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

特許第5423280号
(P5423280)

(45)発行日　平成26年2月19日(2014.2.19)　(24)登録日　平成25年12月6日(2013.12.6)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
G09C 1/00	(2006.01)	G09C	1/00	640E
H04L 9/08	(2006.01)	H04L	9/00	601B
G06F 21/44	(2013.01)	G06F	21/20	144C
G06F 21/62	(2013.01)	G06F	21/24	165H

請求項の数 11　(全 20 頁)　最終頁に続く

(21)出願番号　特願2009-221300 (P2009-221300)
(22)出願日　平成21年9月25日 (2009.9.25)
(65)公開番号　特開2011-71758 (P2011-71758A)
(43)公開日　平成23年4月7日 (2011.4.7)
審査請求日　平成24年9月12日 (2012.9.12)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100082131
弁理士　稲本　義雄
(74)代理人　100121131
弁理士　西川　孝
(72)発明者　朱　瑩琳
東京都港区港南１丁目７番１号　ソニー株式会社内
(72)発明者　中村　光宏
東京都港区港南１丁目７番１号　ソニー株式会社内

最終頁に続く

(54)【発明の名称】通信装置、通信方法、情報処理装置、情報処理方法、プログラム、および通信システム

(57)【特許請求の範囲】
【請求項１】
情報処理装置と通信を行う通信装置において、
通信相手となる前記情報処理装置を探索するためのポーリングを行い、前記ポーリングに応じて前記情報処理装置が送信したターゲットＩＤを取得するポーリング手段と、
取得された前記ターゲットＩＤに含まれるターゲットコードに基づき、前記ターゲットＩＤが、前記情報処理装置の固有ＩＤであるか、または前記固有ＩＤの一部分が乱数により置換されている一部乱数化ＩＤであるかを判定する判定手段と、
前記ターゲットＩＤが前記固有ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤが前記一部乱数化ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない部分を作用させることによりアクセス鍵を生成するアクセス鍵生成手段と、
前記アクセス鍵を用いて前記情報処理装置と相互認証処理を行う認証手段と
を含む通信装置。
【請求項２】
前記情報処理装置において記憶されている、前記固有ＩＤ、または前記一部乱数化ＩＤの何方を前記ターゲットＩＤとして前記通信装置に送信するのかを示すターゲットＩＤ乱数化フラグの状態の変更を指示する指示手段を

さらに含む請求項１に記載の通信装置。
【請求項３】
前記ターゲットＩＤが前記一部乱数化ＩＤであると判定された場合、前記情報処理装置に対して、前記ターゲットＩＤとして送信する前記一部乱数化ＩＤの更新を要求する供給手段を
さらに含む請求項２に記載の通信装置。
【請求項４】
情報処理装置と通信を行う通信装置の通信方法において、
前記通信装置による、
通信相手となる前記情報処理装置を探索するためのポーリングを行い、前記ポーリングに応じて前記情報処理装置が送信したターゲットＩＤを取得するポーリングステップと、
取得された前記ターゲットＩＤに含まれるターゲットコードに基づき、前記ターゲットＩＤが、前記情報処理装置の固有ＩＤであるか、または前記固有ＩＤの一部分が乱数により置換されている一部乱数化ＩＤであるかを判定する判定ステップと、
前記ターゲットＩＤが前記固有ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤが前記一部乱数化ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない部分を作用させることによりアクセス鍵を生成するアクセス鍵生成ステップと、
前記アクセス鍵を用いて前記情報処理装置と相互認証処理を行う認証ステップと
を含む通信方法。
【請求項５】
情報処理装置と通信を行う通信装置の制御用のプログラムであって、
通信相手となる前記情報処理装置を探索するためのポーリングを行い、前記ポーリングに応じて前記情報処理装置が送信したターゲットＩＤを取得するポーリングステップと、
取得された前記ターゲットＩＤに含まれるターゲットコードに基づき、前記ターゲットＩＤが、前記情報処理装置の固有ＩＤであるか、または前記固有ＩＤの一部分が乱数により置換されている一部乱数化ＩＤであるかを判定する判定ステップと、
前記ターゲットＩＤが前記固有ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤが前記一部乱数化ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない部分を作用させることによりアクセス鍵を生成するアクセス鍵生成ステップと、
前記アクセス鍵を用いて前記情報処理装置と相互認証処理を行う認証ステップと
を含む処理を通信装置のコンピュータに実行させるプログラム。
【請求項６】
通信装置と通信を行う情報処理装置において、
自身の固有ＩＤの一部分を乱数で置換することにより一部乱数化ＩＤを生成する一部乱数化ＩＤ生成手段と、
前記固有ＩＤ、または前記一部乱数化ＩＤの何方をターゲットＩＤとして前記通信装置に送信するのかを示すターゲットＩＤ乱数化フラグを記憶する記憶手段と、
前記通信装置からのポーリングに応じ、前記ターゲットＩＤ乱数化フラグに従って、前記固有ＩＤ、または前記一部乱数化ＩＤを前記ターゲットＩＤとして送信する送信手段と、
前記ターゲットＩＤとして前記固有ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤとして前記一部乱数化ＩＤが送信された場合、予め保持

するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない真の部分を作用させることによりアクセス鍵を生成するアクセス鍵生成手段と、
前記アクセス鍵を用いて前記通信装置と相互認証処理を行う認証手段と
を含む情報処理装置。
【請求項７】
前記記憶手段は、前記通信装置からの指示に従い、前記ターゲットＩＤ乱数化フラグの状態を変更して記憶する
請求項６に記載の情報処理装置。
【請求項８】
前記一部乱数化ＩＤ生成手段は、前記通信装置からの要求に従い、前記一部乱数化ＩＤを再生成する
請求項７に記載の情報処理装置。
【請求項９】
通信装置と通信を行う情報処理装置の情報処理方法において、
前記情報処理装置による、
自身の固有ＩＤの一部分を乱数で置換することにより一部乱数化ＩＤを生成する一部乱数化ＩＤ生成ステップと、
前記通信装置からのポーリングに応じ、前記固有ＩＤ、または前記一部乱数化ＩＤの何方をターゲットＩＤとして前記通信装置に送信するのかを示すターゲットＩＤ乱数化フラグに従って、前記固有ＩＤ、または前記一部乱数化ＩＤを前記ターゲットＩＤとして送信する送信ステップと、
前記ターゲットＩＤとして前記固有ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤとして前記一部乱数化ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない真の部分を作用させることによりアクセス鍵を生成するアクセス鍵生成ステップと、
前記アクセス鍵を用いて前記通信装置と相互認証処理を行う認証ステップと
を含む情報処理方法。
【請求項１０】
通信装置と通信を行う情報処理装置の制御用のプログラムであって、
自身の固有ＩＤの一部分を乱数で置換することにより一部乱数化ＩＤを生成する一部乱数化ＩＤ生成ステップと、
前記通信装置からのポーリングに応じ、前記固有ＩＤ、または前記一部乱数化ＩＤの何方をターゲットＩＤとして前記通信装置に送信するのかを示すターゲットＩＤ乱数化フラグに従って、前記固有ＩＤ、または前記一部乱数化ＩＤを前記ターゲットＩＤとして送信する送信ステップと、
前記ターゲットＩＤとして前記固有ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤとして前記一部乱数化ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない真の部分を作用させることによりアクセス鍵を生成するアクセス鍵生成ステップと、
前記アクセス鍵を用いて前記通信装置と相互認証処理を行う認証ステップと
を含む処理を情報処理装置のコンピュータに実行させるプログラム。
【請求項１１】
通信装置と情報処理装置から構成される通信システムにおいて、
前記通信装置は、
通信相手となる前記情報処理装置を探索するためのポーリングを行い、前記ポーリン

