンテンツ鍵により前記記憶媒体に記憶されている暗号化されたコンテンツを復号化する、
ことを特徴とする前記請求項１又は２に記載の情報管理システム。
【請求項４】
前記第１の電子装置は、
さらに、耐タンパー性のメモリを有するＩＣカードが装着されるＩＣカードインターフェースを有し、
前記記憶手段は、前記ＩＣカードに設けられている耐タンパー性のメモリである、
ことを特徴とする前記請求項１乃至３に記憶の情報管理システム。
【請求項５】
種々のデータをダウンロードする機能を有する通信端末装置であって、
復号化鍵を記憶するＩＣカードが装着されるＩＣカードインターフェースと、
当該通信端末装置以外の電子装置にも着脱可能な記憶媒体を着脱するための記憶媒体インターフェースと、
前記ＩＣカードインターフェースに装着されているＩＣカードに記憶されている復号化鍵に対応する暗号化鍵により暗号化されている暗号化データを外部からダウンロードする通信手段と、
前記通信手段により外部からダウンロードした暗号化データを前記記憶媒体インターフェースによりアクセス可能な記憶媒体に書込む書込手段と、
前記ＩＣカードに記憶されている復号化鍵に基づいて、前記記憶媒体に書込まれている暗号化データを当該携帯端末装置以外の電子装置で利用するためのパスワードを生成する生成手段と、
この生成手段により生成したパスワードを報知する報知手段と、
を有することを特徴とする通信端末装置。
【請求項６】
前記生成手段は、前記ＩＣカードに記憶されている復号化鍵を元に発生される乱数によりワンタイムパスワードをパスワードとして生成する、
ことを特徴とする前記請求項５に記載の通信端末装置。
【請求項７】
前記通信手段は、コンテンツ鍵により暗号化されたコンテンツと前記ＩＣカードに記憶されている復号化鍵と対応する暗号化鍵により暗号化された前記コンテンツ鍵とを外部からダウンロードし、
前記書込手段は、前記コンテンツ鍵により暗号化されたコンテンツと、前記ＩＣカードに記憶されている復号化鍵と対応する暗号化鍵により暗号化されたコンテンツ鍵とを前記記憶媒体インターフェースにより前記記憶媒体に書込む、

ことを特徴とする前記請求項５又は６に記載の通信端末装置。
【請求項８】
前記ＩＣカードインターフェースに装着される前記ＩＣカードは、前記復号化鍵を記憶する耐タンパー性のメモリを有する、
ことを特徴とする前記請求項５乃至７に記載の通信端末装置。
【請求項９】
第１の電子装置および第２の電子装置における情報を管理する情報管理方法であって、
前記第１の電子装置は、
前記第１の電子装置および前記第２の電子装置に着脱可能な記憶媒体に、外部からのアクセスが禁止されている記憶手段に記憶されている復号化鍵に対応する暗号化鍵で暗号化された暗号化データを書込み、
前記記憶媒体に書込まれた暗号化データを復号化するための前記記憶手段に記憶されている復号化鍵に基づいてパスワードを生成し、
この生成したパスワードを報知し、
前記第２の電子装置は、
前記第１の電子装置により報知されたパスワードが入力された場合、入力されたパスワードに基づいて前記記憶媒体に記憶されている暗号化データを復号化するための復号化鍵を生成し、
前記パスワードに基づいて生成された復号化鍵を用いて前記記憶媒体に記憶されている暗号化データを復号化する、
ことを特徴とする情報管理方法。
【請求項１０】
前記第１の電子装置は、前記パスワードとして、前記復号化鍵を元に発生される乱数によりワンタイムパスワードを生成し、
前記前記第２の電子装置は、前記第１の電子装置で生成されたワンタイムパスワードに基づいて前記記憶媒体に記憶されている暗号化データを復号化するための復号化鍵を生成する、
ことを特徴とする前記請求項９に記載の情報管理方法。
【請求項１１】
前記第１の電子装置は、暗号化データとして、コンテンツ鍵により暗号化されたコンテンツと、前記復号化鍵に対応する暗号化鍵により暗号化されたコンテンツ鍵とを記憶媒体に書込み、
前記第２の電子装置は、前記入力されたパスワードを解析し、前記入力されたパスワードの解析結果と前記記憶媒体に記憶されている暗号化されたコンテンツ鍵とに基づいてコンテンツ鍵を生成し、生成されたコンテンツ鍵により暗号化されたコンテンツを復号化する、
ことを特徴とする前記請求項９又は１０に記載の情報管理方法。
【請求項１２】
種々のデータを外部からダウンロードする機能を有する通信端末装置に用いられる情報管理方法であって、
当該通信端末装置に装着されているＩＣカードに外部からのアクセスを禁止した状態で記憶されている復号化鍵に対応する暗号化鍵で暗号化された暗号化データを外部からダウンロードし、
前記外部からダウンロードした暗号化データを当該通信端末装置および当該通信端末装置以外の電子装置に着脱可能な記憶媒体に書込み、
前記記憶媒体に書込んだ暗号化データを復号化するための前記ＩＣカードに記憶されている復号化鍵に基づいて、前記記憶媒体に書込まれている暗号化データを当該通信端末装置以外の電子装置で利用するためのパスワードを生成し、
この生成したパスワードを報知する、
を有することを特徴とする情報管理方法。

【請求項１３】
前記パスワードは、前記ＩＣカードに記憶されている復号化鍵を元に発生される乱数により生成されるワンタイムパスワードである、
ことを特徴とする前記請求項１２に記載の情報管理方法。
【請求項１４】
前記外部からダウンロードして前記記憶媒体に書込まれる暗号化データは、コンテンツ鍵により暗号化されたコンテンツと前記ＩＣカードに記憶されている復号化鍵に対応する暗号化鍵により暗号化された前記コンテンツ鍵タである、
ことを特徴とする前記請求項１２又は１３に記載の情報管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、たとえば、外部のサーバからコンテンツをダウンロードするための通信機能を有する携帯電話機などの通信端末装置、および、上記電子装置が保存したデータを別の電子装置で利用するための情報管理システム、および、情報管理方法などに関する。
【背景技術】
【０００２】
従来、欧州を始め海外の多くの国では、携帯電話システム方式として、ＧＳＭ（Ｇｌｏｂａｌ Ｓｙｓｔｅｍ ｆｏｒ Ｍｏｂｉｌｅ ｃｏｍｍｕｎｉｃａｔｉｏｎｓ）方式が存在している。ＧＳＭ方式においては、携帯電話機内にＩＣカードの一種であるＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ Ｉｄｅｎｔｉｔｉｙ Ｍｏｄｕｌｅ）カードを装着することが必須となっている。日本では、従来、ＳＩＭカードを必要としないＰＤＣ（Ｐｅｒｓｏｎａｌ Ｄｉｇｉｔａｌ Ｃｅｌｌｕｌａｒ）方式の携帯電話システムが存在している。近年、日本を始め、欧州などの地域では、３ＧＰＰ（３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ）規格を採用した携帯電話システムが普及してきている。３ＧＰＰ規格では、ＳＩＭカードのように、ＵＳＩＭ（Ｕｎｉｖｅｒｓａｌ ｄｅｎｔｉｔｉｙ Ｍｏｄｕｌｅ）カードと呼ばれるＩＣカードを携帯電話機に装着することが必須となっている。
【０００３】
上記ＧＳＭあるいは３ＧＰＰで使用されるＳＩＭカードあるいはＵＳＩＭカードは、携帯電話機に装着されるＩＣカードである。ＳＩＭカードあるいはＵＳＩＭカードには、通信事業者の通信ネットワークに接続するのに必要な鍵情報、暗号アルゴリズム、各種ネットワークパラメータなどが記録されている。このような携帯電話機では、ＳＩＭカードあるいはＵＳＩＭカードに記憶されている情報を通信事業者のＯＴＡ（Ｏｖｅｒ Ｔｈｅ Ａｉｒ）サーバ、認証サーバあるいは管理サーバなどに送信し、これらのサーバと認証を行う。上記サーバとの認証が成功した携帯電話機は、当該通信事業者の通信サービスを受ることが可能となる。
【０００４】
上記３ＧＰＰ規格の携帯電話機では、無線通信網を介してダウンロードしたコンテンツなどのデータを携帯電話機の内部メモリあるいは当該携帯電話機に装着されたメモリデバイスに記憶することができるようになっている。また、上記３ＧＰＰ規格の携帯電話システムでは、高速かつ大容量のデータ通信が可能となっているため、様々なコンテンツビジネスが出現してきている。たとえば、音楽データ配信、映像データ配信あるいは電子書籍の配信等のコンテンツビジネスが出現してきている。このようなコンテンツビジネスでは、大容量のコンテンツデータがネットワークを通じ、携帯電話機、パソコンあるいはＰＤＡといった電子装置にダウンロードされる。ユーザ側からは、これらの大容量のコンテンツをいつでも、どこでも利用したいとの要望がある。
【０００５】
ところが、これらの大容量のコンテンツは、コピー等が簡単に行われないように、著作権保護などをセキュリティ保護が施されていることが多い。これは、コンテンツに施され

たセキュリティを見破られた場合、電子化されたコンテンツは、広く違法に配布される可能性があるためである。このため、上記のようなコンテンツ（特に、著作権などの保護が必要なコンテンツ）は、当該コンテンツをダウンロードした電子装置以外の電子装置で容易に利用することはできない。

【０００６】

たとえば、セキュリティが施された状態で携帯電話機に配信されたコンテンツは、携帯電話機以外の機器では利用不可であったり、携帯電話機以外の機器で利用するために煩雑な作業が必要となったりしている。従来、ＳＩＭカードあるいはＵＳＩＭカードが装着されていない携帯電話機では、アプリケーションあるいはコンテンツ本体にセキュリティをかける方法でセキュリティを保っている。また、ＧＳＭあるいは３ＧＰＰ規格のシステムでは、携帯電話機に装着されているＳＩＭカードあるいはＵＳＩＭカードにセキュリティ保護の為の機能を持たせていることも多い。

