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

特許第4289552号
(P4289552)

(45)発行日　平成21年7月1日(2009.7.1)　(24)登録日　平成21年4月10日(2009.4.10)

(51)Int.Cl.			F I		
H04L	9/08	(2006.01)	H04L	9/00	601A
G06K	17/00	(2006.01)	H04L	9/00	601B
G09C	1/00	(2006.01)	H04L	9/00	601E
			G06K	17/00	T
			G09C	1/00	660A

請求項の数 2　(全 8 頁)

(21)出願番号　特願2004-32814(P2004-32814)
(22)出願日　平成16年2月10日(2004.2.10)
(65)公開番号　特開2005-229147(P2005-229147A)
(43)公開日　平成17年8月25日(2005.8.25)
審査請求日　平成19年1月18日(2007.1.18)

(73)特許権者　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100111659
弁理士　金山　聡
(72)発明者　半田　富己男
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(72)発明者　姉川　武彦
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】機密データの漏洩防止方法

(57)【特許請求の範囲】
【請求項１】
ＩＣカードとデータの送受信を行う処理装置における機密データの漏洩防止方法であって、
前記処理装置と前記ＩＣカードの間でセッション鍵を共有するステップと、
前記処理装置内においてコマンドメッセージを前記セッション鍵で暗号化し、前記ＩＣカードに送信するステップと、
前記処理装置から前記ＩＣカードに前記セッション鍵で暗号化したコマンドメッセージを送信した際に、予め前記ＩＣカードから前記処理装置に返信される可能性を有する全てのレスポンスについて前記セッション鍵で暗号化し、前記処理装置内に記憶させておくステップと、
前記処理装置の記憶手段から前記セッション鍵を抹消するステップと、
前記ＩＣカードから前記処理装置に対し、暗号化されたレスポンスの返送があった場合に、予め前記処理装置内に記憶させておいた前記セッション鍵で暗号化されたレスポンスと照合し、返送されてきたレスポンスの内容を判定処理するステップと、
を有することを特徴とする機密データの漏洩防止方法。
【請求項２】
前記処理装置と前記ＩＣカードの間でセッション鍵を共有するステップが、
前記処理装置内でセッション鍵をランダムに生成し公開鍵で暗号化するステップと、
前記公開鍵で暗号化したセッション鍵を、前記ＩＣカードに送信するステップと、

からなることを特徴とする請求項１記載の機密データの漏洩防止方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＩＣカードとデータの送受信を行う処理装置における機密データの漏洩防止方法に関し、特に処理装置からデータの暗号化に用いる鍵が盗まれることを防止した機密データの漏洩防止方法に関する。
【背景技術】
【０００２】
従来、ＩＣカードに記憶されているデータをＩＣカードリーダライタで読み取り、パソコンなどの処理装置で利用する場合には、データの漏洩を防止するためにセキュリティ上データを暗号化させて送受信させる必要がある。
例えば、ＩＣカードを使用した機密データを転送する方法としては、公開鍵暗号方式に基づいた暗号処理能力を持つＩＣカードを用いて、ＩＣカード内の公開鍵情報を装置に送信する際に装置内で乱数を生成させ、その生成した乱数をＩＣカードから受信した公開鍵で暗号化させ、更に装置から暗号化されたデータをＩＣカードに送信し、その後、ＩＣカードは、装置に送信した公開鍵に対する秘密鍵で、装置から受信した暗号化されたデータを復号し、装置内で生成した乱数を得るという方法がある。
更に、ＩＣカード内に送信データをその乱数で暗号化し、暗号化されたデータを装置に送信し、装置においてＩＣカードから受信した暗号化されたデータを乱数で復号することで、ＩＣカード内のデータを装置で得るという技術が既に公知となっている。（例えば、特許文献１参照）
【特許文献１】特開平４－９１５３１
【０００３】
しかしながら、上記の公知技術においては、装置内で生成した暗号化に使用する乱数が装置内のメモリ上に記憶された状態のまま保存されることとなり、不正行為をはたらこうとする第三者が、その装置を破壊するなどして装置内のメモリに記憶されている乱数を盗み取ることができる。
そして、盗み取った乱数を利用して、暗号化されたデータを復号し、ＩＣカードに記憶されている機密データを盗み取ることも可能であり、セキュリティー上の安全性が完全に確保されないという問題がある。
このように従来の技術では、データの送受信時におけるセキュリティが保護されているものの、装置自体が破壊された場合に、装置内に記憶させておいた機密データが漏洩されてしまう危険性があるという問題がある。
【発明の開示】
【発明が解決しようとする課題】
【０００４】
本発明は、ＩＣカードとデータの送受信を行うパソコンなどの処理装置において、不正をはたらこうとする第三者がこの処理装置を破壊して、処理装置内に記憶されている送信データの暗号化に使用する機密データを盗み取ろうとしても、第三者に機密データが知られないように保護することができる機密データの漏洩防止方法を提供する。
【課題を解決するための手段】
【０００５】
本発明の機密データの漏洩防止方法は、ＩＣカードとデータの送受信を行う処理装置における機密データの漏洩防止方法であって、前記処理装置と前記ＩＣカードの間でセッション鍵を共有するステップと、前記処理装置内においてコマンドメッセージを前記セッション鍵で暗号化し、前記ＩＣカードに送信するステップと、前記処理装置から前記ＩＣカードに前記セッション鍵で暗号化したコマンドメッセージを送信した際に、予め前記ＩＣカードから前記処理装置に返信される可能性を有する全てのレスポンスについて前記セッ

