

明 細 書

発明の名称：

被認証装置、認証装置、認証要求送信方法、認証方法、及びプログラム
技術分野

[0001] 本発明は、被認証装置、認証装置、認証要求送信方法、認証方法、及びプログラムに関する。

背景技術

[0002] 従来、スマートフォンなどの個人携帯端末を用いて認証を行い、クレジットカードなどを用いた支払を行うことができるシステムが知られている。そのようなシステムにより、ユーザは、自分の個人携帯端末を用いることによって、商品やサービス等の支払を行うことができる（例えば、特許文献1参照）。

先行技術文献

特許文献

[0003] 特許文献1：特表2017-501620号公報

発明の概要

発明が解決しようとする課題

[0004] そのような認証では、ユーザの利便性の向上や、処理負荷の低減のため、より簡単な処理によって認証を行うことができるようにすることが求められている。その一方で、なりすまし等を防止し、セキュアな認証を実現できることも求められている。

[0005] 本発明は、上記課題を解決するためになされたものであり、簡単な処理により、セキュアな認証を実現することができる被認証装置、認証要求送信方法、認証方法、及び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

[0006] 上記目的を達成するため、本発明による被認証装置は、ユニーク情報を取

得する取得部と、ユニーク情報を暗号鍵によって暗号化して暗号情報を生成する暗号化部と、暗号情報を含む認証要求を、認証期間内に繰り返して認証装置に送信する送信部と、を備え、複数のユニーク情報が暗号化された暗号情報をそれぞれ含む複数の認証要求が、認証期間内に送信される、ものである。

[0007] このような構成により、複数のユニーク情報が暗号化された暗号情報をそれぞれ含む複数の認証要求を認証装置に送信することができる。そして、その複数の認証要求を用いて、認証装置において、簡単な処理により、セキュアな認証を実現することができるようになる。

[0008] また、本発明による被認証装置では、ユニーク情報は、乱数値、カウンタ値、時刻のいずれかを含んでもよい。

[0009] このような構成により、ユニーク情報を簡単に取得することができる。

[0010] また、本発明による被認証装置では、暗号鍵は、共通鍵暗号の鍵であってもよい。

[0011] このような構成により、被認証装置ごとに共通鍵暗号の異なる鍵を用いている場合には、攻撃者は、正当な被認証装置から送信された認証要求を受信し、その受信した認証要求を認証装置に送信することによる攻撃しか行うことができないことになる。したがって、攻撃の行われたことをより検出しやすくなる。

[0012] また、本発明による認証装置は、被認証装置から送信された、暗号鍵によって暗号化された暗号情報を含む認証要求を、認証期間内に繰り返して受信する受信部と、暗号情報を復号して復号情報を取得する復号部と、復号できた暗号情報を含む、認証期間内に受信された複数の認証要求を用いて、被認証装置が正当かどうかを判断する認証部と、認証部による判断結果を出力する出力部と、を備え、正当な被認証装置は、複数のユニーク情報を暗号化した暗号情報をそれぞれ含む複数の認証要求を認証期間内に送信するものである。

[0013] このような構成により、被認証装置から送信された複数の認証要求を用い

て、被認証装置が正当かどうかを判断することができる。したがって、簡単な処理により、セキュアな認証を実現することができるようになる。より具体的には、被認証装置が正当かどうかの判断に複数の認証要求を用いるため、認証の処理自体を簡単な処理にしたとしても、なりすましを防止したセキュアな認証を実現することができる。

[0014] また、本発明による認証装置では、認証部は、複数の復号情報に所定数以上の重複が存在する場合に、被認証装置が正当でないと判断してもよい。

[0015] このような構成により、例えば、正当な被認証装置から送信された一つの認証要求を、攻撃者が繰り返して送信した場合に、そのことを検出することができるようになる。

[0016] また、本発明による認証装置では、認証部は、認証要求が所定の期間にあらかじめ決められた回数を超えて受信された場合に、被認証装置が正当でないと判断してもよい。

[0017] このような構成により、例えば、正当な被認証装置以外に、攻撃者の装置からも認証要求が送信された場合に、そのことを検出することができるようになる。

[0018] また、本発明による認証装置では、認証部は、認証期間における認証要求の受信間隔に、確率が閾値より低い受信間隔が含まれる場合に、被認証装置が正当でないと判断してもよい。

[0019] このような構成により、例えば、正当な被認証装置以外に、攻撃者の装置からも認証要求が送信された場合に、そのことを検出することができるようになる。

[0020] また、本発明による認証装置では、認証部は、認証期間に受信された複数の認証要求からそれぞれ取得された複数の復号情報が、ユニーク情報と整合しない場合に、被認証装置が正当でないと判断してもよい。

[0021] このような構成により、例えば、正当な被認証装置から送信された一つの認証要求を、攻撃者が取得して認証装置に送信した場合に、そのことを検出することができるようになる。

- [0022] また、本発明による認証装置では、受信部は、間欠的に認証要求を受信してもよい。
- [0023] このような構成により、認証要求の受信に関する負荷を軽減することができ、認証装置の消費電力を低減することができるようになる。
- [0024] また、本発明による認証装置では、暗号鍵は、共通鍵暗号の鍵であってもよい。
- [0025] このような構成により、公開鍵暗号の鍵を用いた場合と比較して、復号の処理負荷が軽くなる。
- [0026] また、本発明による認証要求送信方法は、ユニーク情報を取得するステップと、ユニーク情報を暗号鍵によって暗号化して暗号情報を生成するステップと、暗号情報を含む認証要求を、認証期間内に繰り返して認証装置に送信するステップと、を備え、複数のユニーク情報が暗号化された暗号情報をそれぞれ含む複数の認証要求が、認証期間内に送信される、ものである。
- [0027] また、本発明による認証方法は、被認証装置から送信された、暗号鍵によって暗号化された暗号情報を含む認証要求を、認証期間内に繰り返して受信するステップと、暗号情報を復号して復号情報を取得するステップと、復号できた暗号情報を含む、認証期間内に受信された複数の認証要求を用いて、被認証装置が正当かどうかを判断するステップと、被認証装置が正当かどうかを判断するステップにおける判断結果を出力するステップと、を備え、正当な被認証装置は、複数のユニーク情報を暗号化した暗号情報をそれぞれ含む複数の認証要求を認証期間内に送信する、ものである。

発明の効果

- [0028] 本発明による被認証装置、認証装置、認証要求送信方法、認証方法、及びプログラムによれば、簡単な処理により、セキュアな認証を実現することができる。

図面の簡単な説明

- [0029] [図1]本発明の実施の形態による被認証装置及び認証装置の構成を示すブロック図

[図2]同実施の形態による被認証装置の動作を示すフローチャート

[図3]同実施の形態による認証装置の動作を示すフローチャート

[図4]同実施の形態における認証要求の送受信について説明するための図

[図5]同実施の形態における認証要求の送受信について説明するための図

[図6]同実施の形態における認証要求の送受信について説明するための図

[図7]同実施の形態における認証要求の送受信について説明するための図

[図8]同実施の形態における認証要求の送受信について説明するための図

[図9]同実施の形態における認証要求の送受信について説明するための図

[図10]同実施の形態におけるコンピュータシステムの構成の一例を示す図

発明を実施するための形態

[0030] 以下、本発明による被認証装置、認証装置、認証要求送信方法、及び認証方法について、実施の形態を用いて説明する。なお、以下の実施の形態において、同じ符号を付した構成要素及びステップは同一または相当するものであり、再度の説明を省略することがある。本実施の形態による被認証装置は、複数のユニーク情報を暗号化した暗号情報を含む複数の認証要求を認証装置に送信する。また、本実施の形態による認証装置は、被認証装置から送信された複数の認証要求を用いて、被認証装置の認証を行う。