【０００７】

上記のように、携帯電話機本体内あるいは携帯電話機に装着されているＳＩＭカードあるいはＵＳＩＭカードにコンテンツのセキュリティ保護の機能を完全に閉じ込めてしまうと、ユーザ本人が使用する場合であっても、当該携帯電話機以外の電子装置では、それらのコンテンツを利用できないという問題がある。

【特許文献１】特開２００４－１３３８４８号公報

【発明の開示】

【発明が解決しようとする課題】

【０００８】

この発明の一形態は、上記のような問題を解決するものであり、ネットワーク経由で配信されるデータのセキュリティを向上させることができ、通信端末装置などの電子装置内でセキュリティが確保されているデータの利便性を向上させることができる情報管理システム、通信端末装置および情報管理方法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】

【０００９】

この発明の一形態としての情報管理システムは、第１の電子装置および第２の電子装置における情報を管理するものであって、前記第１の電子装置は、外部からのアクセスが禁止されている記憶手段と、前記第２の電子装置にも着脱可能な記憶媒体が着脱される第１のインターフェースと、この第１のインターフェースによりアクセス可能な記憶媒体に、前記記憶手段に記憶されている復号化鍵に対応する暗号化鍵で暗号化されている暗号化データを書込む書込手段と、前記書込手段により前記記憶媒体に書込んだ暗号化データを復号化するための前記記憶手段に記憶されている復号化鍵に基づいてパスワードを生成する第１の生成手段と、この第１の生成手段により生成したパスワードを報知する報知手段と、を有し、前記第２の電子装置は、前記記憶媒体が着脱される第２のインターフェースと、前記第１の電子装置の前記報知手段により報知されたパスワードが入力された場合、入力されたパスワードから前記記憶媒体に記憶されている暗号化データを復号化するための復号化鍵を生成する第２の生成手段と、この第２の生成手段により生成された復号化鍵を用いて前記記憶媒体に記憶されている暗号化データを復号化する復号化手段とを有する。

【００１０】

この発明の一形態としての通信端末装置は、種々のデータをダウンロードする機能を有するものであって、復号化鍵を記憶するＩＣカードが装着されるＩＣカードインターフェースと、当該通信端末装置以外の電子装置にも着脱可能な記憶媒体を着脱するための記憶媒体インターフェースと、前記ＩＣカードインターフェースに装着されているＩＣカードに記憶されている復号化鍵に対応する暗号化鍵により暗号化されている暗号化データを外部からダウンロードする通信手段と、前記通信手段により外部からダウンロードした暗号化データを前記記憶媒体インターフェースによりアクセス可能な記憶媒体に書込む書込手段と、前記ＩＣカードに記憶されている復号化鍵に基づいて、前記記憶媒体に書込まれている暗号化データを当該携帯端末装置以外の電子装置で利用するためのパスワードを生成

する生成手段と、この生成手段により生成したパスワードを報知する報知手段とを有する。

【００１１】

この発明の一形態としての情報管理方法は、第１の電子装置および第２の電子装置における情報を管理する方法であって、前記第１の電子装置は、前記第１の電子装置および前記第２の電子装置に着脱可能な記憶媒体に、外部からのアクセスが禁止されている記憶手段に記憶されている復号化鍵に対応する暗号化鍵で暗号化された暗号化データを書込み、前記記憶媒体に書込まれた暗号化データを復号化するための前記記憶手段に記憶されている復号化鍵に基づいてパスワードを生成し、この生成したパスワードを報知し、前記第２の電子装置は、前記第１の電子装置により報知されたパスワードが入力された場合、入力されたパスワードに基づいて前記記憶媒体に記憶されている暗号化データを復号化するための復号化鍵を生成し、前記パスワードに基づいて生成された復号化鍵を用いて前記記憶媒体に記憶されている暗号化データを復号化する。

【００１２】

この発明の一形態としての情報管理方法は、種々のデータを外部からダウンロードする機能を有する通信端末装置に用いられる方法であって、当該通信端末装置に装着されているＩＣカードに外部からのアクセスを禁止した状態で記憶されている復号化鍵に対応する暗号化鍵で暗号化された暗号化データを外部からダウンロードし、前記外部からダウンロードした暗号化データを当該通信端末装置および当該通信端末装置以外の電子装置に着脱可能な記憶媒体に書込み、前記記憶媒体に書込んだ暗号化データを復号化するための前記ＩＣカードに記憶されている復号化鍵に基づいて、前記記憶媒体に書込まれている暗号化データを当該通信端末装置以外の電子装置で利用するためのパスワードを生成し、この生成したパスワードを報知する。

【発明の効果】

【００１３】

この発明の一形態によれば、ネットワーク経由で配信されるデータのセキュリティを向上させることができ、通信端末装置などの電子装置内でセキュリティが確保されているデータの利便性を向上させることができる情報管理システム、通信端末装置および情報管理方法を提供できる。

【発明を実施するための最良の形態】

【００１４】

以下、この発明を実施するための最良の形態について図面を参照しつつ説明する。

図１は、この発明の実施の形態に係る情報管理システムの構成例の概要を示す図である。

図１に示すように、情報管理システムでは、ＩＣカードＣを装着した通信端末装置としての携帯電話機（第１の電子装置）１１と通信事業者システム（通信ネットワーク）２０とが通信を行うようになっている。また、上記携帯電話機１１には、記憶媒体としてのメモリデバイスＭが着脱可能となっている。上記メモリデバイスＭは、たとえば、メモリカードなどが想定される。上記メモリデバイスＭは、パーソナルコンピュータ（以下、単にパソコンと称する）１２などの携帯電話機以外の電子装置（第２の電子装置）にも着脱可能な仕様となっているものとする。

【００１５】

また、上記携帯電話機１１は、ＩＣカードＣが装着されるようになっている。上記携帯電話機１１は、上記ＩＣカードＣが装着された状態で通信事業者システム（通信ネットワーク）との通信（音声通話、データ通信など）を行うようになっている。すなわち、上記携帯電話機１１は、上記ＩＣカードＣを装着した状態で携帯電話として利用可能となっている。

【００１６】

上記ＩＣカードＣは、ＬＳＩ（制御素子）、各種メモリ（ワーキングメモリ、プログラムメモリ、書換え可能な不揮発性メモリ）、および、インターフェースなどを有する。た

とえば、上記ＩＣカードＣは、たとえば、ＵＳＩＭ、あるいは、ＳＩＭなどと称される携帯電話機１１用のＩＣカードである。上記ＩＣカードＣでは、制御素子が、ワーキングメモリを使用してプログラムメモリあるいは不揮発性メモリに記憶されている種々の制御プログラムを実行することにより種々の機能を実現している。

【００１７】

たとえば、上記ＩＣカードＣは、携帯電話機（端末機器）１１との相互認証機能、通信事業者システム２０との相互認証機能、あるいは、携帯電話機１１内の各種モジュールとの相互認証機能などを有している。上記ＩＣカードＣでは、認証用のプログラムを実行することにより、認証用のデータを用いて各種の認証処理を行うようになっている。たとえば、上記ＩＣカードＣは、上記通信事業者システム２０との通信を行うための認証用のデータが記憶されている。これにより、上記通信事業者システム２０との相互認証が成功した場合、上記ＩＣカードＣが装着されている携帯電話機１１は、通信事業者が提供するサービス（通話、および、データ通信など）が利用可能となるようになっている。

【００１８】

また、上記ＩＣカードＣでは、不揮発性メモリに、認証用のデータ、ユーザの個人情報、認証用の制御プログラムなどが記憶される。また、上記ＩＣカードＣの不揮発性メモリには、外部からダウンロードしたデータを使用するための認証用のデータなども記憶されている。また、上記ＩＣカードＣの不揮発性メモリの一部または全部は、耐タンパー性を有するメモリである。

【００１９】

また、上記携帯電話機１１は、上記メモリデバイスＭが着脱可能なインターフェースを有している。上記メモリデバイスＭは、上記携帯電話機１１に装着された状態において、データを保存する記憶媒体として機能する。たとえば、上記メモリデバイスＭには、上記携帯電話機１１が上記通信事業者システム２０を介して外部からダウンロードしたデータなどが記憶できるようになっている。

上記パソコン１２は、上記メモリデバイスＭが着脱可能となインターフェースを有している。たとえば、上記携帯電話機１１から取り外されたメモリデバイスＭは、上記パソコン１２のインターフェースに装着される形態が想定される。また、上記パソコン１２では、種々のアプリケーションをインストールすることにより種々の機能を実現するようになっている。

【００２０】

上記通信事業者システム２０は、通信設備２１、ＯＴＡ（Ｏｖｅｒ　Ｔｈｅ　Ａｉｒ）サーバ２２などを有している。上記通信設備２１は、上記携帯電話機１１との通信を行うための設備である。上記ＯＴＡサーバ２２は、上記通信設備２１を介して上記携帯電話機１１との通信を制御するためのサーバ装置である。

【００２１】

また、上記ＯＴＡサーバ２２は、携帯電話機１１（携帯電話機に装着されているＩＣカード）との認証を行う認証サーバとしても機能する。上記ＯＴＡサーバ２２は、当該装置全体を制御するための制御部、通信設備２１あるいは各サーバとの通信を行うための通信インターフェース、データを記憶するための記憶部などを有している。また、上記ＯＴＡサーバ２２は、携帯電話機１１あるいは携帯電話機１１に装着されるＩＣカードＣに関するデータ（認証データ）などを管理する管理サーバとしても機能するものとする。なお、認証サーバおよび管理サーバは上記ＯＴＡサーバとは別に設けるようにしても良い

