(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2007-166568
(P2007-166568A)
(43)公開日　平成19年6月28日(2007.6.28)

(51)Int.Cl.	F I			テーマコード（参考）
H04L 9/08 (2006.01)	H04L	9/00	601A	5J104
	H04L	9/00	601E	

審査請求 未請求　請求項の数 14　書面　（全 7 頁）

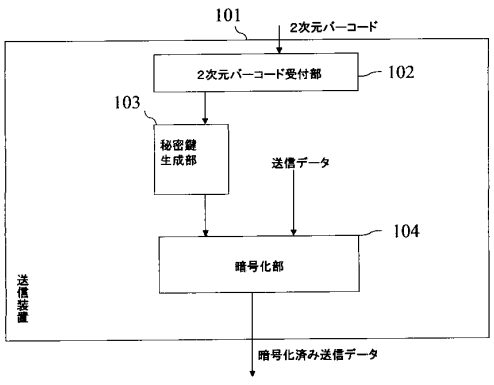
(21)出願番号　特願2005-380959 (P2005-380959)
(22)出願日　平成17年12月14日 (2005.12.14)

(71)出願人　304001545
株式会社カオスウェア
東京都小金井市貫井北町４丁目２番１号
(72)発明者　梅野　健
東京都小金井市貫井北町４丁目２番１号
株式会社カオスウェア内

Fターム(参考)　5J104 AA01 AA16 AA32 EA04 EA15 EA16 EA17 EA18 JA03 NA02 NA27 NA37

(54)【発明の名称】暗号伝送システム、送信装置、受信装置、送信方法、受信方法、ならびに、プログラム

(57)【要約】
【課題】　従来の暗号化伝送装置では、ＰＣと携帯電話端末といった異なる種類の送受信装置との間で、暗号化伝送を行うことが、鍵の共有が実現し難くなため、困難であった。
【解決手段】送信装置１０１は、２次元バーコードを２次元バーコード受付部１０２で受付け、秘密鍵生成部１０３で、２次元バーコードから秘密鍵を生成する。暗号化部１０４で、送信データを、秘密鍵生成部１０３により生成された秘密鍵で暗号化してそれを暗号化済みデータとして送信する。
【選択図】図１



【特許請求の範囲】
【請求項１】
送信装置と、受信装置と、を備える暗号伝送システムであって、
（ａ）前記送信装置は、
２次元バーコードを取得する２次元バーコード受付部、前記取得された２次元バーコードから、秘密鍵を生成する秘密鍵生成部、
前記秘密鍵生成部により生成された秘密鍵から、送信データを暗号化する
暗号化部
を備え、
（ｂ）前記受信装置は、
受信用秘密鍵から２次元バーコードを生成する２次元バーコード生成部、
当該受信用秘密鍵から受信データを復号化する復号化部
を備える
ことを特徴とする物。
【請求項２】
請求項１に記載の暗号伝送システムであって、
前記送信装置で取得される２次元バーコードは、前記受信装置の２次元バーコード生成部により生成される２次元バーコードと等しいことを特徴とする物。
【請求項３】
請求項１に記載の暗号伝送システムであって、
前記受信装置で復号用に用いられる前記受信用秘密鍵は、
前期受信装置に予め登録してある前記送信装置の固有番号を
用いて生成される
ことを特徴とする物。
【請求項４】
請求項１に記載の暗号伝送システムであって、
前記受信装置で復号用に用いられる前記受信用秘密鍵は、
前記受信装置が起動する毎に、毎回異なる
ことを特徴とする物。
【請求項５】
請求項１に記載の暗号伝送システムであって、
前記送信装置は、前記送信データを暗号化した後、前記送信データをメモリ上から
消滅させる
ことを特徴とする物。
【請求項６】
請求項１から５のいずれか１項に記載の暗号伝送システムにおける送信装置。
【請求項７】
請求項１から５のいずれか１項に記載の暗号伝送システムにおける受信装置。
【請求項８】
受信装置と通信する送信装置にて実行される送信方法であって、
２次元バーコードを取得する２次元バーコード受付工程、
前記取得された２次元バーコードから、これに対応する秘密鍵を生成する秘密鍵生成工程、
前記秘密鍵により送信データを暗号化する
暗号化工程
を備えることを特徴とする方法。
【請求項９】
請求項８に記載の送信方法であって、
前記暗号化工程では、送信データを暗号化した後、前記送信データをメモリ上から
消滅させる