ション鍵で暗号化し、前記処理装置内に記憶させておくステップと、前記処理装置のメモリから前記セッション鍵を抹消するステップと、前記ＩＣカードから前記処理装置に対し、暗号化されたレスポンスの返送があった場合に、予め前記処理装置内に記憶させておいた前記セッション鍵で暗号化されたレスポンスと照合し、返送されてきたレスポンスの内容を判定処理するステップと、を有することを特徴とする。

【０００６】

また、本発明の機密データの漏洩防止方法は、前記処理装置と前記ＩＣカードの間でセッション鍵を共有するステップが、前記処理装置内でセッション鍵をランダムに生成し公開鍵で暗号化するステップと、前記公開鍵で暗号化したセッション鍵を、前記ＩＣカードに送信するステップと、からなることを特徴とする。

【発明の効果】

【０００７】

本発明の機密データの漏洩防止方法は、予めＩＣカードから処理装置に返信される可能性を有する全てのレスポンスについてセッション鍵で暗号化して記憶させておき、その後、ＩＣカードから処理装置に返信の暗号化されたレスポンスがあった場合でも、その返信データの意味が識別できるようにしてあるので、たとえ処理装置の記憶手段からセッション鍵を抹消してしまったとしても、処理装置において、ＩＣカードからの返信データへの対応が可能である状態にすることができ、第三者が不正行為をはたらこうとして処理装置を破壊して暗号化に使用するセッション鍵を盗み取ろうとしても、処理装置内の記憶手段からセッション鍵が抹消されているので盗み取ることができず、暗号化に使用する機密データの漏洩を防止することができるという効果がある。

【０００８】

また、本発明の機密データの漏洩防止方法は、処理装置とＩＣカードの間でセッション鍵を共有するステップが、処理装置内でセッション鍵をランダムに生成し公開鍵で暗号化して、ＩＣカードに送信することで共有するので、セッション鍵が第三者へ漏洩される危険性がないという効果がある。

【発明を実施するための最良の形態】

【０００９】

以下、図面を参照しながら本発明の実施形態を詳述する。

図１は、本発明の実施形態に係る機密データの漏洩防止方法に用いる装置の外観図、図２は、本発明の実施形態に係る機密データの漏洩防止方法に用いるシステム構成のシステムブロック図、図３は、本発明の実施形態に係る機密データの漏洩防止方法における処理装置とＩＣカードの間でセッション鍵を共有する方法を説明する図、図４は、本発明の実施形態に係る機密データの漏洩防止方法の手順を説明する図である。

【００１０】

本発明の実施形態に係る機密データの漏洩防止方法は、図１に示すように、ＩＣカード１と、パソコンなどの処理装置２と、この処理装置２に備えられたＩＣカードリーダライタ３とを用いて処理される。