[0031] 図1は、本実施の形態による被認証装置1及び認証装置2の構成を示すブロック図である。本実施の形態による被認証装置1は、取得部11と、記憶部12と、暗号化部13と、送信部14とを備える。本実施の形態による認証装置2は、受信部21と、記憶部22と、復号部23と、認証部24と、出力部25とを備える。被認証装置1は、例えば、スマートフォンや、タブレット端末、PDA(Personal Digital Assistant)、ノートパソコン、トランシーバ等の通信機能を備えた携帯情報端末であってもよく、その他の機器であってもよい。認証装置2は、例えば、自動改札機、イベント等の会場へ入場するためのゲート、自動販売機、ホテルや貸し会議室のドアを施錠・解錠する制御装置、キャッシュレジスタ等であってもよく、スマートフォン等の通信機能を備えた携帯情報端末であってもよい。本実施の形態では、被

認証装置 1 及び認証装置 2 が通信機能を有する携帯情報端末である場合について主に説明する。なお、図 1 では、1 個の被認証装置 1 と、1 個の認証装置 2 とが通信を行う場合について示しているが、そうでなくてもよい。複数の被認証装置 1 と、1 個の認証装置 2 との間で通信が行われてもよい。その通信は通常、無線通信である。

[0032] まず、本実施の形態による被認証装置 1 について説明する。

取得部 11 は、ユニーク情報を取得する。各ユニーク情報は、例えば、異なる情報であってもよい。この場合には、取得部 11 が複数のユニーク情報を取得すると、その複数のユニーク情報は、それぞれ異なるものとなる。ユニーク情報は、後述するように、暗号化されて認証要求に含められ、送信される。したがって、各ユニーク情報が異なる情報である場合には、ユニーク情報は、認証要求に固有の情報であるとも言える。また、通常、ユニークな情報と、ユニークではない情報とから構成される情報（例えば、上位側ビットがユニークな情報であり、下位側ビットがユニークではない情報など）は、結果として、ユニーク情報となる。したがって、ユニーク情報は、そのように、ユニークな情報とユニークではない情報とから構成されてもよい。ユニーク情報と、そのユニーク情報に含まれるユニークな情報とを区別するため、以下、ユニーク情報に含まれるユニークな情報を、「ユニーク部分」と呼ぶこともある。また、ユニーク情報に含まれるユニークではない情報を、「非ユニーク部分」と呼ぶこともある。なお、非ユニーク部分は、必ずユニークな情報であるとは言えない情報であり、後述する位置情報のように、認証要求ごとに変化する情報であってもよい。

[0033] ユニーク情報は、例えば、乱数値を含んでもよく、カウント値を含んでもよく、時刻を含んでもよく、ワンタイムパスワードを含んでもよく、その他のユニークな情報を含んでもよい。乱数値は、例えば、乱数表や、乱数を発生させる関数などを用いて生成されてもよい。カウント値は、例えば、あらかじめ決められた間隔で数値をインクリメントまたはデクリメントした値であってもよい。なお、認証要求ごとに異なるユニーク情報が用いられる場合

には、その乱数値やカウント値は、重複がないことが好適である。時刻は、例えば、図示しない時計部から取得された時分秒や、分秒などであってもよい。また、認証要求ごとに異なるユニーク情報が用いられる場合には、その時刻の精度は、後述する認証要求の送信間隔よりも短い時間間隔の精度であることが好適である。そのようにすることで、例えば、ユニーク情報を認証要求に固有の情報とすることができる。例えば、認証要求の送信間隔が10ミリ秒程度である場合には、時刻の精度は、1ミリ秒であってもよい。なお、複数の認証要求について重複したユニーク情報が用いられてもよい場合には、乱数値やカウントに重複があってもよく、時刻の精度は、送信間隔よりも長い時間間隔の精度であってもよい。この場合であっても、後述するように、認証期間内には、異なるユニーク情報に対応する複数の認証要求が送信される必要があるため、そのような複数の認証要求を送信することができるユニーク情報の取得が行われることが好適である。

[0034] 取得部11は、ユニーク情報を生成してもよく、他の構成要素や装置から受け取ってもよい。ユニーク情報が、ユニーク部分と非ユニーク部分とから構成される場合には、取得部11は、乱数値やカウント値、時刻、ワンタイムパスワードなどのユニーク部分を取得し、そのユニーク部分と、自装置である被認証装置1のIDや送信先の認証装置2のID、自装置である被認証装置1の位置情報などの非ユニーク部分とを用いて、ユニーク情報を生成してもよい。自装置のIDは、例えば、記憶部12から読み出されて用いられてもよい。また、送信先の認証装置2のIDは、例えば、後述する送信指示に含まれていてもよく、記憶部12から読み出されて用いられてもよい。自装置の位置情報は、後述するように、位置取得部によって取得されてもよい。また、取得部11は、例えば、認証装置2からユニーク情報を受信してもよい。その場合には、そのユニーク情報を暗号化した暗号情報を含む認証要求が被認証装置1から認証装置2に送信されることによって、チャレンジ・レスポンス認証が行われることになる。この場合には、認証装置2において、上記のようなユニーク情報が生成されてもよい。なお、取得部11は、例

えば、認証装置 2 からユニーク部分を受信し、そのユニーク部分を用いて、ユニーク情報を生成してもよい。この場合にも、ユニーク情報に含まれるユニーク部分を用いて、チャレンジ・レスポンス認証を行うことができる。

[0035] 記憶部 1 2 では、例えば、被認証装置 1 の ID が記憶されている。この ID は、被認証装置 1 の識別子であり、被認証装置 1 に固有な情報である。また、記憶部 1 2 では、例えば、後述する共通鍵暗号の鍵や、認証装置 2 の識別子である ID 等が記憶されていてもよい。また、ユニーク情報に乱数値やカウント値が含まれる場合には、乱数値を取得するための乱数表や関数、カウント値を生成するための最新のカウンタ値等が記憶部 1 2 で記憶されていてもよい。

[0036] 記憶部 1 2 に情報が記憶される過程は問わない。例えば、記録媒体を介して情報が記憶部 1 2 で記憶されるようになってよく、通信回線等を介して送信された情報が記憶部 1 2 で記憶されるようになってよく、または、入力デバイスを通じて入力された情報が記憶部 1 2 で記憶されるようになってよく。記憶部 1 2 は、不揮発性の記録媒体によって実現されることが好適であるが、揮発性の記録媒体によって実現されてもよい。記録媒体は、例えば、半導体メモリや磁気ディスク、光ディスクなどであってもよい。

[0037] 暗号化部 1 3 は、ユニーク情報を暗号鍵によって暗号化して暗号情報を生成する。暗号鍵は、例えば、共通鍵暗号の鍵であってもよく、または、認証要求の送信先の認証装置 2 に対応する公開鍵暗号の公開鍵であってもよい。暗号鍵が共通鍵暗号の鍵である場合には、共通鍵暗号の鍵は、被認証装置 1 に固有の鍵であってもよい。この場合には、被認証装置 1 ごとに共通鍵暗号の鍵は異なることになる。また、後述するように、この共通鍵暗号の鍵を、認証装置 2 も保持している。また、暗号鍵が公開鍵暗号の公開鍵である場合には、送信先の認証装置 2 の公開鍵暗号の公開鍵は、例えば、後述する送信指示に含まれていてもよい。

[0038] 送信部 1 4 は、暗号化部 1 3 で生成された暗号情報を含む認証要求を、認証期間内に繰り返して認証装置 2 に送信する。なお、複数のユニーク情報が