また、上記通信事業者システム２０には、外部サーバとしてのコンテンツサーバ２５が接続されている。上記コンテンツサーバ２５は、通信事業者システム２０を介してコンテンツ（たとえば、画像データ、動画データ、電子書籍データなど）などを各ユーザの携帯電話機１１に提供するためのサーバ装置である。上記コンテンツサーバ２５は、当該装置全体を制御する制御部、上記ＯＴＡサーバ２２と通信するための通信インターフェース、コンテンツなどのデータを記憶するための記憶部などを有している。上記コンテンツサーバ２５は、上記ＯＴＡサーバ２２に接続され、上記ＯＴＡサーバ２２及び上記通信設備２

１を介して携帯電話機１１にコンテンツなどのサービスを提供するようになっている。
【００２２】
次に、上記携帯電話機１１の構成について詳細に説明する。
図２は、上記携帯電話機１１の構成例を示すブロック図である。
図２に示すように、携帯電話機１１は、制御部３１、ＲＡＭ３２、ＲＯＭ３３、不揮発性メモリ３４、ＩＣカードインターフェース３５、メモリデバイスインターフェース（第１のインターフェース）３６、アンテナ３７、通信部３８、音声部３９、振動部４０、表示部４１、操作部４２、電源部４３などを有している。
【００２３】
上記制御部３１は、携帯電話機１１全体の制御を司るものである。上記制御部３１は、ＣＰＵ、内部メモリ、各種のインターフェースなどを有している。また、上記制御部３１は、その基本機能として、上記表示部４１の表示を制御する表示制御機能、ＰＬＬ（Phase Locked Loop）回路、データストリーム経路切換え、ＤＭＡ（Direct Memory Access）コントローラ、割り込みコントローラ、タイマ、ＵＡＲＴ（Universal Asynchronous Receiver Transmitter）、秘匿、ＨＤＬＣ（High-level Data Link Control procedure）フレーミング、ディバイスコントローラなどの機能を有している。
【００２４】
上記ＲＡＭ３２は、作業用のデータを記憶するための揮発性メモリである。上記ＲＯＭ３３は、制御プログラムや制御データなどが記憶されている不揮発性メモリである。上記ＲＯＭ３３は、不揮発性メモリである。たとえば、上記ＲＯＭ３３には、当該携帯電話機１１の基本的な制御を行うための制御プログラムおよび制御データが予め記憶されている。すなわち、上記制御部３１は、上記ＲＯＭ３３に記憶されている制御プログラムを実行することにより、当該携帯電話機１１の基本的な制御を実現している。
【００２５】
上記不揮発性メモリ３４は、種々のデータが記憶される書き換え可能な不揮発性メモリである。上記不揮発性メモリ３４には、種々のアプリケーションプログラム（アプリケーション）、制御データ、および、ユーザデータなどが記憶される。たとえば、上記制御部３１は、上記不揮発性メモリ３４に記憶されているアプリケーションプログラムを実行することにより、種々の機能を実現するようになっている。
【００２６】
また、上記ＩＣカードインターフェース３５は、ＩＣカードＣが装着されるインターフェースである。上記ＩＣカードインターフェース３５は、上記制御部３１に接続されている。これにより、上記制御部３１は、上記ＩＣカードインターフェース３５を介して上記ＩＣカードＣとのデータ通信が可能となっている。
また、上記メモリデバイスインターフェース３６は、上記メモリデバイスＭが着脱可能なインターフェースである。上記メモリデバイスインターフェース３６は、上記制御部３１に接続されている。これにより、上記制御部３１は、上記メモリデバイスインターフェース３６に装着された上記メモリデバイスＭへのデータの保存および上記メモリデバイスＭからのデータの読出しが可能となっている。
【００２７】
上記通信部３８には、通信用のアンテナ３７が接続される。上記通信部３８は、上記アンテナ３７を介して通話データあるいはデータ通信用のデータを電波で送受信するものである。上記音声部３９は、アナログフロントエンド部及びオーディオ部を有し、音声の入出力を行うものである。上記音声部３９には、図示しないスピーカ、レシーバ、マイクなどが接続されている。上記振動部５０は、当該携帯電話機１１全体を振動させる振動機構により構成される。上記表示部４１は、たとえば、液晶表示装置などにより構成される。上記表示部４１は、上記制御部３１により表示のオンオフや表示内容などが制御されるようになっている。また、携帯電話機１１がシェル型などの形状である場合、上記表示部４１としては、筐体を開放した場合に現れるメインの表示部と筐体の背面に設けられるサブの表示部とから構成されるようにしても良い。上記操作部４２は、キーボードなどにより

構成され、ユーザによる操作指示が入力される。

【００２８】

上記電源部４３は、バッテリーなどにより構成され、当該携帯電話機１１内の各部に電源を供給するようになっている。また、上記電源部４３は、上記第１インターフェース３５を介して接続されたＩＣカードＣおよび上記第２インターフェース３６を介して接続されたメモリデバイスＭにも電源を供給する機能も有している。

【００２９】

次に、上記パソコン１２の構成について詳細に説明する。

図３は、上記パソコン１２の構成例を示すブロック図である。

図３に示すように、パソコン１２は、制御部５１、ＲＡＭ５２、ＲＯＭ５３、不揮発性メモリ５４、メモリデバイスインターフェース（第２のインターフェース）５５、表示部５６、音声部５７、操作部５８、外部インターフェース５９などを有している。

【００３０】

上記制御部５１は、パソコン１２全体の制御を司るものである。上記制御部５１は、ＣＰＵ、内部メモリ、各種のインターフェースなどを有している。上記ＲＡＭ５２は、作業用のデータを記憶するための揮発性メモリである。上記ＲＯＭ５３は、当該パソコン１２の基本的な動作を司る制御プログラムおよび制御データなどが予め記憶されている不揮発性メモリである。上記制御部５１は、上記ＲＯＭ５３に記憶されている制御プログラムを実行することにより、当該パソコン１２の基本的な制御を実現している。

【００３１】

上記不揮発性メモリ５４は、種々のデータが記憶される書き換え可能な不揮発性メモリである。上記不揮発性メモリ５４は、たとえば、ハードディスクドライブ（ＨＤＤ）、ＥＥＰＲＯＭ、フラッシュメモリなどの記憶デバイスが想定される。上記不揮発性メモリ５４には、種々のアプリケーションプログラム（アプリケーション）、制御データ、および、ユーザデータなどが記憶される。たとえば、上記制御部５１は、上記不揮発性メモリ５４に記憶されているアプリケーションプログラムを実行することにより、種々の機能を実現するようになっている。

【００３２】

上記メモリデバイスインターフェース５５は、メモリデバイスＭが着脱可能なインターフェースである。上記メモリデバイスインターフェース５５は、上記制御部５１に接続されている。これにより、上記制御部５１は、上記メモリデバイスインターフェース５５に装着された上記メモリデバイスＭからのデータの読出しおよび上記メモリデバイスＭへのデータの保存が可能となっている。

【００３３】

上記表示部５６は、情報を表示するための表示装置である。上記表示部５６は、たとえば、液晶表示装置などにより構成される。上記音声部５７は、音声の入出力を行うものである。上記表示部５６あるいは上記音声部５７は、ユーザに情報を提供するための報知手段として機能する。上記操作部５８は、キーボードなどにより構成され、ユーザによる操作指示が入力される。たとえば、上記操作部５８では、ユーザがパスワードなどを入力するために使用される。上記外部インターフェース５９は、外部機器とのデータ通信を行うためのインターフェースである。たとえば、上記外部インターフェース５９は、上記携帯電話機１１と通信回線を介して接続され、上記携帯電話機１１とのデータ通信を行う。

【００３４】

次に、上記コンテンツサーバ２５が提供するコンテンツの利用方法について概略的に説明する。

図４は、上記コンテンツサーバ２５が提供するコンテンツの利用方法を概略的に説明するための図である。

図４では、上記携帯電話機１１には、ＩＣカードＣとメモリデバイスＭとが挿入されているものとする。上記ＩＣカードＣには、耐タンパー性のメモリ（書換え可能な不揮発性メモリ）Ｃａを有している。上記ＩＣカードＣの耐タンパー性のメモリＣａには、セキュ

アに鍵データあるいは電子証明書などのデータを保存することが可能である。また、上記通信事業者システム２０では、携帯電話機１１と上記ＯＴＡサーバ２２とが上記通信設備２１を介して通信することにより相互認証し、相互認証が成功した携帯電話機１１による各種のサービスをＯＴＡサーバ２２が許可するようになっている。さらに、上記通信事業者システム２０の上記ＯＴＡサーバ２２は、上記コンテンツ１０１を提供しているコンテンツサーバ２５と接続されている。

【００３５】

上記コンテンツサーバ２５では、図示しない記憶部に携帯電話機１１へ提供可能なコンテンツ１０１とそのコンテンツ１０１に対応するコンテンツ鍵１０２を記憶している。また、上記コンテンツサーバ２５は、図示しない記憶部に上記コンテンツ１０１を携帯電話機１１以外の装置で利用するためのセキュリティアプリケーション１０３も記憶しているものとする。このセキュリティアプリケーション１０３は、上記携帯電話機１１からのダウンロード要求に応じて当該携帯電話機１１へ配信されるようになっている。

なお、上記セキュリティアプリケーション１０３は、予め上記携帯電話機１１にインストールされているようにしても良い。この場合、上記セキュリティアプリケーション１０３は、コンテンツサーバ２５で保存したり、ネットワーク経由で携帯電話機１１に配信したりしなくても良い。