ＩＣカードリーダライタ３には、ＩＣカード１を挿入するためのＩＣカード挿入口３ａが設けられ、ＩＣカード挿入口３ａからＩＣカード１を挿入することでＩＣカード１がセット状態となり、ＩＣカードリーダライタ３を介してＩＣカード１と処理装置２との間におけるデータの送受信が行えるようにしてある。

【００１１】

ＩＣカード１には、図２に示すように、入出力手段４、暗号化処理手段５、復号処理手段６、記憶手段７、制御手段８が備えられている。

記憶手段７には、データの暗号化に用いるための公開鍵９と、この公開鍵９で暗号化したデータを復号するための秘密鍵１０と、制御プログラム１１などが予め記憶されている。

暗号化処理手段５は、ＩＣカード１から処理装置２に送信する情報を公開鍵を利用して暗号化する機能を有している。

また、復号処理手段６は、処理装置２からＩＣカード１で受信した暗号化されている情報を、記憶手段７に記憶されている秘密鍵や、処理装置２から入手したセッション鍵を利用して復号する機能を有している。

【００１２】

また、パソコンなどからなる処理装置２には、表示手段１２、セッション鍵をランダムに生成するセッション鍵生成手段１３、暗号化処理手段１４、セッション鍵を抹消するセッション鍵抹消手段１５、暗号化レスポンス照合判別手段１６、入力手段１７、記憶手段１８、入出力手段１９、制御手段２０、などが備えられている。

処理装置２の記憶手段１８には、制御プログラム２１などが登録されている。

暗号化処理手段１４は、処理装置２からＩＣカード１に送信するコマンドメッセージを暗号化する機能を有している。

【００１３】

また、セッション鍵抹消手段１５は、処理装置２内でランダムに生成したセッション鍵に対して、再度使用しなくなった際にセッション鍵を抹消してわからなくする機能を有している。

暗号化レスポンス照合判別手段１６は、ＩＣカード１から処理装置２に暗号化されたレスポンスが届いた際に、予め記憶手段１８に記憶させておいた複数の返信可能性のある暗号化されたレスポンスと照合し、レスポンスの内容を判別する機能を有している。