暗号化された暗号情報をそれぞれ含む複数の認証要求が、認証期間内に送信されるものとする。上記のように、例えば、各ユニーク情報が異なる情報である場合には、正当な被認証装置 1 から送信される認証要求ごとに、異なるユニーク情報が暗号化された暗号情報が含まれることになる。一方、例えば、ユニーク情報に重複が存在する場合には、正当な被認証装置 1 から送信される少なくとも 2 個の認証要求に、同じユニーク情報が暗号化された暗号情報が含まれることもあり得る。この場合であっても、認証期間内には、異なるユニーク情報に対応する複数の認証要求が送信されるものとする。なお、認証期間に送信される複数の認証要求が、同じユニーク情報が暗号化された暗号情報をそれぞれ含む場合に、例えば、同じユニーク情報が暗号化された暗号情報を含む認証要求の個数は決まってもよい。例えば、あらかじめ決められた個数の認証要求に、同じユニーク情報が暗号化された暗号情報が含まれ、その決められた個数の認証要求ごとに、暗号情報に対応するユニーク情報が異なるものとなってもよい。また、認証要求には、暗号情報以外の情報が含まれていてもよい。例えば、認証要求の送信元の被認証装置 1 の ID が、その認証要求に含まれていてもよい。

[0039] 認証期間は、通常、あらかじめ決められた時間的な長さである。1 個目の認証要求の送信から認証期間が開始されてもよい。そのため、送信部 14 は、例えば、1 個目の認証要求の送信からタイマによる計時を開始し、あらかじめ決められた認証期間が経過すると、認証要求の送信を終了してもよい。認証期間は特に限定されるものではないが、例えば、200 ミリ秒から 10 秒程度の範囲内の時間であってもよい。なお、後述するように、認証期間が終了するまでは認証装置 2 における認証の処理が開始されないため、認証期間は短いほうが好適である。そのため、認証時間は、3 秒以下であることが好適であり、1 秒以下であることがさらに好適である。なお、送信部 14 は、例えば、被認証装置 1 が所定の送信指示を受信した際に、認証要求の送信を開始してもよい。その送信指示は、例えば、認証装置 2 の付近に配置された発信機から送信されるビーコンであってもよい。

[0040] 送信部14は、通常、所定の時間間隔を空けて繰り返して認証要求を送信する。その時間間隔は、例えば、一定であってもよく、または、不定であってもよい。前者の場合には、その時間間隔は、設定されたものであってもよく、そうでなくてもよい。また、その時間間隔が不定の場合であっても、平均の時間間隔は設定できてよい。例えば、認証要求がBluetooth（登録商標）の低消費電力（LE：Low Energy）によって通信される場合には、時間間隔は不定であるが、平均の時間間隔は決まっていることになる。いずれの場合であっても、その時間間隔は、送信部14が認証要求を送信する通信規格で定められた最低の通信間隔以上の間隔となる。また、例えば、認証装置2が間欠的な受信を行う場合であっても、複数の認証要求のうち、少なくともいずれかの認証要求が認証装置2で受信されるように送信されることが好適である。そのため、例えば、認証要求の送信周期は、認証装置2の受信周期と異なってもよく、ランダムな送信間隔で認証要求の送信が行われてもよい。また、送信部14が認証期間に送信する認証要求の個数は、決まってもよく、または、そうでなくてもよい。後者の場合であっても、認証期間が決まっており、認証要求が所定の時間間隔を空けて送信されることによって、通常、認証期間内に送信される認証要求の個数、または個数の範囲は決まることになる。

[0041] 送信部14が認証要求を送信する無線の通信規格は問わない。認証要求は、例えば、Bluetoothの低消費電力（以下、「BLE」と呼ぶこともある。）によって通信されてもよく、BluetoothのBR（Basic Rate）／EDR（Enhanced Data Rate）によって通信されてもよく、無線LAN（IEEE802.11）によって通信されてもよく、ZigBee（登録商標）などのIEEE802.15.4によって通信されてもよく、その他の無線の通信規格によって通信されてもよい。認証要求は、例えば、BLEや、BluetoothのBR／EDR、無線LANなどの近距離無線通信によって送受信されることが好適である。本実施の形態では、認証要求BLEによって通信される場合について主に説明する。

[0042] 送信部 14 は、例えば、認証要求をブロードキャストで送信してもよく、ユニキャストで通信してもよい。通信相手を特定しないで認証要求を送信できることから、ブロードキャストで認証要求を送信することが好適である。本実施の形態では、送信部 14 が認証要求をブロードキャストで送信する場合について主に説明する。

[0043] なお、送信部 14 は、送信を行うための無線の送信デバイス（例えば、アンテナなど）を含んでもよく、または含まなくてもよい。また、送信部 14 は、ハードウェアによって実現されてもよく、または送信デバイスを駆動するドライバ等のソフトウェアによって実現されてもよい。

[0044] 次に、本実施の形態による認証装置 2 について説明する。

受信部 21 は、被認証装置 1 から送信された、暗号鍵によって暗号化された暗号情報を含む認証要求を、認証期間内に繰り返して受信する。なお、認証要求の送信元は、通常、上記説明の被認証装置 1 である。一方、後述するように、攻撃者の装置が、被認証装置 1 から送信された認証要求を受信し、その受信した認証要求を再度、送信することや、ユニーク情報を独自に取得して暗号情報を生成し、その暗号情報を含む認証要求を送信することもあり得る。その場合に、受信部 21 は、認証要求が、正当な被認証装置 1 から送信されたのか、攻撃者の装置から送信されたのかを、その認証要求の受信時に判断することはできない。したがって、認証要求を送信した装置を、被認証装置 1 と呼ぶことにする。そして、後述するように、複数の認証要求が受信された後に、認証部 24 は、それらの認証要求を用いて、送信元が本来の被認証装置 1、すなわち正当な被認証装置 1 であるのか、攻撃者の装置、すなわち正当でない被認証装置 1 であるのかを判断することになる。

[0045] 受信部 21 は、間欠的に認証要求を受信してもよい。間欠的な受信とは、情報を受信する期間と、情報を受信しない期間とが交互に繰り返されることであってもよい。例えば、認証要求が BLE 通信によって、ブロードキャストで送信される場合には、そのような間欠的な受信が行われることになる。間欠的な受信を行うことによって、消費電力を低減することができる。なお

、間欠的な受信が行われる場合に、例えば、情報を受信する期間の長さ、情報を受信しない期間の長さとは一定であってもよく、または、不定であってもよい。本実施の形態では、受信部 2 1 が、間欠的な受信を行う場合について主に説明する。

[0046] なお、受信部 2 1 は、受信を行うための無線の受信デバイス（例えば、アンテナなど）を含んでもよく、または含まなくてもよい。また、受信部 2 1 は、ハードウェアによって実現されてもよく、または受信デバイスを駆動するドライバ等のソフトウェアによって実現されてもよい。

[0047] 記憶部 2 2 では、復号鍵が記憶される。例えば、暗号鍵が共通鍵暗号の鍵である場合には、復号鍵は、その共通鍵暗号の鍵である。この場合には、被認証装置 1 ごとに復号鍵（共通鍵暗号の鍵）が記憶部 2 2 で記憶されていてもよい。記憶部 2 2 では、例えば、被認証装置 1 の ID と、その ID で識別される被認証装置 1 の共通鍵暗号の鍵とを含む鍵対応情報が複数、記憶されていてもよい。また、例えば、暗号鍵が公開鍵暗号の公開鍵である場合には、復号鍵は、その公開鍵暗号の公開鍵とペアになる秘密鍵である。また、ユニーク情報に乱数値やカウント値が含まれる場合には、乱数値を取得するための乱数表や関数、カウント値を生成するための最新のカウント値等が記憶部 2 2 で記憶されていてもよい。また、記憶部 2 2 では、後述する処理で用いられる、受信回数の閾値や、受信の確率が閾値より低い受信間隔を示す情報などが記憶されていてもよい。