グに応じて前記情報処理装置が送信したターゲットＩＤを取得するポーリング手段と、
　取得された前記ターゲットＩＤに含まれるターゲットコードに基づき、前記ターゲットＩＤが、前記情報処理装置の固有ＩＤであるか、または前記固有ＩＤの一部分が乱数により置換されている一部乱数化ＩＤであるかを判定する判定手段と、
　前記ターゲットＩＤが前記固有ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤが前記一部乱数化ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない部分を作用させることによりアクセス鍵を生成する第１のアクセス鍵生成手段と、
　前記アクセス鍵を用いて前記情報処理装置と相互認証処理を行う第１の認証手段と
を含み、
前記情報処理装置は、
　自身の前記固有ＩＤの一部分を乱数で置換することにより一部乱数化ＩＤを生成する一部乱数化ＩＤ生成手段と、
　前記固有ＩＤ、または前記一部乱数化ＩＤの何方を前記ターゲットＩＤとして前記通信装置に送信するのかを示すターゲットＩＤ乱数化フラグを記憶する記憶手段と、
　前記通信装置からの前記ポーリングに応じ、前記ターゲットＩＤ乱数化フラグに従って、前記固有ＩＤ、または前記一部乱数化ＩＤを前記ターゲットＩＤとして送信する送信手段と、
　前記ターゲットＩＤとして前記固有ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤとして前記一部乱数化ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない真の部分を作用させることによりアクセス鍵を生成する第２のアクセス鍵生成手段と、
　前記アクセス鍵を用いて前記通信装置と相互認証処理を行う第２の認証手段と
を含む
通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明は、通信装置、通信方法、情報処理装置、情報処理方法、プログラム、および通信システムに関し、特に、情報を非接触通信する場合に用いて好適な通信装置、通信方法、情報処理装置、情報処理方法、プログラム、および通信システムに関する。
【背景技術】
【０００２】
　従来、FeliCa（ソニー株式会社の登録商標）に代表される非接触通信システムが広く普及している。
【０００３】
　非接触通信システムは、リーダライタ（以下、Ｒ／Ｗと略記する）と非接触通信ＩＣカード（以下、単にＩＣカードと略記する）とから成り、Ｒ／ＷとＩＣカードとの間で電磁波を用いて非接触で情報を通信するものである。なお、各種の情報を通信する前に相互認証処理を行うようになされている。また、ＩＣカードの代わりに、ＩＣカードと同様の機能を有するＩＣチップを内蔵した携帯電話などが用いられることもある。
【０００４】
　ＩＣカードには、例えば、電子マネーとしてのサービス、電車の定期券などとしてのサービス、社員証などとしてのサービスなど、複数のサービスに関する情報を１枚のＩＣカードに搭載することが可能である。
【０００５】

ＩＣカード内のユーザデータに対するアクセス権やアクセス方式は、サービスと称する単位で制御される。このサービス毎にユーザデータにアクセスする鍵が存在し、この鍵によりたＴ九サービスに対応するユーザデータへのアクセス権が制御される。また、サービス毎に、履歴データの書き込み方式や電子マネーの減算方式などの用途に応じたアクセス方式が規定されている。

【０００６】

履歴データの書き込みと電子マネーの減算を一度行うためには、複数のサービスの鍵から１つの鍵(縮退鍵)が生成される、この縮退鍵を用いることで複数のサービスに対して一度の相互認証でアクセスすることが可能となる。ただし、個々のサービスでも、サービス毎に保持された鍵を用いて相互認証を行い、アクセスすることが可能である。

【０００７】

ただし、複数の異なるサービスを使用する、すなわち、各サービスに関する情報にアクセスするには、サービス毎に相互認証処理が必要であり、サービス毎に異なる鍵を用いて相互認証処理を行うとその処理が面倒となる。そこで、各サービスにそれぞれ対応する複数の鍵に基づいて１つの鍵（縮退鍵）を予め生成しておき、この縮退鍵を各サービスにおける相互認証処理に共通して用いる技術が実現されている（例えば、特許文献１参照）。

【０００８】

上述した縮退鍵を用いれば、相互認証処理に要する時間を短縮することができ、所望のサービスに関する情報に速やかにアクセスすることができる。

【０００９】

しかしながら、例えば、複数枚のＩＣカードで共通の縮退鍵を用いている状況において、縮退鍵が漏洩したりすると、前記複数枚のＩＣカードに保持されている共通の縮退鍵を変更する必要が生じてしまう。そこで、縮退鍵を直接的に用いるのではなく、各ＩＣカードの固有の識別情報（以下、固有ＩＤと称する）を縮退鍵に作用させることにより、縮退鍵をＩＣカード毎に個別化して用いる方法が提案されている（例えば、特許文献２参照）。

【先行技術文献】

【特許文献】

【００１０】

【特許文献１】特開平１０－３２７１４２号公報

【特許文献２】特開２００８－９９３３５号公報

【発明の概要】

【発明が解決しようとする課題】

【００１１】

上述したように、縮退鍵にＩＣカードの固有ＩＤを作用させることにより個別化してから相互認証処理に用いることにより、縮退鍵自身の漏洩を抑止することができる。しかしながら、この場合、ＩＣカードは自身の固有ＩＤをＲ／Ｗに通知する必要があるので、この通知過程において、ＩＣカードの固有ＩＤが第３者に漏洩してしまう可能性を否定できない。

【００１２】

漏洩したＩＣカードの固有ＩＤは、ＩＣカードのユーザに対する不正な同定追跡などに利用されてしまう可能性があるので、ＩＣカードの固有ＩＤが漏洩しないようにする必要がある。

【００１３】

本発明はこのような状況に鑑みてなされたものであり、縮退鍵を個別化して用いつつも、ＩＣカードの固有ＩＤの漏洩を抑止できるようにするものである。

【課題を解決するための手段】

【００１４】

本発明の第１の側面である通信装置は、情報処理装置と通信を行う通信装置において、通信相手となる前記情報処理装置を探索するためのポーリングを行い、前記ポーリングに

応じて前記情報処理装置が送信したターゲットＩＤを取得するポーリング手段と、取得された前記ターゲットＩＤに含まれるターゲットコードに基づき、前記ターゲットＩＤが、前記情報処理装置の固有ＩＤであるか、または前記固有ＩＤの一部分が乱数により置換されている一部乱数化ＩＤであるかを判定する判定手段と、前記ターゲットＩＤが前記固有ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤが前記一部乱数化ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない部分を作用させることによりアクセス鍵を生成するアクセス鍵生成手段と、前記アクセス鍵を用いて前記情報処理装置と相互認証処理を行う認証手段とを含む。

【００１５】

本発明の第１の側面である通信装置は、前記情報処理装置において記憶されている、前記固有ＩＤ、または前記一部乱数化ＩＤの何方を前記ターゲットＩＤとして前記通信装置に送信するのかを示すターゲットＩＤ乱数化フラグの状態の変更を指示する指示手段をさらに含むことができる。

【００１６】

本発明の第１の側面である通信装置は、前記ターゲットＩＤが前記一部乱数化ＩＤであると判定された場合、前記情報処理装置に対して、前記ターゲットＩＤとして送信する前記一部乱数化ＩＤの更新を要求する供給手段をさらに含むことができる。