【００１４】

次に、本発明の機密データの漏洩防止方法において、処理装置２とＩＣカード１の間でセッション鍵を共有する方法を図３に基づいて説明する。

まず、ＩＣカード１の記憶手段７に記憶されている公開鍵９をＩＣカード１から処理装置２に送信する。

次に、処理装置２のセッション生成手段１３によりセッション鍵２２をランダムに生成する。

そして、この生成されたセッション鍵２２を、ＩＣカード１から受信した公開鍵９を利用して暗号化処理手段１４により暗号化する。

次に、公開鍵９で暗号化したセッション鍵２２を、処理装置２からＩＣカード１へ送信する。

【００１５】

公開鍵９で暗号化したセッション鍵２２を処理装置２から受信したＩＣカード１は、記憶手段７に記憶されている秘密鍵１０を利用して復号させる。

そして、この秘密鍵１０を利用して復号したセッション鍵２２をＩＣカード１の記憶手段７に記憶させる。

また、処理装置２内で生成したセッション鍵２２は、処理装置２の記憶手段１８に記憶させておく。

以上の処理により、処理装置２内で生成したセッション鍵２２を、処理装置２とＩＣカード１の記憶手段にそれぞれ記憶させて、共有して使用できる状態にする。

【００１６】

次に、本発明の機密データの漏洩防止方法において、処理装置２からＩＣカード１にコマンドメッセージを暗号化させて送信する場合の処理方法を図４に基づいて説明する。

まず、処理装置２からＩＣカード１に送信するコマンドメッセージを、処理装置２の記憶手段１８に記憶させているセッション鍵２２を利用して暗号化する。

【００１７】

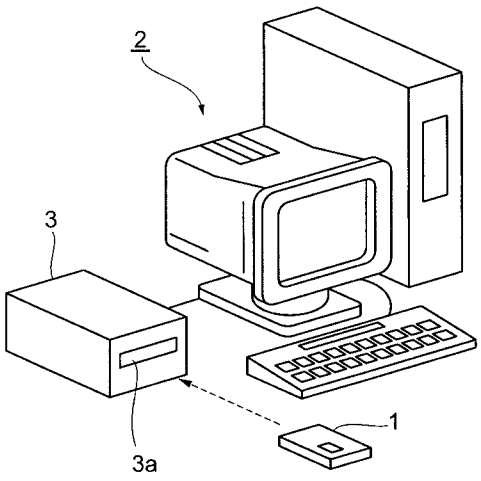
次に、そのコマンドメッセージを処理装置２からＩＣカード１に送信させた場合に、ＩＣカード１から処理装置２に返信されてくる可能性のあるレスポンスの候補が数種類あるが、これらレスポンスの候補の全てについて予めセッション鍵２２を利用して暗号化し、それらの暗号化したレスポンス候補の全てを処理装置２の記憶手段１８に記憶させておく。

その後、記憶手段１８に記憶させておいたセッション鍵２２を抹消処理して、処理装置

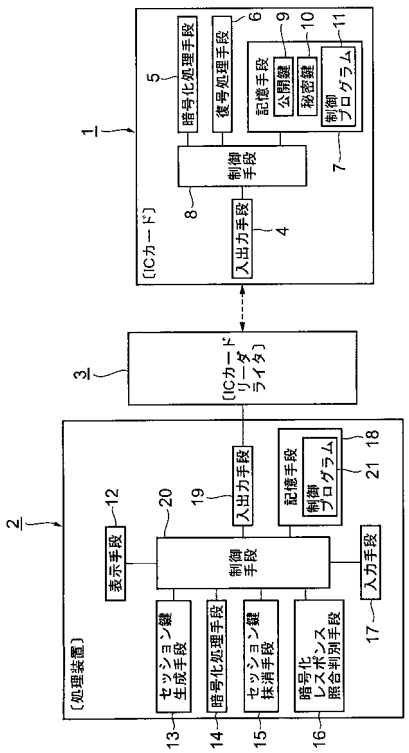
２内のどこにもセッション鍵２２が無い状態とする。
【００１８】
次に、セッション鍵２２で暗号化したコマンドメッセージを、処理装置２からＩＣカード１に送信する。
セッション鍵２２で暗号化したコマンドメッセージを受信したＩＣカード１では、ＩＣカード１の記憶手段７に記憶させておいたセッション鍵２２を利用して復号処理手段６により復号する。
【００１９】
そして、このコマンドメッセージに対するレスポンスを決定する。
次に、決定したレスポンスを、セッション鍵２２を利用して暗号化処理手段５により暗号化する。
次に、セッション鍵２２で暗号化したレスポンスを、ＩＣカード１から処理装置２に送信する。
【００２０】
セッション鍵２２で暗号化したレスポンスをＩＣカード１から受信した処理装置２では、処理装置２の記憶手段１８に予め記憶させておいた全てのレスポンス候補と、受信した暗号化されたレスポンスとの照合を行うことで、処理装置２がＩＣカード１から受信したレスポンスの内容の判別を行う。
以上の処理により、処理装置２の記憶手段１８から既にセッション鍵２２を抹消させておいたとしても、ＩＣカード１から受信した、セッション鍵２２で暗号化したレスポンスがどのような内容であるのかを判別可能にしてある。
【００２１】
本発明の処理装置２は、パソコンに限らず、ＩＣカード１とデータの送受信を行う種々の処理装置であれば適応可能であり、例えば携帯電話機やＡＴＭなどにも適応することができる。
【図面の簡単な説明】
【００２２】
【図１】本発明の実施形態に係る機密データの漏洩防止方法に用いる装置の外観図である。
【図２】本発明の実施形態に係る機密データの漏洩防止方法に用いるシステム構成のシステムブロック図である。
【図３】本発明の実施形態に係る機密データの漏洩防止方法における処理装置とＩＣカードの間でセッション鍵を共有する方法を説明する図である。
【図４】本発明の実施形態に係る機密データの漏洩防止方法の手順を説明する図である。
【符号の説明】
【００２３】
１　ＩＣカード
２　処理装置
３　ＩＣカードリーダライタ
４　入出力手段
５　暗号化処理手段
６　復号処理手段
７　記憶手段
８，２０　制御手段
９　公開鍵
１０　秘密鍵
１１　制御プログラム
１２　表示手段
１３　セッション鍵生成手段
１４　暗号化手段