[0048] 記憶部 2 2 に情報が記憶される過程は問わない。例えば、記録媒体を介して情報が記憶部 2 2 で記憶されるようになっていてもよく、通信回線等を介して送信された情報が記憶部 2 2 で記憶されるようになっていてもよく、または、入力デバイスを介して入力された情報が記憶部 2 2 で記憶されるようになっていてもよい。記憶部 2 2 は、不揮発性の記録媒体によって実現されることが好適であるが、揮発性の記録媒体によって実現されてもよい。記録媒体は、例えば、半導体メモリや磁気ディスク、光ディスクなどであってもよい。

[0049] 復号部 2 3 は、復号鍵を用いて暗号情報を復号して復号情報を取得する。

例えば、復号鍵が共通鍵暗号の鍵であり、認証要求に、その認証要求の送信元の被認証装置 1 の ID が含まれる場合には、復号部 23 は、その ID に対応付けられている共通鍵暗号の鍵を記憶部 22 から読み出し、その読み出した共通鍵暗号の鍵を用いて暗号情報を復号してもよい。また、例えば、復号鍵が秘密鍵である場合には、復号部 23 は、秘密鍵を記憶部 22 から読み出し、その読み出した秘密鍵を用いて暗号情報を復号してもよい。正当な被認証装置 1 から送信された認証要求に含まれる暗号情報が復号された復号情報はユニーク情報となる。したがって、暗号情報を復号できなかった場合や、復号した復号情報が、あらかじめ決められたユニーク情報の形式に合わなかった場合などには、その暗号情報を含む認証要求を送信した装置が、正当な被認証装置 1 ではないと判断することができる。

[0050] 認証部 24 は、復号鍵によって復号できた暗号情報を含む、認証期間内に受信された複数の認証要求を用いて、被認証装置 1 が正当かどうかを判断する。復号鍵が共通鍵暗号の鍵である場合には、認証期間に受信された複数の認証要求のうち、一の共通鍵暗号の鍵を用いて復号できた暗号情報を含んでいる複数の認証要求を用いて、被認証装置 1 の認証が行われることになる。上記のように、共通鍵暗号の鍵が被認証装置 1 ごとに異なる場合には、一の共通鍵暗号の鍵を用いて復号できた暗号情報を含む複数の認証要求は、一の被認証装置 1 から送信されたと考えることができ、その複数の認証要求を用いて認証を行うことによって、その被認証装置 1 についての認証を行うことができることになる。一方、復号鍵が秘密鍵である場合には、認証期間に受信された複数の認証要求のうち、認証装置 2 の秘密鍵を用いて復号できた暗号情報を含んでいる複数の認証要求を用いて、被認証装置 1 の認証が行われることになる。ここで、復号鍵が秘密鍵である場合には、秘密鍵を用いて復号できた暗号情報を含んでいる複数の認証要求に、複数の被認証装置 1 から送信された認証要求が含まれることがあり得る。そのため、例えば、認証要求に、その認証要求の送信元の被認証装置 1 の ID が含まれる場合には、認証部 24 は、認証期間内に受信された、同じ ID を含む複数の認証要求を用

いて、被認証装置 1 が正当かどうかを判断してもよい。なお、複数の認証要求を用いて、被認証装置 1 が正当かどうかを判断するとは、複数の認証要求そのものを用いることであってもよく、複数の認証要求に関連する情報を用いることであってもよい。複数の認証要求に関連する情報は、例えば、複数の認証要求からそれぞれ取得された複数の復号情報であってもよく、複数の認証要求の受信間隔であってもよく、複数の認証要求の個数であってもよく、複数の認証要求に関連するその他の情報であってもよい。また、認証要求に、その認証要求の送信元の被認証装置 1 の ID が含まれる場合には、通常、一の共通鍵暗号の鍵によって復号できる暗号情報を有している認証要求には、同じ ID が含まれることになる。したがって、暗号鍵が共通鍵暗号の鍵である場合には、認証部 24 は、認証期間内に受信された、同じ ID を含む複数の認証要求を用いて、被認証装置 1 が正当かどうかを判断してもよい。認証部 24 は、ある被認証装置 1 から 1 個目の認証要求が受信されてから、あらかじめ決められた認証期間内に、その被認証装置 1 から受信された複数の認証要求を用いて、被認証装置 1 の認証を行ってもよい。

[0051] なお、認証部 24 は、例えば、ある認証期間に受信された複数の認証要求のすべてが、正当ではない被認証装置 1 から送信された場合に、その被認証装置 1 が正当ではないと判断する。また、認証部 24 は、例えば、ある認証期間に受信された複数の認証要求に、正当ではない装置から送信された認証要求が含まれる場合にも、その複数の認証要求を送信した被認証装置 1 が正当ではないと判断する。すなわち、複数の認証要求が、正当な被認証装置 1 と、正当ではない被認証装置 1 とから送信された場合にも、その複数の認証要求の送信元の被認証装置 1 は、正当ではないと判断されることになる。この場合には、認証要求の送信元に、少なくとも攻撃者の装置が含まれることになり、仮に正当な被認証装置 1 が送信元に含まれるとしても、両者を区別することはできないため、両者共に正当でないと判断することになる。

[0052] [復号情報の重複に基づいた判断]

認証部 24 は、例えば、複数の復号情報に所定数以上の重複が存在する場

合に、被認証装置 1 が正当でないと判断してもよい。上記のように、正当な被認証装置 1 が、複数のユニーク情報を暗号化した暗号情報をそれぞれ含む複数の認証要求を認証期間内に送信する場合には、通常、認証期間内に受信された複数の認証要求からそれぞれ取得された複数の復号情報（すなわち、ユニーク情報）の重複の程度は、決まっていることになる。例えば、認証要求ごとに異なるユニーク情報が暗号化された暗号情報が含まれる場合には、ある正当な被認証装置 1 から認証期間内に受信された複数の認証要求からそれぞれ取得された複数の復号情報は、それぞれ異なる情報となるはずであり、複数の復号情報に重複は存在しないことになる。したがって、そうっていない場合、すなわち複数の復号情報に重複が存在する場合に、認証部 24 は、その復号情報の取得元の暗号情報を含む認証要求を送信した被認証装置 1 が正当でないと判断することができる。また、例えば、正当な被認証装置 1 から受信された 1 個目から N 個目の認証要求には、同じ第 1 のユニーク情報を暗号化した暗号情報が含まれ、 $N + 1$ 個目から $2N$ 個目の認証要求には、同じ第 2 のユニーク情報を暗号化した暗号情報が含まれる、というように、 N 個の認証要求ごとに、異なるユニーク情報を暗号化した暗号情報が含まれる場合には、認証期間内に受信された複数の認証要求からそれぞれ取得された複数の復号情報には、最大で N 個の重複が存在することになる。したがって、この場合には、認証部 24 は、複数の復号情報に $N + 1$ 個以上の重複が存在するとき、すなわち $N + 1$ 個以上の同じ復号情報が存在するとき、被認証装置 1 が正当でないと判断してもよい。なお、 N は 1 以上の整数である。また、この例において、認証装置 2 の受信部 21 が間欠的な受信を行っている場合には、 N が 2 以上の整数であっても、正当な被認証装置 1 から認証装置 2 が受信した複数の認証要求から取得された複数の復号情報には、同じ復号情報が M 個しか存在しないことがあり得る。なお、 M は、 N より小さい正の整数である。したがって、このような場合には、認証部 24 は、複数の復号情報に $M + 1$ 個以上の重複が存在するとき、すなわち $M + 1$ 個以上の同じ復号情報が存在するときに、被認証装置 1 が正当でないと判断してもよ