【００１７】

本発明の第１の側面である通信方法は、情報処理装置と通信を行う通信装置の通信方法において、前記通信装置による、通信相手となる前記情報処理装置を探索するためのポーリングを行い、前記ポーリングに応じて前記情報処理装置が送信したターゲットＩＤを取得するポーリングステップと、取得された前記ターゲットＩＤに含まれるターゲットコードに基づき、前記ターゲットＩＤが、前記情報処理装置の固有ＩＤであるか、または前記固有ＩＤの一部分が乱数により置換されている一部乱数化ＩＤであるかを判定する判定ステップと、前記ターゲットＩＤが前記固有ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤが前記一部乱数化ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない部分を作用させることによりアクセス鍵を生成するアクセス鍵生成ステップと、前記アクセス鍵を用いて前記情報処理装置と相互認証処理を行う認証ステップとを含む。

【００１８】

本発明の第１の側面であるプログラムは、情報処理装置と通信を行う通信装置の制御用のプログラムであって、通信相手となる前記情報処理装置を探索するためのポーリングを行い、前記ポーリングに応じて前記情報処理装置が送信したターゲットＩＤを取得するポーリングステップと、取得された前記ターゲットＩＤに含まれるターゲットコードに基づき、前記ターゲットＩＤが、前記情報処理装置の固有ＩＤであるか、または前記固有ＩＤの一部分が乱数により置換されている一部乱数化ＩＤであるかを判定する判定ステップと、前記ターゲットＩＤが前記固有ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤが前記一部乱数化ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない部分を作用させることによりアクセス鍵を生成するアクセス鍵生成ステップと、前記アクセス鍵を用いて前記情報処理装置と相互認証処理を行う認証ステップとを含む処理を通信装置のコンピュータに実行させる。

【００１９】

本発明の第１の側面においては、通信相手となる情報処理装置を探索するためのポーリングが行われ、前記ポーリングに応じて前記情報処理装置が送信したターゲットＩＤが取

得され、取得された前記ターゲットＩＤに含まれるターゲットコードに基づき、前記ターゲットＩＤが、前記情報処理装置の固有ＩＤであるか、または前記固有ＩＤの一部分が乱数により置換されている一部乱数化ＩＤであるかが判定される。さらに、前記ターゲットＩＤが前記固有ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤが作用されることによりアクセス鍵が生成され、前記ターゲットＩＤが前記一部乱数化ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない部分が作用されることによりアクセス鍵が生成される。そして、前記アクセス鍵を用いて前記情報処理装置と相互認証処理が行われる。

【００２０】

本発明の第２の側面である情報処理装置は、通信装置と通信を行う情報処理装置において、自身の固有ＩＤの一部分を乱数で置換することにより一部乱数化ＩＤを生成する一部乱数化ＩＤ生成手段と、前記固有ＩＤ、または前記一部乱数化ＩＤの何方をターゲットＩＤとして前記通信装置に送信するのかを示すターゲットＩＤ乱数化フラグを記憶する記憶手段と、前記通信装置からのポーリングに応じ、前記ターゲットＩＤ乱数化フラグに従って、前記固有ＩＤ、または前記一部乱数化ＩＤを前記ターゲットＩＤとして送信する送信手段と、前記ターゲットＩＤとして前記固有ＩＤが送信された場合、予めＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤとして前記一部乱数化ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない真の部分を作用させることによりアクセス鍵を生成するアクセス鍵生成手段と、前記アクセス鍵を用いて前記通信装置と相互認証処理を行う認証手段とを含む。

【００２１】

前記記憶手段は、前記通信装置からの指示に従い、前記ターゲットＩＤ乱数化フラグの状態を変更して記憶するようにすることができる。

【００２２】

前記一部乱数化ＩＤ生成手段は、前記通信装置からの要求に従い、前記一部乱数化ＩＤを再生成するようにすることができる。

【００２３】

本発明の第２の側面である情報処理方法は、通信装置と通信を行う情報処理装置の情報処理方法において、前記情報処理装置による、自身の固有ＩＤの一部分を乱数で置換することにより一部乱数化ＩＤを生成する一部乱数化ＩＤ生成ステップと、前記通信装置からのポーリングに応じ、前記固有ＩＤ、または前記一部乱数化ＩＤの何方をターゲットＩＤとして前記通信装置に送信するのかを示すターゲットＩＤ乱数化フラグに従って、前記固有ＩＤ、または前記一部乱数化ＩＤを前記ターゲットＩＤとして送信する送信ステップと、前記ターゲットＩＤとして前記固有ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤとして前記一部乱数化ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない真の部分を作用させることによりアクセス鍵を生成するアクセス鍵生成ステップと、前記アクセス鍵を用いて前記通信装置と相互認証処理を行う認証ステップとを含む。

【００２４】

本発明の第２の側面であるプログラムは、通信装置と通信を行う情報処理装置の制御用のプログラムであって、自身の固有ＩＤの一部分を乱数で置換することにより一部乱数化ＩＤを生成する一部乱数化ＩＤ生成ステップと、前記通信装置からのポーリングに応じ、前記固有ＩＤ、または前記一部乱数化ＩＤの何方をターゲットＩＤとして前記通信装置に送信するのかを示すターゲットＩＤ乱数化フラグに従って、前記固有ＩＤ、または前記一部乱数化ＩＤを前記ターゲットＩＤとして送信する送信ステップと、前記ターゲットＩＤ

として前記固有ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤとして前記一部乱数化ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない真の部分を作用させることによりアクセス鍵を生成するアクセス鍵生成ステップと、前記アクセス鍵を用いて前記通信装置と相互認証処理を行う認証ステップとを含む処理を情報処理装置のコンピュータに実行させる。

【００２５】

本発明の第２の側面においては、自身の固有ＩＤの一部分を乱数で置換することにより一部乱数化ＩＤが生成され、通信装置からのポーリングに応じ、前記固有ＩＤ、または前記一部乱数化ＩＤの何方をターゲットＩＤとして前記通信装置に送信するのかを示すターゲットＩＤ乱数化フラグに従って、前記固有ＩＤ、または前記一部乱数化ＩＤが前記ターゲットＩＤとして送信される。また、前記ターゲットＩＤとして前記固有ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤが作用されることによりアクセス鍵が生成され、前記ターゲットＩＤとして前記一部乱数化ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない真の部分が作用されることによりアクセス鍵が生成される。さらに、前記アクセス鍵を用いて前記通信装置と相互認証処理が行われる。

【００２６】

本発明の第３の側面である通信システムは、通信装置と情報処理装置から構成される通信システムにおいて、前記通信装置が、通信相手となる前記情報処理装置を探索するためのポーリングを行い、前記ポーリングに応じて前記情報処理装置が送信したターゲットＩＤを取得するポーリング手段と、取得された前記ターゲットＩＤに含まれるターゲットコードに基づき、前記ターゲットＩＤが、前記情報処理装置の固有ＩＤであるか、または前記固有ＩＤの一部分が乱数により置換されている一部乱数化ＩＤであるかを判定する判定手段と、前記ターゲットＩＤが前記固有ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤが前記一部乱数化ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない部分を作用させることによりアクセス鍵を生成する第１のアクセス鍵生成手段と、前記アクセス鍵を用いて前記情報処理装置と相互認証処理を行う第１の認証手段とを含み、前記情報処理装置が、自身の前記固有ＩＤの一部分を乱数で置換することにより一部乱数化ＩＤを生成する一部乱数化ＩＤ生成手段と、前記固有ＩＤ、または前記一部乱数化ＩＤの何方を前記ターゲットＩＤとして前記通信装置に送信するのかを示すターゲットＩＤ乱数化フラグを記憶する記憶手段と、前記通信装置からの前記ポーリングに応じ、前記ターゲットＩＤ乱数化フラグに従って、前記固有ＩＤ、または前記一部乱数化ＩＤを前記ターゲットＩＤとして送信する送信手段と、前記ターゲットＩＤとして前記固有ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤを作用させることによりアクセス鍵を生成し、前記ターゲットＩＤとして前記一部乱数化ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない真の部分を作用させることによりアクセス鍵を生成する第２のアクセス鍵生成手段と、前記アクセス鍵を用いて前記通信装置と相互認証処理を行う第２の認証手段と
を含む。