１５　セッション鍵抹消手段
１６　暗号化レスポンス照合判別手段
１７　入力手段
１８　記憶手段
１９　入出力手段
２１　制御プログラム
２２　セッション鍵

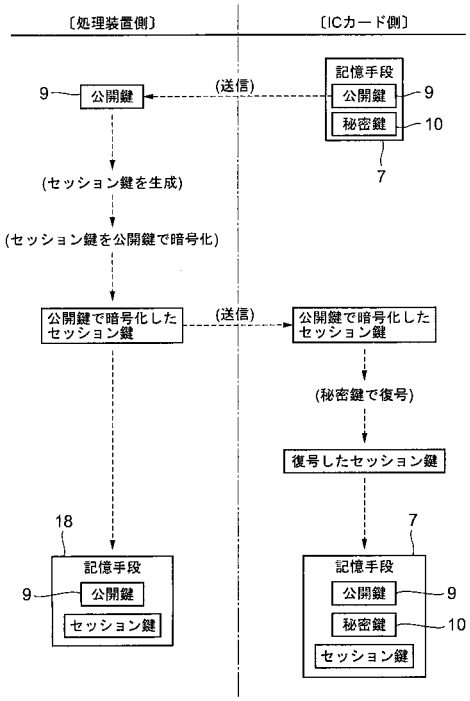
【図１】



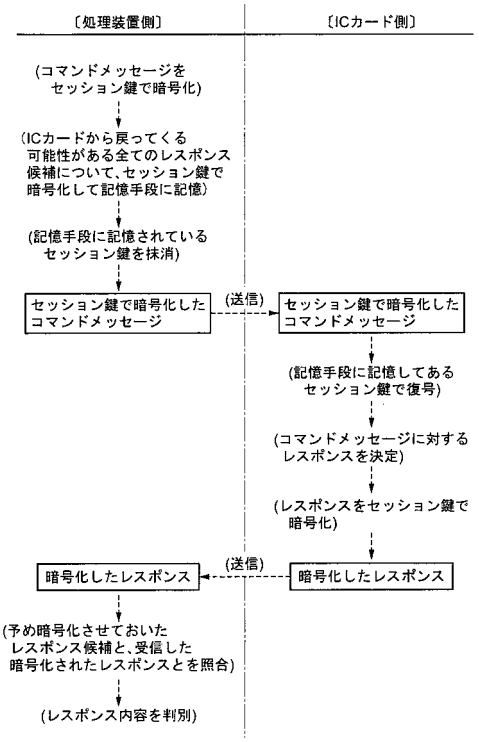
【図２】



【図３】


〔処理装置側〕
〔ICカード側〕
記憶手段
公開鍵
秘密鍵
9
10
7
(送信)
(セッション鍵を生成)
(セッション鍵を公開鍵で暗号化)
公開鍵で暗号化した
セッション鍵
(秘密鍵で復号)
復号したセッション鍵
18
セッション鍵

【図４】


〔処理装置側〕
〔ICカード側〕
(コマンドメッセージを
セッション鍵で暗号化)
(ICカードから戻ってくる
可能性がある全てのレスポンス
候補について、セッション鍵で
暗号化して記憶手段に記憶)
(記憶手段に記憶されている
セッション鍵を抹消)
セッション鍵で暗号化した
コマンドメッセージ
(送信)
(記憶手段に記憶してある
セッション鍵で復号)
(コマンドメッセージに対する
レスポンスを決定)
(レスポンスをセッション鍵で
暗号化)
暗号化したレスポンス
(予め暗号化させておいた
レスポンス候補と、受信した
暗号化されたレスポンスとを照合)
(レスポンス内容を判別)

フロントページの続き

(56)参考文献 特開平０７－３１１８１９（ＪＰ，Ａ）
特開平０７－１４０８９７（ＪＰ，Ａ）
特開２０００－０４８１４１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｇ０９Ｃ　　１／００