【００３６】

上記コンテンツサーバ２５は、上記通信事業者システム２０を介して上記携帯電話機１１からのコンテンツのダウンロード要求に応じてコンテンツ１０１を配信する処理を行う。上記コンテンツを配信する処理において、上記コンテンツサーバ２５では、コンテンツ１０１を携帯電話機１１へ提供するために、コンテンツ鍵１０２により暗号化したコンテンツ（暗号化コンテンツ）２０２とコンテンツ鍵１０２とをＯＴＡサーバ２２へ供給する。なお、上記携帯電話機１１がコンテンツ１０１を利用するためのセキュリティアプリケーション１０３を有していない場合、上記コンテンツサーバ２５は、上記通信事業者システム２０を介してセキュリティアプリケーション１０３も携帯電話機１１へ配信するようになっている。

【００３７】

上記ＯＴＡサーバ２２では、コンテンツサーバ２５から供給された暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２を図示しない記憶部に保存する。また、上記ＯＴＡサーバ２２では、図示しない記憶部に暗号化鍵１０４および暗号化鍵１０４に対応する復号化鍵２０４を記憶しているものとする。上記暗号化鍵１０４と上記復号化鍵２０４とは対をなすペアのデータであり、上記暗号化鍵１０４により暗号化されたデータは、上記復号化鍵２０４を用いなければ復号化できないようになっている。また、上記暗号化鍵１０４は、上記ＯＴＡサーバ２２で管理するようにしても良いし、コンテンツサーバ２５で管理するようにしても良い。

【００３８】

すなわち、上記コンテンツ鍵１０２を暗号化するための暗号化鍵１０４は、上記ＯＴＡサーバ２２あるいは上記コンテンツサーバ２５などのコンテンツを配信する側のサーバで管理され、暗号化されたコンテンツ鍵１０２を復号化するための復号化鍵（または復号化鍵を導き出せる暗号化鍵）２０４は、携帯電話機１１で管理される。たとえば、上記携帯電話機１１では、当該携帯電話機１１に装着されているＩＣカードＣ内の耐タンパー性のメモリＣａに復号化鍵２０４を保存するようになっている。

【００３９】

また、上記復号化鍵２０４をＩＣカードＣのメモリＣａに格納する手法は、種々の携帯が適用可能である。たとえば、携帯電話機１１は、上記ＯＴＡサーバ２２あるいは上記コンテンツサーバ２５からコンテンツ（暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２）をダウンロードする際、復号化鍵２０４もダウンロードしてＩＣカードＣのメモリＣａに保存するようにしても良いし、上記ＯＴＡサーバ２２あるいは上記コンテンツサーバ２５で管理している暗号化鍵１０４に対応する復号化鍵２０４を携帯電話機１１に装

着されているＩＣカードＣのメモリＣａに予め保存しておくようにしても良い。

【００４０】

また、コンテンツ１０１を提供する事業者が通信事業者である場合、上記携帯電話機１１（あるいは携帯電話機１１に装着されているＩＣカードＣ）と通信事業者とが相互認証するための認証データを暗号化鍵１０４および復号化鍵２０４として用いるようにしても良い。この場合、携帯電話機１１は、当該携帯電話機１１が予め保持している認証データ（予めＩＣカードＣに設定されている認証データ）を復号化鍵２０４とし、通信事業者が管理している当該携帯電話機１１（当該携帯電話機１１に装着されているＩＣカードＣ）用の認証データを暗号化鍵として利用することが可能である。

【００４１】

なお、ここでは、コンテンツ１０１を配信する事業者と通信事業者システムを提供している事業者とが同一である場合（つまり、コンテンツサーバ２５と通信事業者システム２０とが同じ事業者により運用されている場合）を想定するものとする。このため、以下の説明では、上記暗号化鍵１０４および復号化鍵２０４は、上記ＯＴＡサーバ２２で管理されるものとする。

【００４２】

上記コンテンツ１０１を携帯電話機１１へ配信する場合、上記ＯＴＡサーバ２２では、コンテンツ鍵１０２を暗号化鍵１０４により暗号化する。上記コンテンツ鍵１０２を暗号化すると、上記ＯＴＡサーバ２２は、上記コンテンツ鍵１０２により暗号化された暗号化コンテンツ２０１、暗号化鍵１０４により暗号化した暗号化コンテンツ鍵２０２、および、暗号化コンテンツ鍵を復号化するための復号化鍵２０４を上記通信設備２１を介して携帯電話機１１へ配信する。

【００４３】

上記携帯電話機１１では、上記通信設備２１を介して上記ＯＴＡサーバ２２から暗号化コンテンツ２０１、暗号化コンテンツ鍵２０２および復号化鍵２０４をダウンロードする。上記携帯電話機１１では、ダウンロードした暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２をメモリデバイスＭに保存し、復号化鍵２０４をＩＣカードＣ内の耐タンパー性のメモリＣａに保存するものとする。

【００４４】

すなわち、ダウンロードした暗号化コンテンツ２０１は、暗号化コンテンツ鍵２０２と復号化鍵２０４とがなければ、復号化できない仕組みとなっている。ここで、上記携帯電話機１１において、ダウンロードしたコンテンツ自体に関する情報（暗号化コンテンツ２０１及び暗号化コンテンツ鍵２０２）の保存場所は、適宜選択可能であるが、復号化鍵２０４の保存場所は、耐タンパー性のメモリＣａに限定されているようになっている。これは、復号化鍵２０４のセキュリティ性（つまり、コンテンツ全体のセキュリティ性）を保つため仕様である。

【００４５】

一方、上記携帯電話機１１では、上記メモリデバイスＭの着脱が可能である。たとえば、上記携帯電話機１１から抜き取られたメモリデバイスＭは、パソコン１２等の携帯電話機１１以外の機器に装着することが可能である。メモリデバイスＭに保存したコンテンツを他の機器（たとえば、パソコン）で利用したい場合がある。たとえば、上記携帯電話機１１では、表示部の大きさなどに物理的な制限があるため、画像あるいは映像関連のコンテンツをパソコン１２などの大きな表示画面を有する表示部で閲覧したいと考えるユーザが多い。

【００４６】

上記のような要望に答えるため、上記携帯電話機１１には、メモリデバイスＭに保存したコンテンツをパソコン１２などの他の機器で利用可能とするためのセキュリティアプリケーション１０３がインストールされている。上記セキュリティアプリケーション１０３は、たとえば、上記通信事業者システム２０を介して上記コンテンツサーバ２５からダウンロードされる。また、上記セキュリティアプリケーション１０３は、予め携帯電話機１

１にインストールされているようにしても良い。
【００４７】
上記携帯電話機１１において上記セキュリティアプリケーション１０３を実行すると、上記携帯電話機１１では、上記ＩＣカードＣに記憶している復号化鍵２０４に基づいて乱数発生機能により発生させた乱数によりワンタイムパスワード１１１を発生させる。生成したワンタイムパスワード１１１は、上記携帯電話機１１の表示部４１に表示される。上記ワンタイムパスワード１１１は、上記コンテンツを当該携帯電話機１１以外の機器で利用するために必要なパスワードであり、１度だけ有効なパスワードである。すなわち、上記のようなシステムでは、携帯電話機１１がダウンロードしたコンテンツは上記ワンタイムパスワード１１１により携帯電話機１１以外の機器で１度だけ利用できるようになっている。
【００４８】
たとえば、ユーザが、上記携帯電話機１１からコンテンツが記憶されているメモリデバイスＭを取り外し、上記パソコン１２に装着したものとする。この状態において、ユーザは、上記パソコン１２の操作部５８によりワンタイムパスワード１１１を入力する。すると、上記パソコン１２の制御部５１は、コンテンツ利用アプリケーションにより入力されたワンタイムパスワード１１１を解析し、その解析結果から復号化鍵２０４を生成する。上記ワンタイムパスワード１１１から復号化鍵２０４を生成すると、上記パソコン１２の制御部５１は、生成した復号化鍵２０４を用いてメモリデバイスＭに記憶されている暗号化コンテンツ２０１を復号化する。これにより復号化が成功すれば（つまり、ユーザが入力したワンタイムパスワードが正しいものであれば）、上記パソコン１２では、上記メモリデバイスＭに記憶されているコンテンツ１０１が利用可能となる。
【００４９】
次に、上記コンテンツサーバ２５から携帯電話機１１へコンテンツを配信するプロセスについて詳細に説明する。
上記コンテンツサーバ２５が提供しているコンテンツ１０１を利用するユーザは、上記携帯電話機１１の操作部４２によりコンテンツ１０１のダウンロードを要求する操作を行う。すると、上記携帯電話機１１の制御部３１は、上記通信事業者システム２０を介して上記コンテンツサーバ２５へコンテンツ１０１のダウンロード要求を行う。この際、上記携帯電話機１１には、上記通信事業者システム２０との相互認証が成功しているＩＣカードＣとダウンロードするコンテンツ１０１を保存するためのメモリデバイスＭとが装着されているものとする。
【００５０】
上記携帯電話機１１からコンテンツ１０１のダウンロード要求を受けたコンテンツサーバ２５は、ダウンロードが要求されたコンテンツ１０１と当該コンテンツ１０１のコンテンツ鍵１０２とを図示しない記憶部から読み出す。なお、ここで、コンテンツサーバ２５が記憶部から読み出すコンテンツ１０１およびコンテンツ鍵１０２は、暗号化される前の状態である。コンテンツ１０１とコンテンツ鍵１０２とを読み出すと、上記コンテンツサーバ２５は、コンテンツ１０１をコンテンツ鍵１０２により暗号化することにより、暗号化コンテンツ２０１を生成する。暗号化コンテンツ２０１を生成すると、上記コンテンツサーバ２５は、暗号化コンテンツ２０１とコンテンツ鍵１０２とを携帯電話機１１へ配信用のデータとして上記ＯＴＡサーバ２２へ送信する。
【００５１】
上記ＯＴＡサーバ２２では、配信先の携帯電話機１１を示す情報とともに、暗号化コンテンツ２０１とコンテンツ鍵１０２とを上記コンテンツサーバ２５から受信する。これらの情報を受信すると、上記ＯＴＡサーバは、暗号化鍵１０４によりコンテンツ鍵１０２を暗号化することにより暗号化コンテンツ鍵２０２を生成する。また、上記ＯＴＡサーバ２２は、上記暗号化鍵１０４に対応する復号化鍵２０４を生成する。上記復号化鍵２０４は、上記暗号化鍵１０４とペアとなっている。上記ＯＴＡサーバ２２は、上記通信設備２１を介して、暗号化コンテンツ２０１、暗号化コンテンツ鍵２０２、復号化鍵２０４を携帯