い。なお、複数の復号情報にあらかじめ決められた個数以上の重複が存在する場合には、例えば、正当でない被認証装置 1 が、正当な被認証装置 1 から送信された認証要求をコピーして送信したと考えることができる。そのあらかじめ決められた個数は、例えば、記憶部 22 で記憶されていてもよい。

[0053] 通常、異なるユニーク情報が暗号化されると、異なる暗号情報となる。したがって、認証部 24 は、複数の復号情報に所定数以上の重複が存在するかどうかを、複数の暗号情報に所定数以上の重複が存在するかどうかによって判断してもよい。また、例えば、認証要求に含まれる暗号情報以外の情報が認証要求ごとに同一である場合には、認証部 24 は、複数の復号情報に所定数以上の重複が存在するかどうかを、複数の認証要求に所定数以上の重複が存在するかどうかによって判断してもよい。

[0054] [認証要求の受信回数に基づいた判断]

認証部 24 は、例えば、認証要求が所定の期間にあらかじめ決められた回数を超えて受信された場合に、被認証装置 1 が正当でないと判断してもよい。所定の期間は、例えば、認証期間であってもよく、または、認証期間よりも短い期間（例えば、単位期間など）であってもよい。あらかじめ決められた回数は、例えば、記憶部 22 で記憶されていてもよい。上記のように、被認証装置 1 が、所定の時間間隔を空けて繰り返して認証要求を送信する場合には、所定の期間に受信される認証要求の最大個数は決まることになる。したがって、その最大個数を超える個数の認証要求が所定の期間に受信された場合には、少なくとも、正当でない被認証装置 1 から認証要求が送信されたことになるため、認証部 24 は、認証要求を送信した被認証装置 1 が正当でないと判断することができる。

[0055] [認証要求の受信間隔に基づいた判断]

認証部 24 は、例えば、認証期間における認証要求の受信間隔に、確率が閾値より低い受信間隔が含まれる場合に、被認証装置 1 が正当でないと判断してもよい。認証要求の受信間隔とは、ある認証要求が受信されてから、次の認証要求が受信されるまでの時間的な長さである。なお、この認証要求の

受信間隔は、同じ I D の被認証装置 1 から送信された認証要求に関する受信間隔である。ある通信規格によって被認証装置 1 が認証要求を繰り返して送信する場合には、受信部 2 1 が間欠的な受信を行っているかどうかに関わらず、認証要求の受信間隔は、統計的に特定の間隔となることが多く、ある受信間隔については、確率が著しく低くなる。したがって、そのような著しく低い受信間隔で認証要求が受信された場合には、正当ではない被認証装置 1 からも認証要求が送信されたと考えることができたため、認証部 2 4 は、認証要求を送信した被認証装置 1 が正当ではないと判断することができる。なお、受信間隔の確率は、例えば、認証要求を送信する通信規格によって、実際に 1 つの装置からの情報の送信と受信とを繰り返すことによって取得してもよい。そのようにすることで、例えば、横軸が受信間隔であり、縦軸が確率であるヒストグラムを取得することができる。そのヒストグラムによって、例えば、 $T_1 \sim T_2$ ミリ秒の受信間隔で情報を受信する確率は P_1 であり、 $T_2 \sim T_3$ ミリ秒の受信間隔で情報を受信する確率は P_2 であるなどを知ることができる。そして、あらかじめ決められた確率（例えば、1 % や、0.1 % など）より低い確率の受信間隔で認証要求が受信された場合には、認証部 2 4 は、その認証要求を送信した被認証装置 1 が正当ではないと判断することができる。

[0056] [復号情報とユニーク情報との整合に基づいた判断]

認証部 2 4 は、例えば、認証期間に受信された複数の認証要求からそれぞれ取得された複数の復号情報が、ユニーク情報と整合しない場合に、被認証装置 1 が正当でないと判断してもよい。認証要求から取得された復号情報とは、認証要求に含まれる暗号情報を復号した復号情報のことである。認証部 2 4 は、被認証装置 1 におけるユニーク情報の生成ルールを用いて、複数の復号情報がユニーク情報と整合するかどうかを判断してもよい。なお、複数の認証要求からそれぞれ取得された複数の復号情報が、ユニーク情報と整合しない場合には、少なくとも一部の認証要求が、正当ではない被認証装置 1 から送信されたと考えることができる。復号情報がユニーク情報と整合しな

いは、例えば、復号情報の値が、ユニーク情報の値と一致しないことであってもよく、複数の復号情報が、ユニーク情報のルールに合わないことであってもよい。

[0057] 例えば、ユニーク情報が乱数値である場合には、認証部24は、その乱数値の取得に用いられる乱数表や関数を用いて判断を行ってもよい。また、ユニーク情報がカウント値である場合には、認証部24は、そのカウント値の生成ルール（例えば、2ずつインクリメントするなど）を用いて判断を行ってもよい。また、ユニーク情報が時刻である場合には、その時刻の形式（例えば、時分秒であるのか、分秒であるのかなど）を用いて判断を行ってもよい。また、ユニーク情報がワンタイムパスワードである場合には、認証部24は、そのワンタイムパスワードの生成ルールや、ワンタイムパスワードの生成器を用いて判断を行ってもよい。

[0058] 認証部24は、複数の復号情報がユニーク情報と整合するかどうかを、例えば、各復号情報について判断し、1つでもユニーク情報と整合しない復号情報が存在する場合に、複数の復号情報がユニーク情報と整合しないと判断してもよい。例えば、ユニーク情報が乱数値やカウント値、ワンタイムパスワードである場合には、認証部24は、復号情報が、認証部24において生成したユニーク情報と一致するときに、復号情報とユニーク情報とが整合すると判断し、両者が一致しないときに、復号情報とユニーク情報とが整合しないと判断してもよい。また、例えば、ユニーク情報が、認証装置2から送信された場合（例えば、ユニーク情報がチャレンジである場合）には、認証部24は、復号情報が、送信されたユニーク情報と一致するときに、復号情報とユニーク情報とが整合すると判断し、両者が一致しないときに、復号情報とユニーク情報とが整合しないと判断してもよい。このようにして、例えば、チャレンジ・レスポンス認証を行うことができる。なお、この場合には、認証部24は、復号情報とユニーク情報とが一致するかどうかを判断するのではなく、暗号情報と、認証装置2から送信されたユニーク情報を、暗号鍵で暗号化した情報とが一致するかどうかを判断してもよい。また、例えば

、ユニーク情報が時刻である場合には、認証部 24 は、復号情報である時刻と、その復号情報に対応する認証要求の受信時刻との差が所定の閾値より小さいときに、復号情報とユニーク情報とが整合すると判断し、両者の差が所定の閾値より大きいときに、復号情報とユニーク情報とが整合しないと判断してもよい。なお、両者の差が所定の閾値と一致する場合には、認証部 24 は、復号情報とユニーク情報とが整合すると判断してもよく、または、そうでなくてもよい。また、認証部 24 は、復号情報の時刻の形式が、ユニーク情報の時刻の形式と異なる場合に、復号情報とユニーク情報と整合しないと判断してもよい。