【００２７】

本発明の第３の側面においては、一方の通信装置により、通信相手となる情報処理装置を探索するためのポーリングが行われ、前記ポーリングに応じて前記情報処理装置が送信したターゲットＩＤが取得され、取得された前記ターゲットＩＤに含まれるターゲットコ

ードに基づき、前記ターゲットＩＤが、前記情報処理装置の固有ＩＤであるか、または前記固有ＩＤの一部分が乱数により置換されている一部乱数化ＩＤであるかが判定される。さらに、前記ターゲットＩＤが前記固有ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤが作用されることによりアクセス鍵が生成され、前記ターゲットＩＤが前記一部乱数化ＩＤであると判定された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない部分が作用されることによりアクセス鍵が生成される。また、他方の情報処理装置により、自身の固有ＩＤの一部分を乱数で置換することにより一部乱数化ＩＤが生成され、通信装置からのポーリングに応じ、前記固有ＩＤ、または前記一部乱数化ＩＤの何方をターゲットＩＤとして前記通信装置に送信するのかを示すターゲットＩＤ乱数化フラグに従って、前記固有ＩＤ、または前記一部乱数化ＩＤが前記ターゲットＩＤとして送信される。また、前記ターゲットＩＤとして前記固有ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記固有ＩＤが作用されることによりアクセス鍵が生成され、前記ターゲットＩＤとして前記一部乱数化ＩＤが送信された場合、予め保持するＩＣチップ内のユーザデータにアクセスするための鍵に前記一部乱数化ＩＤのうちの前記乱数により置換されていない真の部分が作用されることによりアクセス鍵が生成される。そして、前記通信装置と前記情報処理装置との間で前記アクセス鍵を用いて相互認証処理が行われる。

【発明の効果】

【００２８】

本発明の第１の側面によれば、情報処理装置から送信されたターゲットＩＤを縮退鍵に作用させることによりアクセス鍵を生成して相互認証処理を行うことができる。

【００２９】

本発明の第２の側面によれば、通信処理装置からのポーリングに応じ、ターゲットＩＤ乱数化フラグに従って、固有ＩＤ、または一部乱数化ＩＤをターゲットＩＤとして送信することができる。

【００３０】

本発明の第３の側面によれば、通信処理装置からのポーリングに応じ、情報処理装置はターゲットＩＤ乱数化フラグに従って、固有ＩＤ、または一部乱数化ＩＤをターゲットＩＤとして送信することができる。よって、ターゲットＩＤ乱数化フラグを、一部乱数化ＩＤをターゲットＩＤとして送信するように設定すれば、情報処理装置の固有ＩＤの漏洩を抑止することができる。

【図面の簡単な説明】

【００３１】

【図１】本発明を適用した非接触通信システムの構成例を示すブロック図である。

【図２】Ｒ／ＷおよびＩＣカードの機能的な構成例を示すブロック図である。

【図３】ターゲットＩＤのデータ構造を示す図である。

【図４】縮退鍵の個別化について説明するための図である。

【図５】図２のＲ／ＷとＩＣカードによる通信処理を説明するフローチャートである。

【図６】図２のＩＣカードの処理を説明するフローチャートである。

【図７】図２のＲ／Ｗの処理を説明するフローチャートである。

【図８】従来のＲ／Ｗの処理を説明するフローチャートである。

【発明を実施するための形態】

【００３２】

以下、発明を実施するための最良の形態（以下、実施の形態と称する）について、図面を参照しながら詳細に説明する。

＜１．実施の形態＞

［非接触通信システムの構成例］

図１は、本発明の第１の実施の形態である非接触通信システムの構成例を示している。この非接触通信システム１は、Ｒ／Ｗ１０とＩＣカード２０から構成される。ＩＣカード

２０は、ユーザによりＲ／Ｗ１０に近づけられることにより、その内部で駆動電力を発生するようになされている。

【００３３】

Ｒ／Ｗ１０は、CPU１１を内蔵しており、CPU１１にはバス１５を介してROM１２、RAM１３、NVM(non volatile memory)１４、および変復調回路１６が接続されている。CPU１１は、ROM１２に予め記憶されている制御用プログラムを実行することにより、Ｒ／Ｗ１０の各部を制御する。RAM１３は、CPU１１が各種の処理を行う際の作業領域として利用される。NVM１４には、縮退鍵が保持されている。

【００３４】

変復調回路１６は、CPU１１から出力され、バス１５を介して入力される、ＩＣカード２０に送信するための情報によって搬送波を変調してアンテナ１７に出力する。また、変復調回路１６は、アンテナ１７が受信した受信波を復調し、その結果得られるＩＣカード２０からの情報を、バス１５を介してCPU１１に出力する。アンテナ１７は、変復調回路１６から入力される変調波を送信するとともに、ＩＣカード２０から送信された変調波を受信して変復調回路１６に出力する。

【００３５】

ＩＣカード２０は、CPU２１を内蔵しており、CPU２１にはバス２５を介してROM２２、RAM２３、NVM２４、および変復調回路２６が接続されている。CPU２１は、ROM２２に予め記憶されている制御用プログラムを実行することにより、ＩＣカード２０の各部を制御する。RAM２３は、CPU２１が各種の処理を行う際の作業領域として利用される。NVM２４には、縮退鍵や各種のサービス（電子マネー、電車の定期券、社員証などとしてのサービス）に関する情報がサービス毎に階層化されて記憶されている。

【００３６】

変復調回路２６は、アンテナ２７が受信した、Ｒ／Ｗ１０からの搬送波を復調し、その結果得られるＲ／Ｗ１０からの情報を、バス２５を介してCPU２１に出力する。また、変復調回路２６は、CPU２１から出力され、バス２５を介して入力される、Ｒ／Ｗ１０に送信するための情報によって搬送波を変調し、アンテナ２７に出力する。アンテナ２７は、Ｒ／Ｗ１０から送信された変調波を受信して変復調回路２６に出力するとともに、変復調回路２６から入力される変調波を送信する。

【００３７】

次に、図２は、Ｒ／Ｗ１０のCPU１１とＩＣカード２０のCPU２１が、それぞれ制御用プログラムを実行することにより実現される機能ブロック図を示している。

【００３８】

Ｒ／Ｗ１０においては、通信部５１、ターゲットコード判定部５２、アクセス鍵生成部５３、鍵管理部５４、およびデータ処理部５５が実現される。

【００３９】

通信部５１は、ＩＣカード２０との間の通信を制御する。ターゲットコード判定部５２は、ＩＣカード２０から通知されるターゲットＩＤのうちのターゲットコードを読み出して、当該ターゲットＩＤがカード固有ＩＤであるか、一部乱数化ＩＤであるかを判定する。

【００４０】

アクセス鍵生成部５３は、ターゲットコード判定部５２に判定結果に基づいて縮退鍵を個別化することによりアクセス鍵を生成する。なお、縮退鍵の個別化については、図４を参照して後述する。

【００４１】

鍵管理部５４は、予め保持されている縮退鍵、および生成されたアクセス鍵を管理する。データ処理部５５は、通信部５１を介し、生成されたアクセス鍵を用いてＩＣカード２０と相互認証処理を行う。また、データ処理部５５は、相互認証処理後において、ＩＣカード２０から送信される、暗号化された情報を復号したり、ＩＣカード２０に送信する情報を暗号化したりする。