電話機１１へ送信する。
【００５２】
なお、上記暗号化鍵１０４は、携帯電話機１１へ配信されるコンテンツに対するセキュリティサービスを提供する事業者が管理するものである。上述したように、ここでは、通信事業者システムを運営する事業者とコンテンツに対するセキュリティサービスを提供する事業者とが同じであることを想定している。このため、上記暗号化鍵１０４は、上記ＯＴＡサーバ２２が管理するものとする。
【００５３】
上記のような手順により、上記携帯電話機１１の通信部３８では、上記通信設備２１を介して、ダウンロード要求したコンテンツとしての暗号化コンテンツ２０１と暗号化コンテンツ鍵２０２と復号化鍵２０４とを上記ＯＴＡサーバ２２から受信する。これの情報を受信すると、上記携帯電話機１１の制御部３１は、上記復号化鍵２０４をＩＣカードＣ内の耐タンパー性のメモリＣａに記憶するとともに、暗号化コンテンツ２０１と暗号化コンテンツ鍵２０２をユーザが指定するメモリ（不揮発性メモリ３４、あるいは、メモリデバイスＭ）に書込む。
【００５４】
ここでは、暗号化コンテンツ２０１と暗号化コンテンツ鍵２０２とは、メモリデバイスＭに記憶されるものとする。これは、コンテンツが大容量のデータであることを想定しているためである。ただし、上記携帯電話機１１の不揮発性メモリ３４の記憶容量がコンテンツのデータ量に比較して十分に大きなものであれば、上記暗号化コンテンツ２０１と暗号化コンテンツ鍵とは、上記携帯電話機１１の不揮発性メモリ３４に記憶するようにしても良い。
【００５５】
上記のようにメモリデバイスＭに記憶された暗号化コンテンツ２０１は、復号化鍵２０４を用いて復号化されたコンテンツ鍵１０２により復号化されるようになっている。これにより、当該携帯電話機１１では、上記暗号化コンテンツ鍵２０２および復号化鍵２０４により復号化されたコンテンツ１０１が利用可能となる。なお、復号化された状態のコンテンツ１０１は、当該携帯電話機１１から外部へは送信できないようになっている。
【００５６】
また、上記コンテンツサーバ２５から配信するコンテンツ（暗号化コンテンツ）２０１あるいは上記ＯＴＡサーバ２２から配信する復号化鍵２０４には電子証明書を添付するようにしても良い。たとえば、暗号化コンテンツ２０１に電子証明書２１１が添付される場合、上記携帯電話機１１の制御部５１は、暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２とともに電子証明書２１１をメモリデバイスＭに保存する。また、復号化鍵２０４に電子証明書２１４が添付される場合、上記携帯電話機１１の制御部５１は、復号化鍵２０４とともに電子証明書２１４をＩＣカードＣ内のメモリＣａに保存する。
【００５７】
次に、コンテンツの暗号化および復号化のプロセスについて説明する。
図５は、コンテンツサーバ２５から携帯電話機１１へ配信されるコンテンツ１０１の暗号化および復号化のプロセスを説明するための図である。
まず、コンテンツ１０１およびコンテンツ鍵１０２の暗号化のプロセスについて説明する。
暗号化されていないオリジナルのコンテンツ１０１は、オリジナルのコンテンツ鍵１０２によって暗号化される。これにより、コンテンツ鍵１０２で暗号化された暗号化コンテンツ２０１が生成される。一方、暗号化されていないオリジナルのコンテンツ鍵１０２は、暗号化鍵１０４によって暗号化される。これにより、暗号化鍵１０４で暗号化された暗号化コンテンツ鍵２０２が生成される。上記暗号化鍵１０４は、暗号化コンテンツ鍵２０２を復号化するための復号化鍵２０４とペアをなすものである。
【００５８】
上記のような暗号化のプロセスは、携帯電話機１１へダウンロードするまでに実行され

る。つまり、上記携帯電話機１１には、コンテンツ１０１をコンテンツ鍵１０２により暗号化された暗号化コンテンツ２０１と上記コンテンツ鍵１０２を暗号化鍵１０４により暗号化された暗号化コンテンツ鍵２０２とが通信事業者システム２０から配信される。したがって、暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２は、暗号化鍵１０４あるいは暗号化鍵１０４とペアをなす復号化鍵２０４がなければ、復号化することができない。これは、暗号化鍵１０４あるいは復号化鍵２０４が、コンテンツ１０１を保護するための重要なデータであることを示している。

【００５９】

すなわち、上記携帯電話機１１においてコンテンツ１０１を利用するためには、上記復号化鍵２０４も、上記暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２に対応づけて上記携帯電話機１１へ配信される必要がある。ただし、暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２は、ユーザが保存場所を指定するようにしても良いが、上記復号化鍵２０４は、ユーザ自身であっても自由に読み出したり、外部装置からアクセスしたりできないように、携帯電話機１１内に特定のメモリに保存される。たとえば、図２に示すような構成の携帯電話機１１では、ＩＣカードＣにおける耐タンパー性のメモリＣａに上記復号化鍵２０４が記憶されるようになっている。この場合、ＩＣカードＣのメモリＣａには、特定のアプリケーションでなければアクセスできないようになっているものとする。

【００６０】

次に、復号化のプロセスについて説明する。

上記のような暗号化のプロセスによれば、暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２は、復号化鍵２０４あるいは復号化鍵２０４とペアをなす暗号化鍵１０４がなければ、復号化できない。このため、復号化のプロセスでは、専用のアプリケーション（セキュリティアプリケーション）により復号化鍵２０４を取得し、取得した復号化鍵２０４を用いて暗号化コンテンツ鍵２０２の復号化を行う。また、復号化されたコンテンツ鍵１０２が得られると、上記暗号化コンテンツ２０１は、コンテンツ鍵１０２により復号化される。

【００６１】

上記のように、上記携帯電話機１１には、復号化鍵２０４が特定のアプリケーション（セキュリティアプリケーション）でなければアクセスできないＩＣカードＣ内のメモリＣａに復号化鍵２０４が保存され、暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２がメモリデバイスＭに保存されているものとする。ここで、セキュリティアプリケーションは、上記携帯電話機１１にダウンロードされているものとする。

【００６２】

このような場合、上記携帯電話機１１の制御部３１は、暗号化コンテンツ２０１を復号化するため、まず、セキュリティアプリケーションによりＩＣカードＣ内のメモリに記憶されている復号化鍵２０４を用いてメモリデバイスＭに記憶されている暗号化コンテンツ鍵２０２を復号化する。暗号化コンテンツ鍵２０２を復号化すると、上記携帯電話機１１の制御部３１は、復号化したコンテンツ鍵１０２を用いてメモリデバイスＭに記憶されている暗号化コンテンツ２０１を復号化する。

【００６３】

次に、上記携帯電話機１１がダウンロードしたコンテンツをパソコン１２で利用する場合のプロセスについて説明する。

上述したような手順によれば、上記携帯電話機１１のメモリデバイスＭには、暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２が保存されているものの、暗号化コンテンツ鍵２０２を復号化するための復号化鍵２０４は格納されていない。上述しような暗号化および復号化のプロセスによれば、復号化鍵２０４（あるいは復号化鍵とペアをなす暗号化鍵）がなければ、メモリデバイスＭに記憶されている暗号化コンテンツおよび暗号化コンテンツ鍵を復号化できない。つまり、上記携帯電話機１１から取り外されたメモリデバイスＭだけでは、メモリデバイスＭに記憶されている暗号化コンテンツ２０１が利用で

きない。言い換えれば、上記携帯電話機１１から取り外したメモリデバイスＭをパソコン１２に装着しただけでは、メモリデバイスＭに暗号化された状態で記憶されているデータ（暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２）は使用できない。

【００６４】

しかしながら、上記のようなコンテンツは、運用上、ユーザ自身の私的な利用であれば（つまり、著作権などのセキュリティが確保されている状態であれば）、上記携帯電話機１１以外の電子装置で利用することが許容されるものが多い。たとえば、上記携帯電話機１１には、その物理的な制約によって表示部の表示画面を大きくすることが困難である。このため、ユーザとしては、携帯電話機１１でダウンロードしたコンテンツをパソコン１２などの大きな表示画面で表示させたい場合があるという要望がある。また、コンテンツを提供する事業者側も、コンテンツの利用を促進するために、著作権などのセキュリティが確保された状態であれば、上記携帯電話機１１以外の電子装置でのコンテンツの利用を許容したいという要望もある。

【００６５】

また、上記メモリデバイスＭを携帯電話機１１からパソコン１２に差し替えた状態でコンテンツがパソコン１２で利用可能となれば、ケーブル等で携帯電話機１１とパソコン１２を直接的に接続したり、携帯電話機１１からＩＣカードＣと取り出してパソコン１２に接続したＩＣカードリーダに装着したりする必要がないという利点もある。すなわち、携帯電話機１１でダウンロードしたコンテンツをメモリデバイスＭに保存した場合、上記メモリデバイスＭを携帯電話機１１からパソコン１２に差し替えてメモリデバイスＭに保存されているコンテンツをパソコン１２で利用できるようなものが要望されている。