[0059] また、認証部 24 は、複数の復号情報がユニーク情報と整合するかどうかを、例えば、複数の復号情報の集合について判断してもよい。例えば、ユニーク情報がカウント値である場合には、認証部 24 は、受信された順番に応じた複数の復号情報が、カウント値のルールに合うときに、複数の復号情報がユニーク情報と整合すると判断し、そうでないときに、複数の復号情報がユニーク情報と整合しないと判断してもよい。具体的には、複数の復号情報が、受信された順番に、「2」「4」「6」「8」…であり、ユニーク情報の生成ルールが、2 ずつのインクリメントである場合に、複数の復号情報は、ユニーク情報の生成ルールに合っているため、認証部 24 は、複数の復号情報がユニーク情報と整合すると判断する。一方、例えば、複数の復号情報が、受信された順番に、「2」「4」「6」「6」「8」…であり、ユニーク情報の生成ルールが、2 ずつのインクリメントである場合には、複数の復号情報は、ユニーク情報の生成ルールに合っていないため、認証部 24 は、複数の復号情報がユニーク情報と整合しないと判断する。また、例えば、ユニーク情報が時刻である場合には、認証部 24 は、複数の復号情報について、復号情報である時刻と、その復号情報に対応する認証要求の受信時刻との差である時刻差をそれぞれ取得し、取得した複数の時刻差が一定であるときに、複数の復号情報がユニーク情報と整合すると判断し、取得した複数の時刻差が一定でないときに、複数の復号情報がユニーク情報と整合しないと判

断してもよい。このようにすることで、被認証装置 1 の時計部と、認証装置 2 の時計部とが完全に同期していない場合でも、復号情報が、時刻であるユニーク情報と整合しているかどうかを適切に判断することができる。被認証装置 1 と認証装置 2 とは通常、短距離で無線通信が行われ、その無線通信に起因する遅延が、複数の認証要求について略一定であると考えられるからである。なお、複数の時刻差が一定であるとは、例えば、複数の時刻差の最大値と最小値との差が、あらかじめ決められた閾値より小さいことであってもよく、複数の時刻差のばらつき（例えば、分散や標準偏差など）が、あらかじめ決められた閾値より小さいことであってもよい。また、例えば、ユニーク情報が時刻である場合には、認証部 24 は、受信の順番に応じて復号情報である時刻が増加しないとき、例えば、時点 A に受信された認証要求に対応する復号情報である時刻の方が、時点 A の後である時点 B に受信された認証要求に対応する復号情報である時刻よりも後の時点を示すときに、複数の復号情報がユニーク情報と整合しないと判断してもよい。その場合には、時刻 B に受信された認証要求は、時刻 A に受信された認証要求よりも以前に送信された認証要求を、攻撃者の装置がコピーして送信したものと考えられるからである。

[0060] また、認証部 24 は、複数の復号情報がユニーク情報と整合するかどうかを、例えば、各復号情報について判断すると共に、複数の復号情報の集合についても判断してもよい。この場合には、認証部 24 は、少なくともいずれかの判断において整合しないと判断したときに、複数の復号情報がユニーク情報と整合しないと判断し、両判断において整合すると判断したときに、複数の復号情報がユニーク情報と整合すると判断する。

[0061] また、ユニーク情報に、ユニーク部分（例えば、乱数値等）と、非ユニーク部分（例えば、装置の ID 等）とが含まれる場合には、復号情報にも、ユニーク部分に対応する情報と、非ユニーク部分に対応する情報とが含まれることになる。この場合には、認証部 24 は、複数の復号情報がユニーク情報と整合するかどうかを、ユニーク情報に含まれるユニーク部分と、復号情報

に含まれる、ユニーク部分に対応する情報とが整合するかどうかによって判断してもよく、ユニーク情報そのものと、復号情報そのものとが整合するかどうかによって判断してもよい。

[0062] なお、認証部24は、上記以外の判断を行ってもよい。認証部24は、認証要求に含まれている暗号情報を、復号鍵を用いて復号できなかった場合にも、その認証要求を送信した被認証装置1が正当ではないと判断してもよい。復号鍵が共通鍵暗号の鍵である場合には、その認証要求を送信した被認証装置1は、認証装置2が保持している共通鍵暗号の鍵を保持していないため、正当な被認証装置1ではないと考えられるからである。

[0063] また、認証部24は、複数の判断を行う場合に、すべての判断において被認証装置1が正当ではないと判断しなかったときに、被認証装置1が正当であると判断し、少なくともいずれかの判断において被認証装置1が正当ではないと判断したときに、被認証装置1が正当ではないと判断する。被認証装置1が正当であると判断することは、その被認証装置1を認証することである。また、被認証装置1が正当ではないと判断することは、その被認証装置1を認証しないことである。

[0064] 出力部25は、認証部24による判断結果を出力する。この判断結果は、被認証装置1が正当であるか、正当でないのかの判断結果、すなわち被認証装置1が認証されたのか、認証されなかったのかを示す情報である。出力部25は、認証部24による判断結果を、認証結果に応じて処理を行う構成や装置等に出力することが好適である。また、出力部25は、認証部24による判断結果を、認証要求の送信元である被認証装置1に送信してもよい。

[0065] ここで、この出力は、例えば、表示デバイス（例えば、液晶ディスプレイや有機ELディスプレイなど）への表示でもよく、所定の機器への通信回線を介した送信でもよく、プリンタによる印刷でもよく、スピーカによる音声出力でもよく、記録媒体への蓄積でもよく、他の構成要素への引き渡しでもよい。なお、出力部25は、出力を行うデバイス（例えば、表示デバイスや通信デバイス、プリンタなど）を含んでもよく、または含まなくてもよい。

また、出力部 25 は、ハードウェアによって実現されてもよく、または、これらのデバイスを駆動するドライバ等のソフトウェアによって実現されてもよい。

[0066] なお、ユニーク情報やユニーク部分が認証装置 2 から被認証装置 1 に送信される場合（例えば、チャレンジ・レスポンス認証が行われる場合）には、認証装置 2 は、ユニーク情報やユニーク部分を送信する送信部を備えていてもよい。その送信部は、例えば、認証要求の送信ごとに、ユニーク情報やユニーク部分を送信してもよく、複数のユニーク情報や、複数のユニーク部分を一括して送信してもよい。前者の場合には、ユニーク情報やユニーク部分の送信と、認証要求の受信とが繰り返されることになる。後者の場合には、複数のユニーク情報や、複数のユニーク部分は、認証要求の送信指示に含まれていてもよい。

[0067] 次に、被認証装置 1 の動作について図 2 のフローチャートを用いて説明する。図 2 は、被認証装置 1 が認証要求の送信を開始すると判断した後の処理である認証要求送信方法について示すフローチャートである。上記のように、被認証装置 1 は、例えば、所定の送信指示を受信した際に、認証要求の送信を開始すると判断してもよい。

[0068] （ステップ S 1 0 1）送信部 14 は、認証期間を開始させる。送信部 14 は、例えば、認証期間の終了を検知するために、タイマによる計時を開始してもよい。

[0069] （ステップ S 1 0 2）送信部 14 は、認証要求を送信するかどうか判断する。そして、認証要求を送信する場合には、ステップ S 1 0 3 に進み、そうでない場合には、ステップ S 1 0 6 に進む。例えば、認証要求を所定の時間間隔で送信する場合には、送信部 14 は、その所定の時間間隔ごとに、認証要求を送信すると判断してもよい。

[0070] （ステップ S 1 0 3）取得部 11 は、ユニーク情報を取得する。このユニーク情報の取得は、例えば、ユニーク部分の取得と、取得したユニーク部分と、非ユニーク部分との結合とによって行われてもよい。