ことを特徴とする方法。
【請求項１０】
請求項８に記載の送信方法であって、
前記送信工程では、暗号化済みデータを、第三者がアクセス可能なサーバ装置にアップロードすることによって、前記送信工程における送信が行われる
ことを特徴とする方法
【請求項１１】
送信装置と通信する受信装置にて実行される受信方法であって、
受信用秘密鍵から２次元バーコードを生成する２次元バーコード生成工程、当該受信用秘密鍵により受信データを復号化する復号化工程を備える
ことを特徴とする方法。
【請求項１２】
請求項１１に記載の受信方法であって、
前記受信工程は、前記サーバ装置にアップロードされた送信側暗号済みデータをダウンロードすることによって、前記受信工程における受信が行われる
ことを特徴とする方法。
【請求項１３】
コンピュータを、請求項６に記載の送信装置として機能させることを特徴とするプログラム。
【請求項１４】
コンピュータを、請求項７に記載の受信装置として機能させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報を暗号化して復号化するのに好適な暗号伝送システム、送信装置、受信装置、送信方法、受信方法、ならびに、これらをコンピュータ上にて実現するプログラムに関する。
【従来技術】
【０００２】
従来から、暗号技術の分野においては、情報漏洩を防止するため、種々の技術が提案されている。たとえば、公開鍵暗号と共通鍵暗号の技術を用いて情報を特定の人のみが復号化すること可能にするハイブリッド暗号化方式を用いて、共有ファイルサーバーに情報漏えい防止データを暗号化する技術である。
【０００３】
更に、サーバー・クライアント型システムにおいて、クライアント側の暗号化復号化操作の決裁情報を管理する所謂電子決済システムもある。
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら、情報漏洩を防止するための技術は、常に新しいものが求められていることはいうまでもない。また、出張先で携帯電話により撮ったデジタルカメラ画像といった出張先の機密性の高いデータを本社のＰＣへ送信する際に、暗号化されている方が望ましい。
【０００５】
ところで、公知の技術の中では、携帯電話等の送信装置と、ＰＣ等で実現する受信装置といった異なる種類の送受信装置の場合、秘密鍵を共有し、暗号化通信を行うことが困難であった。
【０００６】
本発明は、上記のような課題を解決するものであって、情報を暗号化伝送するのに好適

な暗号化伝送システム、送信装置、受信装置、送信方法、受信方法、ならびに、これらをコンピュータ上にて実現するプログラム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】

【０００７】

以上の目的を達成するため、本発明の原理にしたがって、下記の発明を開示する。

【０００８】

本発明の第１の観点に係る暗号化伝送システムは、送信装置と、受信装置と、を備え、以下のように構成する。

【０００９】

すなわち、送信装置は、２次元バーコード受付部、秘密鍵生成部、及び、暗号化部、を備える。

【００１０】

ここで、２次元バーコード受付部は、２次元バーコードを、送信装置に受付る。

【００１１】

秘密鍵生成部は、前記２次元バーコード受付部により受け付けられた２次元バーコードから、１対１に変換することにより、暗号化する際必要な秘密鍵を生成する。

【００１２】

一方、暗号化部は、前記秘密鍵生成部により生成された秘密鍵により送信データを暗号化する。

【００１３】

受信装置は、２次元バーコード生成部、及び、復号化部を備える。

【００１４】

ここで、２次元バーコード生成部は、受信用秘密鍵から２次元バーコードを１対１の変換により生成する。

【００１５】

復号化部は、前記受信用秘密鍵により受信データを復号化する。

【００１６】

また、本発明の暗号化伝送システムにおいて、前記送信装置で取得される２次元バーコードは、前記受信装置の２次元バーコード生成部により生成される２次元バーコードと等しいことを特徴とする特徴とすることができる。

【００１７】

本発明のその他の観点に係る送信装置は、上記の暗号化伝送システムにおける送信装置である。

【００１８】

本発明のその他の観点に係る受信装置は、上記の暗号化伝送システムにおける受信装置である。

【００１９】

本発明のその他の観点に係る送信方法は、上記の送信装置において実行される方法である。

【００２０】

本発明のその他の観点に係る受信方法は、上記の受信装置において実行される方法である。

【００２１】

本発明の他の観点に係るプログラムは、コンピュータを、上記の送信装置、もしくは、受信装置として機能させ、コンピュータに、上記の送信方法もしくは受信方法を実行させるように構成する。

【００２２】

当該プログラムは、コンピュータ読取可能な情報記録媒体（コンパクトディスク、フレキシブルディスク、ハードディスク、光磁気ディスク、ディジタルビデオディスク、磁気テープ、または、半導体メモリを含む。）に記録することができる。