【００６６】

図６は、上記携帯電話機１１が上記メモリデバイスＭに保存した暗号化コンテンツ２０１をパソコン１２で利用するためのプロセスを概略的に説明するための図である。

ここで、上記携帯電話機１１には、コンテンツ１０１をパソコン１２で利用可能とする為のアプリケーション（セキュリティアプリケーション）１０３がインストールされているものとする。

【００６７】

暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２が記憶されているメモリデバイスＭが携帯電話機１１より引き抜かれた場合、上記携帯電話機１１の制御部３１は、上記セキュリティアプリケーション１０３によりワンタイムパスワード１１１を生成する。生成されるワンタイムパスワード１１１は、上記パソコン１２で動作する所定のアプリケーション（コンテンツ利用アプリケーション）２０３により復号化鍵２０４が生成されるようになっている。なお、上記ワンタイムパスワード１１１の生成手法については、後で詳細に説明する。上記ワンタイムパスワード１１１を生成すると、上記携帯電話機１１の制御部３１は、生成したワンタイムパスワード１１１を表示部４１に表示する。

【００６８】

上記携帯電話機１１の表示部４１にワンタイムパスワード１１１が表示されると、ユーザは、上記携帯電話機１１から取り出したメモリデバイスＭをパソコン１２のインターフェース５５に装着し、上記携帯電話機１１の表示部４１に表示されたワンタイムパスワード１１１を操作部５８により入力する。

【００６９】

上記操作部５８によりワンタイムパスワード１１１が入力されると、上記パソコン１２の制御部５１は、上記コンテンツ利用アプリケーション２０３により入力されたワンタイムパスワード１１１を解析することにより復号化鍵２０４を生成する。上記ワンタイムパスワード１１１から復号化鍵２０４を生成すると、上記パソコン１２の制御部５１は、上記コンテンツ利用アプリケーション２０３により生成した復号化鍵２０４を用いてメモリデバイスＭに記憶されている暗号化コンテンツ鍵２０２を復号化する。コンテンツ鍵を復元すると、上記制御部５１は、上記コンテンツ利用アプリケーション２０３により復元したコンテンツ鍵１０２を用いて暗号化コンテンツ２０１を復号化する。これにより、メモ

リデバイスＭに暗号化された状態で記憶されているコンテンツ１０１は復号化（復元）され、当該パソコン１２で利用可能となる。

【００７０】

次に、ワンタイムパスワード１１１によるパソコン１２でのコンテンツの利用方法について詳細に説明する。

【００７１】

図７は、ワンタイムパスワード１１１によるパソコン１２でのコンテンツの利用について説明するための図である。

【００７２】

ここでは、メモリデバイスＭには、上記携帯電話機１１がダウンロードした暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２が記憶され、上記ＩＣカードＣのメモリＣａには、暗号化コンテンツ鍵２０２を復号化するための復号化鍵２０４が記憶されているものとする。また、上記携帯電話機１１には、上記セキュリティアプリケーション１０３がインストールされており、上記パソコン１２には、コンテンツ利用アプリケーション２０３がインストールされているものとする。

【００７３】

まず、上記セキュリティアプリケーション１０３により実現される機能について説明する。

上記セキュリティアプリケーション１０３は、主に、セキュリティ設定機能（セキュリティ設定部）３０１、ユーザ認証機能（ユーザ認証部）３０２、パスワード生成機能（パスワード生成部）３０３、パスワード表示機能（パスワード表示部）３０４などの機能を提供する。

上記セキュリティ設定部３０１は、コンテンツの利用に伴うセキュリティ設定を行うものである。たとえば、上記セキュリティ設定部３０１では、ユーザ認証部３０２によるユーザ認証の必要性、コンテンツの利用制限などを設定する機能を提供している。また、上記セキュリティ設定部３０１は、上記ＯＴＡサーバ２２あるいは上記コンテンツサーバ２５などの外部装置からも遠隔でセキュリティ設定を行うことが可能となっている。つまり、セキュリティ設定部３０１では、コンテンツごとのセキュリティ設定をコンテンツを提供する事業者側から設定できるようになっている。

【００７４】

上記ユーザ認証部３０２は、ユーザ認証（本人確認）を行うための機能を提供している。たとえば、上記ユーザ認証部３０２では、ユーザが入力するパスワード（ユーザパスワード）に基づいてユーザ認証を行う。このようなユーザ認証は、たとえば、ＩＣカードＣに記憶されている暗証番号とユーザが入力する暗証番号とを照合することにより実現可能である。なお、上記ユーザ認証部３０２によるユーザ認証は、パスワードによる認証に限られるものではなく、たとえば、指紋などの生体情報を用いてユーザ認証を行うようにしても良い。

【００７５】

上記パスワード生成部３０３は、ＩＣカードＣのメモリＣａに保存されている復号化鍵２０４を上記コンテンツ利用アプリケーション２０３で解析可能なワンタイムパスワードを生成する機能を提供している。たとえば、上記パスワード生成部３０３では、上記復号化鍵２０４、ユーザ認証部３０２による認証結果、セキュリティ設定部３０１により設定されているセキュリティ条件などに基づいて、ワンタイムパスワード１１１を生成する。たとえば、上記パスワード生成部３０３では、上記復号化鍵２０４を種に乱数を生成し、ワンタイムパスワードの一部を生成する。また、上記パスワード表示部３０４は、上記パスワード生成部３０３により生成されたワンタイムパスワードを表示部４１に表示させる機能を提供している。

【００７６】

次に、上記コンテンツ利用アプリケーション２０３により実現される機能について説明する。

上記コンテンツ利用アプリケーション２０３は、主に、パスワード解析機能（パスワード解析部）３１１、コンテンツ鍵復号化機能（コンテンツ鍵復号化部）３１２、コンテンツ復号化機能（コンテンツ復号化部）３１３、コンテンツ実行機能（コンテンツ実行部）３１４などの機能を提供する。

上記パスワード解析部３１１は、ユーザがワンタイムパスワード１１１として入力したパスワードを解析する機能を提供している。上記パスワード解析部３１１では、入力されたパスワードからコンテンツ鍵を復号化（生成）するための復号化鍵、当該コンテンツ１０１を利用するためのセキュリティ条件、ユーザ認証結果などを解析する。

【００７７】

上記コンテンツ鍵生成部３１２は、上記パスワード解析部３１１による解析結果に基づいて暗号化コンテンツ鍵２０２を復号化する機能（コンテンツ鍵１０２を生成する機能）を提供している。すなわち、上記コンテンツ鍵生成部３１２は、上記パスワード解析部３１１によりユーザが入力したパスワードを解析した結果としての復号化鍵（鍵データ）を用いて上記メモリデバイスＭに記憶されている暗号化コンテンツ鍵２０２を復号化する処理を行う。

【００７８】

上記コンテンツ復号化部３１３は、上記コンテンツ鍵生成部３１２により復号化されたコンテンツ鍵（オリジナル）１０２を用いて暗号化コンテンツ２０１を復号化する機能を提供している。すなわち、上記コンテンツ復号化部３１３は、上記コンテンツ鍵生成部３１２により復号化されたコンテンツ鍵１０２を用いて上記メモリデバイスＭに記憶されている暗号化コンテンツ２０１を復号化する処理を行う。

上記コンテンツ実行部３１４は、上記コンテンツ復号化部３１３により復号化されたコンテンツ（オリジナル）１０１を実行するための機能を提供している。すなわち、上記コンテンツ実行部３１４は、上記コンテンツ復号化部３１３により復号化されたコンテンツ１０１をパソコン１２で実行する処理を行う。

【００７９】

次に、上記携帯電話機１１がメモリデバイスＭに保存したコンテンツ（暗号化コンテンツ）をパソコン１２で利用する場合の処理手順について説明する。

図８は、携帯電話機１１がダウンロードした暗号化されたコンテンツを他の装置で利用可能とするためのワンタイムパスワードを生成する処理を説明ためのフローチャートである。また、図９は、パソコン１２がメモリデバイスＭに記憶されている暗号化されたコンテンツを利用するための処理を説明するためのフローチャートである。

【００８０】

ここで、上記携帯電話機１１では、上記通信事業者システム２０を介してダウンロードした暗号化コンテンツ２０１および暗号化コンテンツ鍵２０２をメモリデバイスＭに保存しているものとする。また、上記携帯電話機１１では、上記暗号化コンテンツ鍵２０２を復号化するための復号化鍵２０４をＩＣカードＣの耐タンパー性のメモリＣａに保存しているものとする。

【００８１】

ユーザは、携帯電話機１１からメモリデバイスＭを取り外し、そのメモリデバイスＭをパソコン１２に装着する。上記携帯電話機１１では、上記メモリデバイスＭが取り外された場合、上記制御部３１が、上記セキュリティアプリケーション１０３により上記メモリデバイスＭに記憶されている暗号化コンテンツ２０１をパソコン１２で利用するためのワンタイムパスワード１１１を生成するための処理を実行する。上記ワンタイムパスワード１１１を生成するための処理は、ユーザによる指示に応じて実行されるようにしても良いし、メモリデバイスＭが取り外されたことを制御部３１が検知した際に実行されるようにしても良い。

【００８２】

上記ワンタイムパスワード１１１を生成するための処理を開始すると、上記携帯電話機１１の制御部３１は、まず、上記セキュリティ設定部３０１により設定されている上記コ

ンテンツ１０１をパソコン１２で利用するためのセキュリティ条件を確認する（ステップＳ１１）。上記セキュリティ条件により上記コンテンツ１０１をパソコン１２で利用するためにユーザ認証が必要であると判断した場合、つまり、ワンタイムパスワードを発行するためのユーザ認証が必要であると判断した場合（ステップＳ１２、ＹＥＳ）、上記制御部３１は、上記ユーザ認証部３０２によりユーザ認証処理を行う（ステップＳ１３）。上記ユーザ認証部３０２によるユーザ認証処理は、上述したように、ユーザパスワードによるものであっても良いし、ユーザの生体情報などによるものであっても良い。このユーザ認証が失敗した場合（ステップＳ１４、ＮＯ）、上記制御部３１は、ワンタイムパスワードの生成処理を中止する。なお、上記のようなユーザ認証は、所定回数に至るまで、繰り返し実行するようにしても良い。