【００４２】
ＩＣカード２０においては、通信部６１、ターゲットＩＤ出力部６２、フラグ保持部６３、乱数発生部６４、アクセス鍵生成部６５、鍵管理部６６、およびデータ処理部６７が実現される。
【００４３】
通信部６１は、Ｒ／Ｗ１０との間の通信を制御する。ターゲットＩＤ出力部６２は、フラグ保持部６３が保持するフラグの状態に応じ、カード固有ＩＤをターゲットＩＤとして出力するか、またはカード固有ＩＤの一部を乱数などで置換することにより生成した一部乱数化ＩＤをターゲットＩＤとして出力する。なお、カード固有ＩＤは、NVM２４に予め記憶されている。また、一部乱数化ＩＤは、ターゲットＩＤ出力部６２により所定のタイミングで生成されてNVM２４に記憶されている。一部乱数化ＩＤの生成については、図３を参照して後述する。
【００４４】
フラグ保持部６３は、ターゲットＩＤとして、従来どおりカード固有ＩＤをそのまま用いるか、または一部乱数化ＩＤを用いるかを示すターゲットＩＤ乱数化フラグが予め設定されている。以下、当該ターゲットＩＤ乱数化フラグが無効の場合、従来どおりカード固有ＩＤをそのまま用いることとし、当該ターゲットＩＤ乱数化フラグが有効の場合、一部乱数化ＩＤを用いることとする。
【００４５】
すなわち、このＩＣカード２０は、ユーザに引き渡される前の段階において、Ｒ／Ｗ１０に対して通知するターゲットＩＤとして、カード固有ＩＤをそのまま用いるか、または一部乱数化ＩＤを用いるかが決定されている。
【００４６】
ただし、フラグ保持部６３に保持されているターゲットＩＤ乱数化フラグの有効／無効は、Ｒ／Ｗ１０からの所定のコマンドに応じて切り替えることができる。
【００４７】
したがって、例えば、本発明を適用したＲ／Ｗ１０が社会に広く普及するまでは、ターゲットＩＤとしてカード固有ＩＤを通知するようにターゲットＩＤ乱数化フラグを無効に設定しておき、従来のＲ／Ｗが廃止されてＲ／Ｗ１０が社会に広く普及した後において、ターゲットＩＤとして一部乱数化ＩＤを通知するようにターゲットＩＤ乱数化フラグを有効に設定し直すことができる。
【００４８】
乱数発生部６４は、ターゲットＩＤ出力部６２からの要求に応じて乱数を発生する。アクセス鍵生成部６５は、所定にタイミングにおいて、生成されたターゲットＩＤのターゲットコードに基づいて縮退鍵を個別化することによりアクセス鍵を生成する。鍵管理部６６は、NVM２４に予め保持されている縮退鍵を管理する。なお、縮退鍵の個別化については、図４を参照して後述する。
【００４９】
データ処理部６７は、通信部６１を介し、生成されたアクセス鍵を用いてＲ／Ｗ１０と相互認証処理を行う。また、データ処理部６７は、相互認証処理後において、Ｒ／Ｗ１０から送信される、暗号化された情報を復号したり、Ｒ／Ｗ１０に送信する情報を暗号化したりする。
【００５０】
なお、上述したように、図２に示された各機能ブロックは、ソフトウェア（制御用プログラム）により実現されるが、これらをハードウェアとして実装するようにしてもよい。
【００５１】
［一部乱数化ＩＤの生成について］
図３は、ＩＣカード２０のターゲットＩＤ出力部６２によるターゲットＩＤの生成過程を説明するための図である。
【００５２】

同図Ａは、ＩＣカード２０に予め付与され、NVM２４などに記憶されているカード固有ＩＤのデータ構造を示している。カード固有ＩＤは、例えば８バイトＤ０乃至Ｄ７の情報量を有し、そのMSB(Most Significant Bit)側から順に、４ビットのシステム番号、１２ビットの製造者コード、６バイトのカードナンバが記録されている。同一の製造者によって製造されたＩＣカード２０は、システム番号および製造者コードが共通である。したがって、６バイトのカードナンバが、ＩＣカード２０の実質的な固有情報となる。

【００５３】

同図Ｂは、ターゲットＩＤ出力部６２において生成される一部乱数化ＩＤのデータ構造を示している。すなわち、一部乱数化ＩＤは、カード固有ＩＤのうちの、製造者コードが所定の値からなるＩＤｒコードに置換されているとともに、６バイトのカードナンバのMSB側の所定のｎバイト（同図の場合、４バイト）が乱数発生部６４により発生された乱数で置換されている。ここで、ｎは１以上６未満の整数とする。

【００５４】

したがって、ＩＣカード２０からターゲットＩＤとして、同図Ａのカード固有ＩＤ、または同図Ｂの一部乱数化ＩＤがＲ／Ｗ１０に通知された場合、システム番号に続く１２ビットをみれば、当該ターゲットＩＤがカード固有ＩＤであるか、または一部乱数化ＩＤであるかを判定することができる。

【００５５】

なお、以下において同図Ｃに示すように、システム番号に続く１２ビットを、ターゲットコードと称し、それに続く６バイトＤ２乃至Ｄ７をターゲットＩＤ下位６バイトと称する。

【００５６】

［縮退鍵の個別化について］

図４は、Ｒ／Ｗ１０のアクセス鍵生成部５３、およびＩＣカード２０のアクセス鍵生成部６５のそれぞれにおいて行われる、縮退鍵の個別化について説明するための図である。

【００５７】

同図に示すように、縮退鍵の個別化は、縮退鍵に対して個別化コードを作用させる、例えば、縮退鍵に個別化コードを加算することにより実行する。以下、個別化処理の結果得られる個別化された縮退鍵をアクセス鍵と称する。

【００５８】

ここで、個別化コードとは、個別化コードの入力パラメータによって生成されるものである。ただし、個別化コードとして入力パラメータをそのまま使用してもよい。

【００５９】

ターゲットＩＤがカード固有ＩＤである場合には、ターゲットＩＤの下位６バイト、すなわち、カードナンバの全体が個別化コードの入力パラメータとされる。また、ターゲットＩＤが一部乱数化ＩＤである場合には、ターゲットＩＤの下位（６－ｎ）バイト、すなわち、ターゲットＩＤ下位６バイトから乱数部分を除いたカードナンバの下位（６－ｎ）バイトが個別化コードの入力パラメータとされる。同図の場合、ターゲットＩＤが一部乱数化ＩＤであるので、ターゲットＩＤの下位２バイトＤ６，Ｄ７が個別化コードの入力パラメータとされる。

【００６０】

［非接触通信システム１の動作説明］

次に、非接触通信システム１による通信処理の概要について説明する。図５は、非接触通信システム１による通信処理を説明するフローチャートである。

【００６１】

初めに、ステップＳ１においては、ポーリング処理が行われる。すなわち、Ｒ／Ｗ１０が通信相手となるＩＣカード２０を探索するためのポーリング処理を行うと、これに応じたＩＣカード２０が自己のターゲットＩＤ（一部乱数化ＩＤ、またはカード固有ＩＤ）をＲ／Ｗ１０に通知する。

【００６２】

ステップＳ２においては、相互認証処理が行われる。すなわち、一方のＲ／Ｗ１０では、ＩＣカード２０から通知されたターゲットＩＤから個別化コードを抽出して縮退鍵に作用させることにより個別化し、その結果としてアクセス鍵を得る。他方のＩＣカード２０では、Ｒ／Ｗ１０に通知したターゲットＩＤから個別化コードを抽出して縮退鍵に作用させることにより個別化し、その結果としてアクセス鍵を得る。これにより、Ｒ／Ｗ１０とＩＣカード２０とが同一のアクセス鍵を得たことになるので、これを用いて相互認証処理が行われる。