【００２３】
そして、上記の情報記録媒体は、コンピュータとは独立して配布、販売することができるほか、インターネット等のコンピュータ通信網を介して上記のプログラムそのものを配布、販売することができる。
【発明の効果】
【００２４】
本発明によれば、情報を暗号化して伝送するのに好適な暗号化伝送システム、送信装置、受信装置、送信方法、受信方法、ならびに、これらをコンピュータ上にて実現するプログラムを提供することができる。
【発明を実施するための最良の形態】
【００２５】
以下に本発明の実施形態を説明する。なお、以下にあげる実施形態は、説明のためのものであり、本発明の範囲を制限する物ではない。したがって、当業者であれば、これらの各要素または全要素を、これと均等なものに置換した実施形態を採用することが可能であるが、これらの実施形態も、本発明の範囲に含まれる。
【実施例１】
【００２６】
図１は、本発明の暗号化伝送システムの送信装置の実施形態の概要構成を示す説明図である。以下、本図を参照して説明する。
【００２７】
本図に示す通り、送信装置１０１は、２次元バーコードを２次元バーコード受付部１０２で受付け、秘密鍵生成部１０３で、２次元バーコード受付部１０２にて受け付けられた２次元バーコードより秘密鍵を生成する。送信データは、秘密鍵生成部１０３により生成された秘密鍵により、暗号化部１０４により暗号化され、暗号化済みデータとして送信される。
【００２８】
例えば、２次元バーコードを送信装置と受信装置の共通の秘密鍵と表現するものと見なすことにより、送信装置１０１によって２次元バーコードを受け付けられた２次元バーコードから１対１変換することにより、秘密鍵生成部１０３にて生成される秘密鍵は、受信装置で生成される２次元バーコードと前記送信装置で受け付けられた２次元バーコードと等しい場合、共有され、暗号化通信が可能となる。
【００２９】
又、暗号化部１０４で送信データを暗号化する際、メモリ上に、元のデータを完全に消滅させることができる。この場合、情報保護の観点から不要なデータを消滅させるという点で安全性を高めることになる。
【００３０】
図２は、本発明の暗号化伝送システムの受信装置の実施形態の概要構成を示す説明図である。以下、本図を参照して説明する。
【００３１】
本図に示す通り、受信装置２０１は、２次元バーコード生成部２０２、復号化部２０３、から構成され、２次元バーコード生成部２０２で、受信用秘密鍵から１対１変換することにより２次元バーコードを生成し出力し、復号化部２０３で、受信データを、前記受信用秘密鍵で復号化する。
【００３２】
この場合、前記受信用秘密鍵は、受信装置１０２に予め登録してある送信装置１０１の固有の番号を用いて生成されるようにすることができる。例えば、送信装置が携帯電話端末である場合、携帯電話端末の端末番号を固有の番号として用いることができる。
【００３３】
また、前記受信用秘密鍵は、受信装置を起動する毎に毎回異なる様にすることができる。この場合、２次元バーコード生成部２０２で生成される２次元バーコードがそれに伴

い、毎回異なる様になり、鍵管理の安全性が高まる。

【００３４】

送信装置１０１をカメラ付き携帯電話端末とする場合、２次元バーコードを読み取れる機種があり、携帯電話端末上で、紙媒体等に印刷された２次元バーコードをカメラで読み取ることができ、秘密鍵を取得することができる。　この場合、携帯電話端末のカメラで撮影した送信データを携帯電話のメモリバッファ上でダイレクトに暗号化することにより、生の写真データが保存されなく完全に消滅する様になる。

【産業上の利用可能性】

【００３５】

以上説明したように、本発明によれば、情報を暗号化して伝送するのに好適な暗号化伝送システム、送信装置、受信装置、送信方法、受信方法、ならびに、これらをコンピュータ上にて実現するプログラムを提供することができ、暗号通信の分野に適用することができる。

【図面の簡単な説明】

【００３６】

【図１】　本発明の実施形態に係る暗号化伝送システムの送信装置の概要構成を示す模式図である。

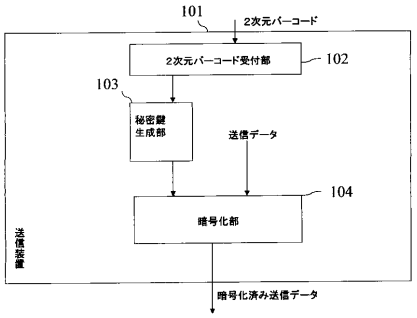
【図２】　暗号化伝送システムの受信装置の概要構成を示す模式図である。

【符号の説明】

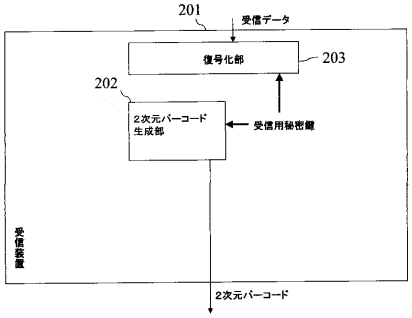
【００３７】

１０１　送信装置
１０２　２次元バーコード受付部
１０３　秘密鍵生成部
１０４　暗号化部
２０１　受信装置
２０２　２次元バーコード生成部
２０３　復号化部

【図１】


101
2次元バーコード
2次元バーコード受付部
102
103
秘密鍵
生成部
送信データ
104
暗号化部
送信装置
暗号化済み送信データ

【図２】


201
受信データ
復号化部
203
202
2次元バーコード
生成部
受信用秘密鍵
受信装置
2次元バーコード