【００８３】

上記ユーザ認証が成功した場合（ステップＳ１４、ＹＥＳ）、あるいは、上記セキュリティ条件によりユーザ認証が不要であると判断した場合（ステップＳ１２、ＮＯ）、上記制御部３１は、上記パスワード生成部３０３により上記コンテンツ１０１を利用するためのワンタイムパスワード１１１を生成する処理を行う（ステップＳ１５）。上記パスワード生成部３０３によるワンタイムパスワードの生成処理では、上述したように、復号化鍵２０４を元に発生させた乱数、セキュリティ条件、ユーザ認証結果などの情報に基づいてワンタイムパスワード１１１が生成される。

【００８４】

上記パスワード生成部３０３によりワンタイムパスワード１１１が生成されると、上記制御部３１は、上記パスワード表示部３０４により上記パスワード生成部３０３により生成されたワンタイムパスワード１１１を表示部４１に表示する（ステップＳ１６）。以上の処理により、上記携帯電話機１１では、メモリデバイスMに保存したコンテンツ１０１をパソコンで利用可能とするための処理（暗号化されているコンテンツ２０１をパソコン１２で復号化可能とする処理）を終了する。

【００８５】

一方、ユーザによりメモリデバイスMが装着されたパソコン１２では、上記コンテンツ利用アプリケーション２０３により上記メモリデバイスMに記憶されているコンテンツを利用するための処理（暗号化コンテンツ２０１を復号化する処理）を実行する。上記メモリデバイスMに記憶されているコンテンツを利用するための処理は、ユーザによる指示に応じて上記コンテンツ利用アプリケーションを起動して実行するようにしても良いし、メモリデバイスMが装着されたことを制御部５１が検知した際に上記コンテンツ利用アプリケーションを起動して実行するようにしても良い。

【００８６】

上記コンテンツ利用アプリケーション２０３が起動すると、上記パソコン１２の制御部５１は、まず、上記メモリデバイスMに記憶されているコンテンツ１０１を利用するためのワンタイムパスワードの入力を促す案内を表示部５６に表示する（ステップＳ２１）。上記表示部５６にパスワードの入力案内が表示されると、ユーザは、上記携帯電話機１１の表示部４１に表示されたワンタイムパスワードを操作部５８により入力する。

【００８７】

上記操作部５８によりパスワードが入力されると（ステップＳ２２、ＹＥＳ）、上記制御部５１は、入力されたパスワードを上記パスワード解析部３１１により解析するパスワード解析処理を行う（ステップＳ２３）。上記パスワード解析部３１１によるパスワード解析処理では、上述したように、入力されたパスワード（ワンタイムパスワード）からコンテンツ鍵を復号化（生成）するための復号化鍵、当該コンテンツを利用するためのセキュリティ条件などを解析する。なお、上記パスワード解析部３１１では、パスワードの解析処理において、ユーザが入力したパスワードが正しいか否かを判定するようにしても良い。この場合、上記制御部５１は、上記パスワード解析部３１１によるユーザが入力したパスワードが正しくないとの判定結果に基づいてワンタイムパスワードの再入力を促すようにしても良い。

【００８８】
上記パスワード解析部３１１による入力されたパスワード解析結果が得られると、上記制御部５１は、上記コンテンツ鍵生成部３１２により上記メモリデバイスＭに記憶されている暗号化コンテンツ２０１を復号化するためのコンテンツ鍵１０２を生成する処理を行う（ステップＳ２４）。上記コンテンツ鍵生成部３１２にコンテンツ鍵生成処理では、上述したように、上記パスワード解析部３１１によりユーザが入力したパスワードから得られた復号化鍵（鍵データ）を用いて上記メモリデバイスＭに記憶されている暗号化コンテンツ鍵２０２を復号化する。なお、ユーザが入力したパスワードが正しいものでなければ、正しいコンテンツ鍵は生成されない（暗号化コンテンツ鍵が正しく復号化されない）。この結果として、誤ったパスワードが入力された場合、誤ったコンテンツ鍵が生成されるため、コンテンツが正しく復号化されないようになっている。
【００８９】
上記コンテンツ鍵生成部３１２によりコンテンツ鍵１０２が生成されると、上記制御部５１は、上記コンテンツ復号化部３１３により上記メモリデバイスＭに記憶されている暗号化コンテンツ２０１を復号化するコンテンツ復号化処理を行う（ステップＳ２５）。上記コンテンツ復号化部３１３によるコンテンツ復号化処理では、上記コンテンツ鍵生成部３１２により復号化されたコンテンツ鍵１０２を用いて上記メモリデバイスＭに記憶されている暗号化コンテンツ２０１を復号化する。
上記コンテンツ復号化部３１３によりコンテンツが復号化されると、上記制御部５１は、上記コンテンツ実行部３１４により上記コンテンツ復号化部３１３により復号化されたコンテンツ１０１を実行する（ステップＳ２６）。以上の処理により、携帯電話機１１が取り外したメモリデバイスＭが装着されたパソコン１２では、上記メモリデバイスＭに保存されている暗号化されたコンテンツを復号化する。
【００９０】
上記のような処理によれば、携帯電話機１１自体をケーブル等により直接的にパソコンに接続したり、携帯電話機１１からＩＣカードＣを取り出してパソコン１２に接続したカードリーダに装着したりすることなく、携帯電話機１１に装着されているＩＣカード内の耐タンパー性のメモリＣａに記憶されている鍵データでセキュリティ保護されているコンテンツが、メモリデバイスＭを着脱することにより、パソコン１２で簡単に利用できる。
【００９１】
上記のように、本実施の形態で説明した情報管理システムでは、携帯電話機が、コンテンツ鍵により暗号化されたコンテンツおよび暗号化されたコンテンツ鍵をサーバからダウンロードし、コンテンツ鍵を復号化するための復号化鍵を当該携帯電話機内の耐タンパー性のメモリに保存する。また、上記復号化鍵を保存する耐タンパー性のメモリは、たとえば、携帯電話機に装着されるＩＣカード内のメモリである。これにより、上記のような情報管理システムでは、ネットワークを介して携帯電話機にダウンロードされるコンテンツのセキュリティを確実に確保できる。
【００９２】
また、上記情報管理システムでは、携帯電話機が、ダウンロードしたコンテンツ鍵により暗号化されたコンテンツおよび暗号化されたコンテンツ鍵を携帯電話機に着脱可能なメモリデバイスに保存し、コンテンツ鍵を復号化するための復号化鍵を携帯電話機に装着されているＩＣカード内の耐タンパー性のメモリに保存する。上記携帯電話機がダウンロードしたコンテンツを携帯電話機以外の電子装置で利用する場合、上記携帯電話機では、上記ＩＣカード内の耐タンパー性のメモリに保存されている復号化鍵を元に発生される乱数を用いてワンタイムパスワードを生成する。
【００９３】
上記携帯電話機以外の電子装置（パソコン）では、ユーザが携帯電話機１１から取り外したメモリデバイスＭを上記携帯電話機以外の電子装置に装着するとともに上記携帯電話機１１が生成したワンタイムパスワードを入力すると、ユーザが入力したワンタイムパスワードの解析し、その解析結果に基づいてメモリデバイスＭに記憶されている暗号化され

たコンテンツ鍵およびコンテンツを復号化する。

【００９４】

これにより、パソコンなどの携帯電話機以外の電子装置で、携帯電話機がダウンロードしたセキュリティ保存された状態のコンテンツを簡単に利用できるようになる。さらに、パソコンなどの携帯電話機以外の電子装置から直接的に携帯電話機内のメモリにアクセスしなくとも、メモリデバイスを差し替えてパスワードを入力するだけで、コンテンツのセキュリティを確保しつつ、パソコンなどの携帯電話機以外の電子装置で、当該コンテンツが利用できる。