【００６３】

ステップＳ３においては、ユーザブロックアクセス処理が行われる。すなわち、Ｒ／Ｗ１０が図示せぬコントローラからの指示に従い、ＩＣカード２０に記録されている情報を読み出したり、ＩＣカード２０に記録されている情報を書き換えたり、ＩＣカード２０に新たな情報を書き込んだりする処理を行う。

【００６４】

ステップＳ４においては、乱数変更処理が行われる。この乱数変更処理は、ＩＣカード２０がターゲットＩＤとして一部乱数化ＩＤを通知するように設定されている場合のみ、Ｒ／Ｗ１０からの所定のコマンドに従ってＩＣカード２０が実行する。具体的には、ターゲットＩＤとしての一部乱数化ＩＤに含まれる乱数を変更して一部乱数化ＩＤを更新する処理を行う。

【００６５】

なお、ステップＳ４の乱数変更処理は、通信処理が行われる毎に必ずしも毎回実行しなくてもよい。すなわち、Ｒ／Ｗ１０が必要に応じて上記所定のコマンドを用い、ＩＣカード２０に乱数変更処理を実行させるようにすればよい。

【００６６】

［ＩＣカード２０の動作説明］

次に、通信処理におけるＩＣカード２０の処理について詳述する。図６は、ＩＣカード２０の処理を説明するフローチャートである。この処理は、ＩＣカード２０がユーザによりＲ／Ｗ１０に近づけられたことにより、その内部において駆動電力が発生したときに開始される。

【００６７】

なお、ＩＣカード２０においては、既にターゲットＩＤ出力部６２によって生成された一部乱数化ＩＤがNVM２４に保持されているものとする。

【００６８】

ステップＳ１１において、ＩＣカード２０の通信部６１は、Ｒ／Ｗ１０からのポーリングを受けるまで待機し、ポーリングを受けた場合、処理をステップＳ１２に進める。

【００６９】

ステップＳ１２において、ターゲットＩＤ出力部６２は、フラグ保持部６３が保持するターゲットＩＤ乱数化フラグの状態を判定する。ここで、ターゲットＩＤ乱数化フラグが有効であると判定された場合、処理はステップＳ１３以降に進められて、ターゲットＩＤとして一部乱数化ＩＤがＲ／Ｗ１０に通知されることになる。

【００７０】

すなわち、ステップＳ１３において、ターゲットＩＤ出力部６２は、前回生成してNVM２４に記憶されている一部乱数化ＩＤを読み出して通信部６１およびアクセス鍵生成部６５に出力する。なお、ここでは、一部乱数化ＩＤが既に生成されていることを前提としているが、何らかの理由により生成されていない場合には、ステップＳ１３において、一部乱数化ＩＤを生成するようにすればよい。

【００７１】

ステップＳ１４において、通信部６１は、ターゲットＩＤ出力部６２から入力された一部乱数化ＩＤをターゲットＩＤとしてＲ／Ｗ１０に送信する。

【００７２】

ステップＳ１５において、アクセス鍵生成部６５は、鍵管理部６６に縮退鍵を読み出さ

せ、読み出した縮退鍵に、ターゲットＩＤ出力部６２から入力された一部乱数化ＩＤのカードナンバ下位２バイトを作用させてアクセス鍵を生成し、データ処理部６７に出力する。

【００７３】

ステップＳ１６において、データ処理部６７は、通信部６１を介し、生成されたアクセス鍵を用いてＲ／Ｗ１０と相互認証処理を行う。相互認証処理が成功した後、ステップＳ１７において、データ処理部６７は、ユーザブロックアクセス処理を行う。すなわち、Ｒ／Ｗ１０からの要求に応じ、NVM２４に対して情報の読み出しや書き込みを行う。

【００７４】

ステップＳ１８において、ターゲットＩＤ出力部６２は、Ｒ／Ｗ１０から乱数変更コマンドが送信されたか否かを判定する。乱数変更コマンドが送信されたと判定された場合、処理はステップＳ１９に進められる。ステップＳ１９において、ターゲットＩＤ出力部６２は、乱数発生部６４に乱数を発生させて、この乱数を用いて、現在の一部乱数化ＩＤの乱数部分を置換することにより、一部乱数化ＩＤを再生成してNVM２４に記憶させる。ここで、再生成された一部乱数化ＩＤは、次回の通信処理時にＩＣカード２０からＲ／Ｗ１０に通知されるターゲットＩＤとして利用される。以上で、ＩＣカード２０の処理は終了される。

【００７５】

ところで、ステップＳ１２において、ターゲットＩＤ乱数化フラグが無効であると判定された場合には、処理はステップＳ２２以降に進められて、ターゲットＩＤとしてカード固有ＩＤがＲ／Ｗ１０に通知されることになる。

【００７６】

すなわち、ステップＳ２０において、ターゲットＩＤ出力部６２は、NVM２４に記憶されているカード固有ＩＤを読み出して通信部６１およびアクセス鍵生成部６５に出力する。

【００７７】

ステップＳ２１において、通信部６１は、ターゲットＩＤ出力部６２から入力されたカード固有ＩＤをターゲットＩＤとしてＲ／Ｗ１０に送信する。

【００７８】

ステップＳ２２において、アクセス鍵生成部６５は、鍵管理部６６に縮退鍵を読み出させ、読み出した縮退鍵に、ターゲットＩＤ出力部６２から入力されたカード固有ＩＤの６バイトのカードナンバを作用させてアクセス鍵を生成し、データ処理部６７に出力する。

【００７９】

ステップＳ２３において、データ処理部６７は、通信部６１を介し、生成されたアクセス鍵を用いてＲ／Ｗ１０と相互認証処理を行う。相互認証処理が成功した後、ステップＳ１７において、データ処理部６７は、ユーザブロックアクセス処理を行う。以上で、ＩＣカード２０の処理は終了される。

【００８０】

以上で、ＩＣカード２０の処理の説明を終了する。

【００８１】

なお、上述した説明においては、ポーリングを受ける毎にターゲットＩＤ乱数化フラグが有効であるか、または無効であるかを判定するようにしたが、これを省略し、予め一部乱数化ＩＤまたはカード固有ＩＤをターゲットＩＤに対応付けておくようにしてもよい。

【００８２】

また、上述した説明においては、ターゲットＩＤとして一部乱数化ＩＤをＲ／Ｗ１０に通知するに際し、予め生成されて記憶されている一部乱数化ＩＤを読み出して通知するようにしたが、通知毎に乱数を発生し、一部乱数化ＩＤを生成するようにしてもよい。

【００８３】

以上説明したように、ＩＣカード２０のフラグ保持部６３に保持させるターゲットＩＤ乱数化フラグを有効に設定しておけば、ＩＣカード２０からＲ／Ｗ１０に対し、ターゲッ

トＩＤとして一部乱数化ＩＤが通知される。したがって、ＩＣカード２０のカード固有ＩＤの漏洩を抑止することができる。

【００８４】

［Ｒ／Ｗ１０の動作説明］

次に、通信処理におけるＲ／Ｗ１０の処理について詳述する。図７は、Ｒ／Ｗ１０の処理を説明するフローチャートである。この処理は、図示せぬコントローラからの制御に従って開始される。

【００８５】

ステップＳ５１において、Ｒ／Ｗ１０の通信部５１は、ポーリングを行い、Ｒ／Ｗ１０に近づけられたＩＣカード２０からターゲットＩＤを取得し、取得したターゲットＩＤをターゲットコード判定部５２に出力する。