- [0071] (ステップS 1 0 4) 暗号化部 1 3 は、暗号鍵を用いて、ステップS 1 0 3 で取得されたユニーク情報を暗号化して、暗号情報を生成する。
- [0072] (ステップS 1 0 5) 送信部 1 4 は、ステップS 1 0 4 で生成された暗号情報を含む認証要求を送信する。なお、認証要求には、暗号情報以外の情報が含まれていてもよい。そして、ステップS 1 0 2 に戻る。
- [0073] (ステップS 1 0 6) 送信部 1 4 は、認証要求の送信を終了するかどうか判断する。そして、終了する場合には、認証要求を送信する一連の処理が終了となり、そうでない場合には、ステップS 1 0 2 に戻る。なお、送信部 1 4 は、例えば、ステップS 1 0 1 で開始された認証期間が終了した場合に、認証要求の送信を終了すると判断してもよい。具体的には、送信部 1 4 は、ステップS 1 0 1 で計時を開始したタイマの値が、認証期間の時間的な長さを超えた場合に、認証要求の送信を終了すると判断し、そうでない場合に、終了しないと判断してもよい。
- [0074] なお、図 2 のフローチャートでは、ユニーク情報の取得と、暗号情報の生成と、認証要求の送信とが繰り返される場合について示しているが、そうでなくてもよい。例えば、複数のユニーク情報が取得され、その複数のユニーク情報をそれぞれ暗号化した複数の暗号情報が生成された後に、各暗号情報を含む認証要求の送信が繰り返されてもよい。また、同じユニーク情報が暗号化された暗号情報が、複数の認証要求に含まれる場合には、ユニーク情報の重複数だけ、ユニーク情報の取得や、暗号情報の生成が行われず、同じユニーク情報や、同じ暗号情報が繰り返して用いられてもよい。また、ステップS 1 0 1 やステップS 1 0 6 における認証期間の管理は、送信部 1 4 以外の構成要素、例えば、取得部 1 1 等によって行われてもよい。また、図 2 のフローチャートにおける処理の順序は一例であり、同様の結果を得られるのであれば、各ステップの順序を変更してもよい。
- [0075] 次に、認証装置 2 の動作について図 3 のフローチャートを用いて説明する。図 3 は、認証装置 2 による複数の認証要求を用いた被認証装置 1 の認証に関する処理である認証方法について示すフローチャートである。

- [0076] (ステップS201) 受信部21は、認証要求を受信したかどうか判断する。そして、認証要求を受信した場合には、ステップS202に進み、そうでない場合には、ステップS203に進む。なお、受信部21が間欠的に認証要求を受信する場合には、受信部21は、受信期間にのみ認証要求を受信し、受信期間ではない期間には、認証要求を受信しなくてもよい。
- [0077] (ステップS202) 復号部23は、ステップS201で受信された認証要求に含まれる暗号情報を、復号鍵を用いて復号し、復号情報を取得する。そして、ステップS201に戻る。復号部23は、その復号情報を、認証要求の送信元である被認証装置1のIDに対応付けて記憶部22に蓄積してもよい。また、復号部23は、復号情報を、その復号情報に対応する認証要求の受信時刻に対応付けて記憶部22に蓄積してもよい。なお、ステップS201で受信された認証要求に含まれる暗号情報が、復号鍵を用いて復号できない場合には、復号部23は、復号を行うことなく、ステップS201に戻ってもよい。また、この場合には、認証部24は、復号できない暗号情報を含んでいる認証要求の送信元である被認証装置1について、正当ではないと判断してもよい。
- [0078] (ステップS203) 認証部24は、認証の処理を行うかどうか判断する。そして、認証の処理を行う場合には、ステップS204に進み、そうでない場合には、ステップS201に戻る。認証部24は、例えば、ある共通鍵暗号の鍵で復号できた暗号情報を含む1個目の認証要求が受信されてから認証期間が経過した際に、その共通鍵暗号の鍵で復号できた暗号情報を含む複数の認証要求を用いた認証の処理を行うと判断してもよい。また、認証部24は、例えば、あるIDの被認証装置1から1個目の認証要求を受信してから認証期間が経過した際に、そのIDの被認証装置1から送信された複数の認証要求を用いた認証の処理を行うと判断してもよい。
- [0079] (ステップS204) 認証部24は、複数の認証要求からそれぞれ取得された複数の復号情報に所定数以上の重複が存在するかどうか判断する。そして、複数の復号情報に所定数以上の重複が存在する場合には、ステップS2

０９に進み、そうでない場合には、ステップＳ２０５に進む。

[0080] （ステップＳ２０５）認証部２４は、所定の期間における認証要求の受信回数が、あらかじめ決められた閾値の回数を超えているかどうか判断する。そして、認証要求の受信回数があらかじめ決められた閾値の回数を超えている場合には、ステップＳ２０９に進み、そうでない場合には、ステップＳ２０６に進む。

[0081] （ステップＳ２０６）認証部２４は、認証期間における認証要求の受信間隔に、確率が閾値より低い受信間隔が含まれるかどうか判断する。そして、認証要求の受信間隔に、確率が閾値より低い受信間隔が含まれる場合には、ステップＳ２０９に進み、そうでない場合には、ステップＳ２０７に進む。

[0082] （ステップＳ２０７）認証部２４は、認証期間に受信された複数の認証要求にそれぞれ対応する複数の復号情報が、ユニーク情報と整合するかどうか判断する。そして、複数の復号情報がユニーク情報と整合する場合には、ステップＳ２０８に進み、整合しない場合には、ステップＳ２０９に進む。

[0083] なお、ステップＳ２０４からステップＳ２０７までの処理は、例えば、復号鍵によって復号できた暗号情報を含む、認証期間内に受信された複数の認証要求について行われるものとする。すなわち、ステップＳ２０４からステップＳ２０７までの処理は、例えば、あるＩＤの被認証装置１から認証期間内に受信された複数の認証要求について行われてもよい。

[0084] （ステップＳ２０８）認証部２４は、複数の認証要求を送信した被認証装置１が正当であると判断する。すなわち、その被認証装置１が認証されたことになる。

[0085] （ステップＳ２０９）認証部２４は、複数の認証要求を送信した被認証装置１が正当でないと判断する。すなわち、その被認証装置１が認証されなかったことになる。

[0086] （ステップＳ２１０）出力部２５は、ステップＳ２０８、Ｓ２０９の判断結果を出力する。そして、ステップＳ２０１に戻る。

[0087] なお、図３のフローチャートでは、認証の処理において、ステップＳ２０

4からステップS207までの各処理を行う場合について示しているが、そうでなくてもよい。それらの処理のうち、1以上の処理を行わなくてもよい。ただし、その場合であっても、複数の認証要求を用いた認証の処理、例えば、ステップS204からステップS206までの少なくともいずれかの処理は行われることが好適である。また、図3のフローチャートにおける処理の順序は一例であり、同様の結果を得られるのであれば、各ステップの順序を変更してもよい。例えば、ステップS204からステップS207までの各処理を異なる順序にしてもよい。また、図3のフローチャートにおいて、電源オフや処理終了の割り込みにより処理は終了する。

[0088] 次に、本実施の形態による被認証装置1及び認証装置2の動作について、具体例を用いて説明する。この具体例では、認証装置2の受信部21は、間欠的に認証要求を受信するものとする。すなわち、受信部21は、受信期間にのみ認証要求を受信し、それ以外の期間には、被認証装置1から送信された認証要求を受信しないものとする。

[0089] また、この具体例では、正当な被認証装置1は、認証期間に10個の認証要求を送信するものとする。上記のように、受信部21は、間欠的な受信を行うため、認証部24は、ある被認証装置1から認証期間に受信された認証要求の個数が、閾値「7」を超える場合に、その被認証装置1が正当でないと判断するものとする。

[0090] また、この具体例では、ユニーク情報が時刻であるとする。そして、認証部24は、復号情報である時刻と、その復号情報に対応する認証要求が受信された時刻との差があらかじめ決められた閾値を超えている場合に、その認証要求を送信した被認証装置1が正当ではないと判断するものとする。また、ユニーク情報は、共通鍵暗号の鍵によって暗号化されるものとする。

[0091] また、この具体例では、送信される認証要求ごとに、異なるユニーク情報が暗号化された暗号情報が含まれる場合について主に説明し、認証期間に送信される複数の認証要求に、同じユニーク情報が暗号化された暗号情報が含まれる場合については後述する。