【図面の簡単な説明】

【００９５】

【図１】この発明の実施の形態に係る情報管理システムの構成例の概要を示す図である。

【図２】携帯電話機の構成例を示すブロック図。

【図３】パソコンの構成例を示すブロック図。

【図４】コンテンツサーバが提供するコンテンツの利用方法を概略的に説明するための図。

【図５】コンテンツサーバから携帯電話機へ配信されるコンテンツの暗号化および復号化のプロセスを説明するための図。

【図６】携帯電話機がメモリデバイスに保存した暗号化コンテンツをパソコンで利用するためのプロセスを概略的に説明するための図。

【図７】ワンタイムパスワードによるパソコンでのコンテンツの利用について説明するための図。

【図８】携帯電話機がダウンロードした暗号化されたコンテンツをパソコンで利用可能とするためのワンタイムパスワードを生成する処理を説明ためのフローチャート。

【図９】パソコンがメモリデバイスに記憶されている暗号化されたコンテンツを利用するための処理を説明するためのフローチャート。

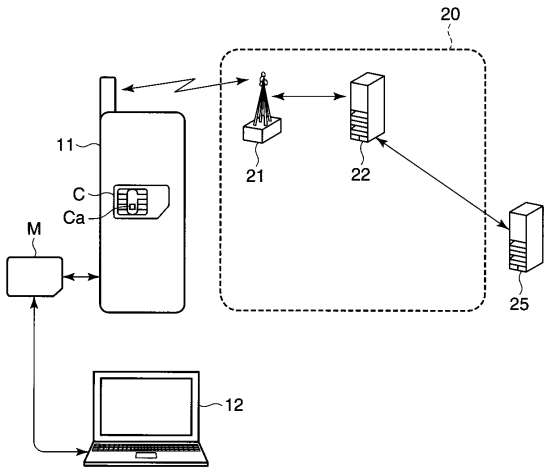
【符号の説明】

【００９６】

Ｃ…ＩＣカード、Ｃａ…耐タンパー性のメモリ、Ｍ…メモリデバイス、１１…携帯電話機、１２…パーソナルコンピュータ（パソコン）、２０…通信事業者システム、２１…通信設備、２２…ＯＴＡサーバ、２５…コンテンツサーバ、３１…制御部、３４…不揮発性メモリ、３５…ＩＣカードインターフェース、３６…メモリデバイスインターフェース、３８…通信部、４１…表示部、４２…操作部、５１…制御部、５４…不揮発性メモリ、５５…メモリデバイスインターフェース、５６…表示部、５８…操作部、１０１…コンテンツ、１０２…コンテンツ鍵、１０３…セキュリティアプリケーション、１０４…暗号化鍵、１１１…ワンタイムパスワード、２０１…暗号化コンテンツ、２０２…暗号化コンテンツ鍵、２０３…コンテンツ利用アプリケーション、２０４…復号化鍵、３０１…セキュリティ設定部、３０２…ユーザ認証部、３０３…パスワード生成部、３０４…パスワード表示部、３１１…パスワード解析部、３１２…コンテンツ鍵生成部、３１３…コンテンツ復号化部、３１４…コンテンツ実行部

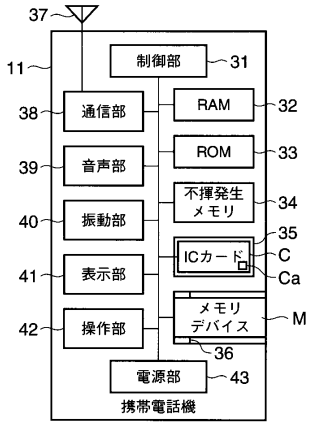
【図１】

図１



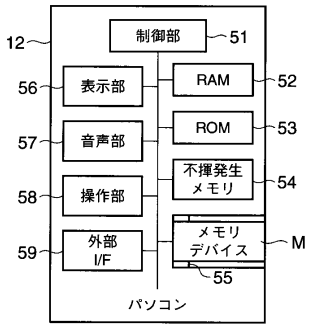
【図２】

図２



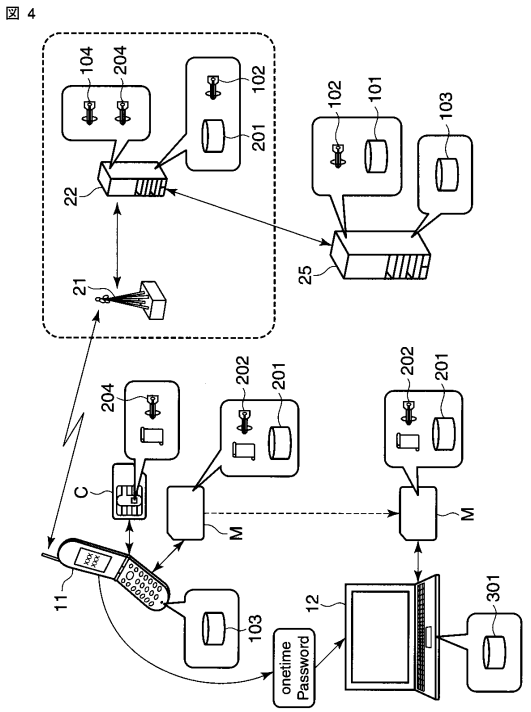
【図３】

図３



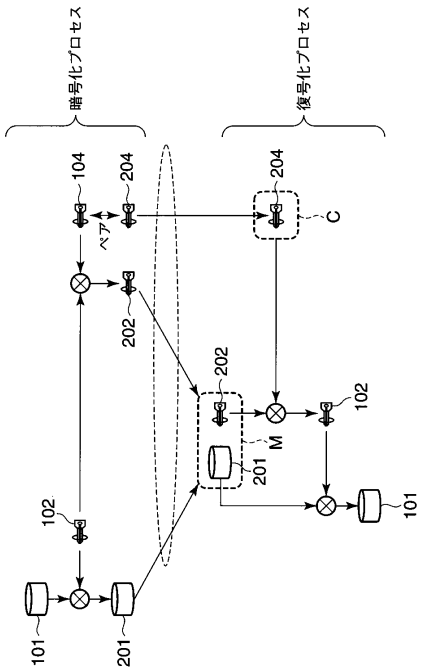
【図４】

図４



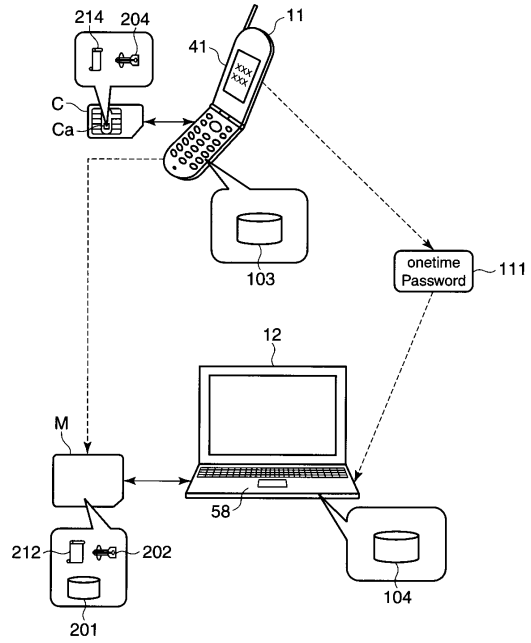
【図５】

図５



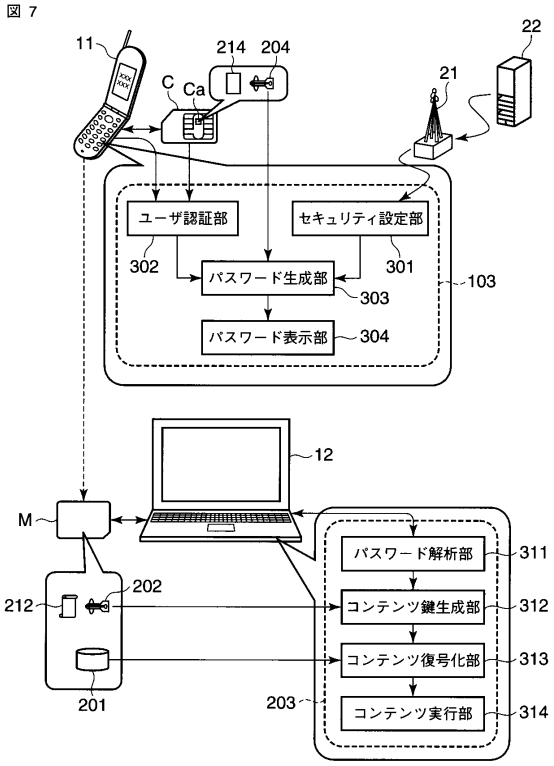
【図６】

図 6



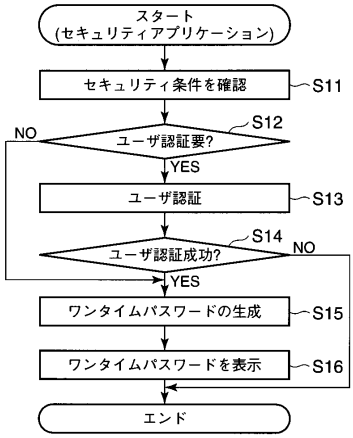
【図７】

図 7



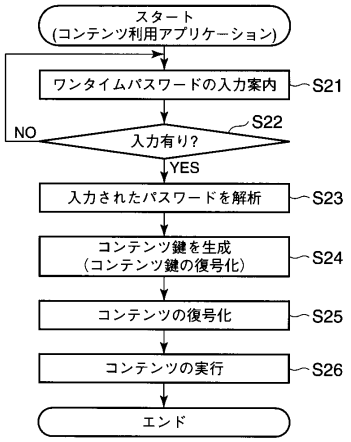
【図８】

図 8



【図９】

図 9



フロントページの続き

(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 石橋 孝信
東京都港区芝浦一丁目１番１号 株式会社東芝内

審査官 松平 英

(56)参考文献 特開平９－２８２２３５（ＪＰ，Ａ）
特開２００２－１８９９５８（ＪＰ，Ａ）
特開２００４－１５２２６２（ＪＰ，Ａ）
特表２００７－５０３６４６（ＪＰ，Ａ）
特開２００７－２８６９３５（ＪＰ，Ａ）
特開２００８－１５９２４（ＪＰ，Ａ）
国際公開第２００８／００４３１２（WO，Ａ１）
山田 英之 HIDEYUKI YAMADA，セキュリティの基礎（ＩＩ）リモート・アクセス，日経オープンシステム 第４７号 NIKKEI OPEN SYSTEMS，日本，日経ＢＰ社 Nikkei Business Publications,Inc.，１９９７年 2月１５日，第４７号，p.285-299
モバイルだからこそ［セキュリティ］，ｍｏｂｉｌｅ ｍｅｄｉａ ｍａｇａｚｉｎｅ 第8巻 第1号，日本，株式会社シーメディア，１９９９年１２月１３日，第8巻 第1号，p.28-36

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／００
Ｇ０９Ｃ １／００
Ｇ０６Ｋ １７／００
Ｇ０６Ｋ １９／００
Ｇ０６Ｆ ２１／２０
Ｇ０６Ｆ ２１／２４
Ｈ０４Ｑ ７／００
Ｈ０４Ｍ ３／００
Ｈ０４Ｍ ７／００
Ｈ０４Ｍ １１／００