【００８６】

ステップＳ５２において、ターゲットコード判定部５２は、ターゲットＩＤのターゲットコードがＩＤｒコードであるか、または製造者コードであるかを判定し、その判定結果とターゲットＩＤをアクセス鍵生成部５３に通知する。ここで、ターゲットコードがＩＤｒコードであると判定された場合、処理はステップＳ５３に進められる。この場合、ＩＣカード２０から通知されたターゲットＩＤは一部乱数化ＩＤである。

【００８７】

ステップＳ５３において、アクセス鍵生成部５３は、鍵管理部５４に縮退鍵を読み出させ、縮退鍵に対して、ターゲットＩＤ（一部乱数化ＩＤ）のカードナンバ下位２バイトを個別化コードの入力パラメータとして作用させることによりアクセス鍵を生成し、データ処理部５５に出力する。

【００８８】

ステップＳ５４において、データ処理部５５は、通信部５１を介し、生成されたアクセス鍵を用いてＩＣカード２０と相互認証処理を行う。相互認証処理が成功した後、ステップＳ５５において、データ処理部５５は、ユーザブロックアクセス処理を行う。すなわち、ＩＣカード２０に対して情報の読み出しや書き込みを行う。

【００８９】

ステップＳ５６において、通信部５６は、ＩＣカード２０に対して乱数変更コマンドを送信する。この乱数変更コマンドに応じ、ＩＣカード２０では一部乱数化ＩＤが再生成されることになる。なお、ステップＳ５６に処理は省略してもよい。あるいは、例えば、所定の時間帯に通信処理が行われた場合にのみ、この乱数変更コマンドを送信するようにしてもよい。以上で、Ｒ／Ｗ１０の処理は終了される。

【００９０】

なお、ステップＳ５２において、ターゲットコードが製造者コードであると判定された場合、処理はステップＳ５７に進められる。この場合、ＩＣカード２０から通知されたターゲットＩＤはカード固有ＩＤである。

【００９１】

ステップＳ５７において、アクセス鍵生成部５３は、鍵管理部５４に縮退鍵を読み出させ、縮退鍵に対して、ターゲットＩＤ（カード固有ＩＤ）のカードナンバ６バイトを個別化コードの入力パラメータとして作用させることによりアクセス鍵を生成し、データ処理部５５に出力する。

【００９２】

ステップＳ５８において、データ処理部５５は、通信部５１を介し、生成されたアクセス鍵を用いてＩＣカード２０と相互認証処理を行う。相互認証処理が成功した後、ステップＳ５９において、データ処理部５５は、ユーザブロックアクセス処理を行う。すなわち、ＩＣカード２０に対して情報の読み出しや書き込みを行う。以上で、Ｒ／Ｗ１０の処理は終了される。

【００９３】

［ＩＣカード２０と通信を行う従来のＲ／Ｗの動作説明］

次に、ＩＣカード２０と通信を行う従来のＲ／Ｗの処理について詳述する。図８は、従来のＲ／Ｗの処理を説明するフローチャートである。なお、従来のＲ／Ｗと通信を行う可能性があるＩＣカード２０は、そのターゲットＩＤ乱数化フラグが無効とされているものとする。

【００９４】

ステップＳ７１において、従来のＲ／Ｗはポーリングを行い、従来のＲ／Ｗに近づけられたＩＣカード２０からターゲットＩＤ（カード固有ＩＤ）を取得する。

【００９５】

ステップＳ７２において、従来のＲ／Ｗは、予め保持している縮退鍵に、取得したターゲットＩＤ（カード固有ＩＤ）のカードナンバ６バイトを個別化コードの入力パラメータとして作用させることによりアクセス鍵を生成する。

【００９６】

ステップＳ７３において、従来のＲ／Ｗは、生成したアクセス鍵を用いてＩＣカード２０と相互認証処理を行う。相互認証処理が成功した後、ステップＳ７４において、ユーザブロックアクセス処理を行う。以上で、従来のＲ／Ｗの処理は終了される。

【００９７】

以上説明したように、ＩＣカード２０のターゲットＩＤ乱数化フラグを無効としておくことにより、ＩＣカード２０は、従来のＲ／Ｗとも通信処理を行うことができる。

【００９８】

なお、本発明の情報処理装置は、本実施の形態であるＩＣカード２０に限らず、ＩＣカード２０と同等のＩＣチップを搭載した携帯電話機などにも適用することができる。

【００９９】

また、本発明の通信システムは、本実施の形態である非接触通信システム１に限らず、相互認証処理を行うあらゆる通信システムに適用することができる。

【０１００】

ところで、上述した一連の処理は、ハードウェアにより実行することもできるし、ソフトウェアにより実行することもできる。一連の処理をソフトウェアにより実行する場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、プログラム記録媒体からインストールされる。

【０１０１】

なお、コンピュータが実行するプログラムは、本明細書で説明する順序に沿って時系列に処理が行われるプログラムであってもよいし、並列に、あるいは呼び出しが行われたとき等の必要なタイミングで処理が行われるプログラムであってもよい。

【０１０２】

また、プログラムは、１台のコンピュータにより処理されるものであってもよいし、複数のコンピュータによって分散処理されるものであってもよい。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであってもよい。

【０１０３】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０１０４】

なお、本発明の実施の形態は、上述した実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲において種々の変更が可能である。

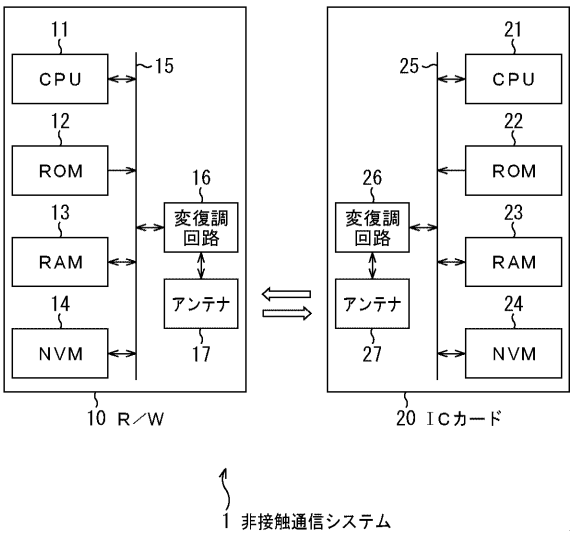
【符号の説明】

【０１０５】

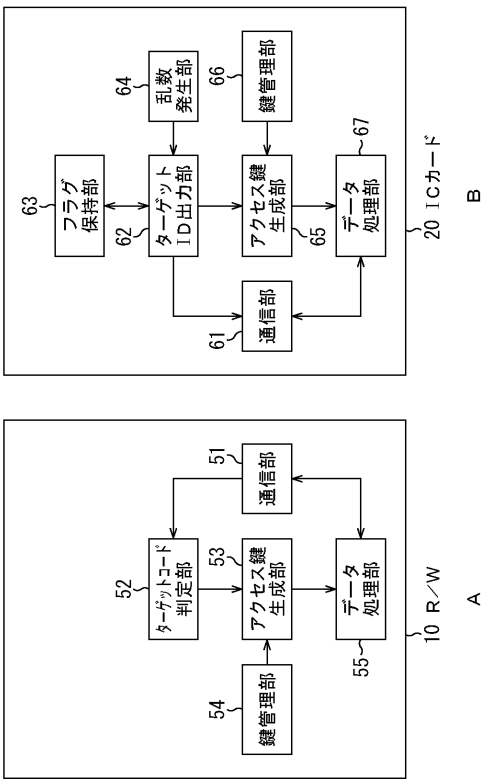
１　非接触通信システム，　１０　Ｒ／Ｗ，　１１　CPU，　２０　ＩＣカード，　２１　CPU，　２４　NVM，　５１　通信部，　５２　ターゲットコード判定部，　５３　アクセス鍵生成部，　５４　鍵管理部，　５５　データ処理部，　６１　通信部，　６２

ターゲットＩＤ出力部，　６３　フラグ保持部，　６４　乱数発生部，　６５　アクセス鍵生成部，　６６　鍵管理部，　６７　データ処理部

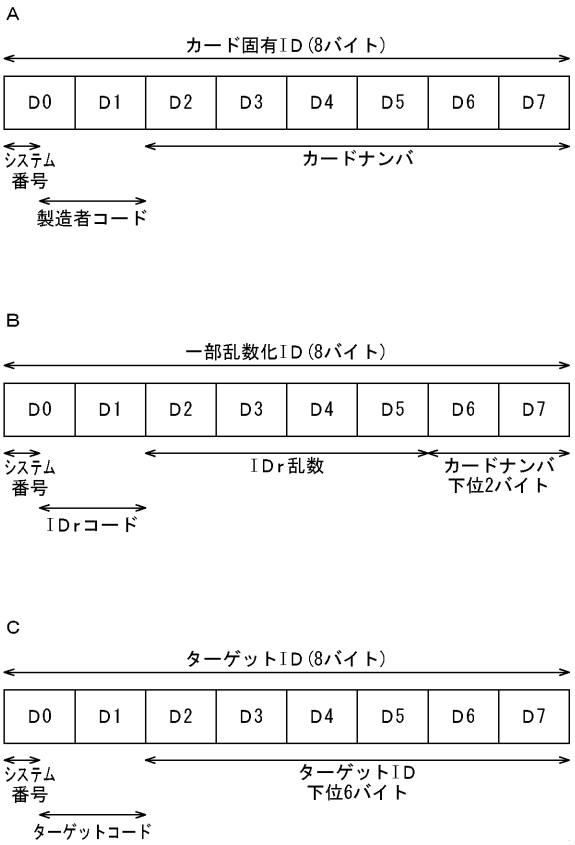
【図１】
図1



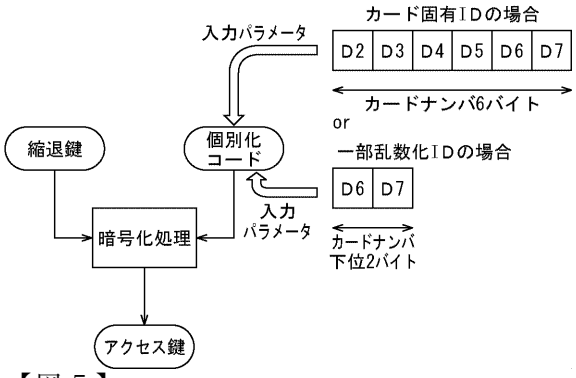
【図２】
図2



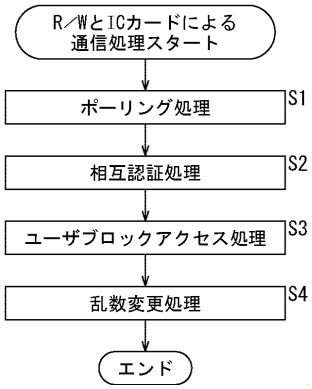
【図３】
図3



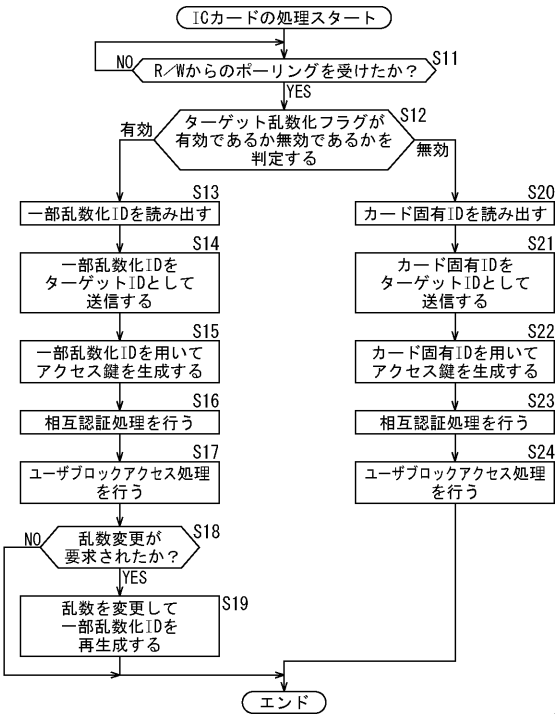
【図４】
図4



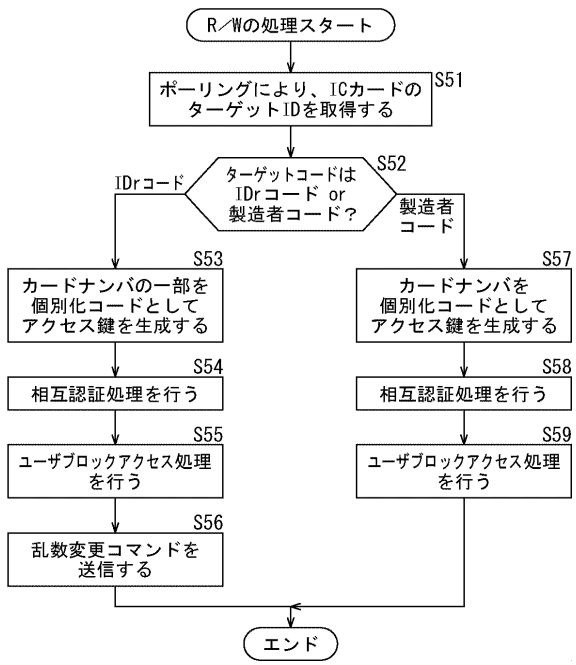
【図５】
図5



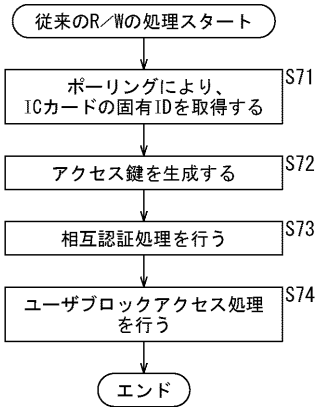
【図６】
図6



【図７】
図7



【図８】
図8


従来のR／Wの処理スタート
ポーリングにより、
ICカードの固有IDを取得する
S71
アクセス鍵を生成する
S72
相互認証処理を行う
S73
ユーザブロックアクセス処理
を行う
S74
エンド

フロントページの続き

(51)Int.Cl.		FI		
G06K 19/10	*(2006.01)*	G06K	19/00	R

(72)発明者 中津川 泰正
東京都港区港南１丁目７番１号 ソニー株式会社内
(72)発明者 東川 寿充
東京都港区港南１丁目７番１号 ソニー株式会社内

審査官 金沢 史明

(56)参考文献 特開２００６－０８０６４２（ＪＰ，Ａ）
特開２００８－０９９３３５（ＪＰ，Ａ）
特開平０２－２７３８８６（ＪＰ，Ａ）
特表２００３－５１９４２０（ＪＰ，Ａ）
特開２００６－３５２２１５（ＪＰ，Ａ）
特開２００２－２６１７５５（ＪＰ，Ａ）
米国特許出願公開第２００９／０１５９６６６（ＵＳ，Ａ１）
欧州特許出願公開第１７６０６７１（ＥＰ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｈ０４Ｌ ９／０８
Ｇ０９Ｃ １／００
Ｇ０６Ｆ ２１／４４
Ｇ０６Ｆ ２１／６２