[0092] [正当な被認証装置 1 のみからの認証要求の送信]

まず、正当な被認証装置 1 のみから認証要求が送信される場合について、図 4 を用いて説明する。図 4 で示されるように、時刻 $t_1 \sim t_{10}$ に、それぞれユニーク情報である時刻 $t_1 \sim t_{10}$ を暗号化した情報を含む認証要求が、被認証装置 1 から認証装置 2 に送信されるものとする。

[0093] 具体的には、被認証装置 1 の送信部 14 は、認証装置 2 から送信された、認証装置 2 の ID を含む送信指示を受信すると、タイマによる計時を開始する（ステップ S101）。なお、その時点の時刻は t_1 であったとする。また、被認証装置 1 は、例えば、記憶部 12 で記憶されている認証装置 2 の ID と、送信指示に含まれる ID とが一致することによって、送信指示が認証装置 2 から送信されたと判断してもよい。また、1 個目の認証要求の送信であるため、送信部 14 は、時間待ちを行わないですぐに認証要求を送信すると判断し、図示しない経路で、取得部 11 に、ユニーク情報の取得の指示を渡す（ステップ S102）。その指示を受け取ると、取得部 11 は、その時点の時刻 t_1 であるユニーク情報を取得して暗号化部 13 に渡す（ステップ S103）。ユニーク情報である時刻 t_1 を受け取ると、暗号化部 13 は、記憶部 12 で記憶されている被認証装置 1 の ID を取得すると共に、送信指示または記憶部 12 から認証装置 2 の ID を取得し、時刻 t_1 と、被認証装置 1 の ID と、認証装置 2 の ID とを、記憶部 12 で記憶されている共通鍵暗号の鍵を用いて暗号化して暗号情報を生成し、送信部 14 に渡す（ステップ S104）。暗号情報を受け取ると、送信部 14 は、その暗号情報と、記憶部 12 から取得した被認証装置 1 の ID とを含む認証要求を BLE 通信のブロードキャストによって送信する（ステップ S105）。このような認証要求の送信が繰り返されることによって、時刻 t_{10} までに 10 個の認証要求が被認証装置 1 から認証装置 2 に送信される（ステップ S102～S105）。なお、時刻 t_{10} に 10 個目の認証要求が送信された直後に、時刻 t_1 に開始されたタイマの値が、認証期間の時間的な長さを超えたとなると、認証要求の送信の処理が終了される（ステップ S106）。

- [0094] 認証装置2の受信部21が間欠的な受信を行っているとする、図4で示されるように、時刻 t_2 、 t_4 、 t_5 、 t_7 、 t_8 、 t_{10} に送信された認証要求のみが認証装置2で受信されることになる。そして、各認証要求が受信されると（ステップS201）、復号部23は、認証要求に含まれる被認証装置1のIDを取得し、そのIDに対応付けられている共通鍵暗号の鍵を、記憶部22から取得する。そのようにして取得した共通鍵暗号の鍵を用いて、復号部23は、受信された認証要求に含まれる暗号情報を復号して復号情報を取得する（ステップS202）。そして、復号部23は、復号情報に含まれる被認証装置1のIDが、認証要求に平文で含まれる被認証装置1のIDと一致するかどうか、また、復号情報に含まれる認証装置2のIDが、自装置のIDと一致するかどうか判断する。この場合には、いずれにおいてもIDが一致したものとする。すると、復号部23は、その復号情報を、認証要求に含まれる被認証装置1のID、及びその認証要求の受信時刻に対応付けて記憶部22に蓄積する。なお、いずれか一方のIDが一致しなかった場合には、復号部23は、その復号情報を記憶部22に蓄積しなくてもよい。このような処理が、認証要求が受信されるごとに繰り返される。
- [0095] 認証部24は、記憶部22において記憶されている復号情報について、被認証装置1のIDごとに、最も古い受信時刻から現在の時刻までの期間が、認証期間の時間的な長さを超えたかどうか判断する。そして、最も古い受信時刻から現在の時刻までの期間が、認証期間の時間的な長さを超えたIDが存在する場合には、認証部24は、そのIDの被認証装置1について、認証の処理を行うと判断し、そのIDに対応付けられて記憶されている複数の復号情報や受信時刻を用いて認証の処理を行う（ステップS203）。
- [0096] 具体的には、認証部24は、復号情報に重複が存在するかどうか判断する（ステップS204）。この場合には、各復号情報は、異なる時刻を含んでいるため、各復号情報は重複しないことになる。そのため、認証部24は、受信回数が閾値を超えているかどうか判断する（ステップS205）。この具体例では、上記のように、閾値は「7」に設定されていたとする。すると

、図4で示されるように、受信回数「6」が、閾値「7」を超えていないと判断される。

[0097] 次に、認証部24は、記憶部22で記憶されている受信時刻を用いて、ある認証要求が受信されてから次の認証要求が受信されるまでの時間間隔である受信間隔をそれぞれ取得する。そして、その受信間隔に、記憶部22で記憶されている、確率が閾値より低い受信間隔が含まれているかどうか判断する（ステップS206）。この場合には、確率が閾値より低い受信間隔は含まれていなかったとする。そのため、認証部24は、復号情報がユニーク情報に整合するかどうか判断する（ステップS207）。なお、ここでは、復号情報のうち、ユニーク部分である時刻が、受信時刻と整合するかどうか判断されるものとする。具体的には、上記のように、復号情報に含まれる時刻と、その復号情報に対応する認証要求の受信時刻との差が、あらかじめ決められた閾値より小さい場合に、認証部24は、その復号情報がユニーク情報に整合していると判断するものとする。そして、認証部24は、各復号情報について、そのような判断を行う。この具体例では、すべての復号情報がユニーク情報に整合していると判断されたとする。すると、認証部24は、複数の認証要求を送信した被認証装置1が正当であると判断する（ステップS208）。そして、出力部25は、その判断結果を出力する（ステップS209）。なお、一連の判断が終了した後に、記憶部22で記憶されている、判断対象の被認証装置1のIDに対応する復号情報等が削除されてもよく、または、その復号情報等について処理済みである旨のフラグ等が設定されてもよい。後者の場合には、処理済みである旨のフラグ等が設定されている復号情報等は、それ以降の認証の処理では用いられないものとする。

[0098] [異なる共通鍵暗号の鍵を用いた認証要求の送信]

攻撃者の装置から、正当な被認証装置1とは異なる共通鍵暗号の鍵を用いて暗号化された暗号情報を含む認証要求が送信された場合について説明する。この場合には、例えば、図5で示されるように、攻撃者の装置から認証装置2に送信される認証要求に含まれる各暗号情報は、異なる共通鍵暗号の鍵

で暗号化されている。なお、認証要求には、攻撃者の装置のIDが平文で含まれているが、そのIDに対応する共通鍵暗号の鍵は、認証装置2の記憶部22で記憶されていないものとする。すると、認証装置2において、各認証要求は受信されるが（ステップS201）、復号部23によって復号することができないため、復号情報が取得できないことになる（ステップS202）。したがって、共通鍵暗号の鍵によって復号できた暗号情報を含む認証要求を用いた認証を行うことができず、その結果、その攻撃者の装置が正当な被認証装置1と判断されることはないことになる。すなわち、その攻撃者の装置は認証されないことになる。

[0099] [1個の認証要求の繰り返しての送信]

正当な被認証装置1から送信された1個の認証要求を受信した攻撃者の装置が、その認証要求を、認証装置2に繰り返して送信した場合について説明する。攻撃者の装置は、時刻t3に正当な被認証装置1から送信された認証要求を受信し、図6で示されるように、正当な被認証装置1から送信される認証要求の認証期間が終了した後の時刻t21から、その認証要求を繰り返して認証装置2に送信したとする。この場合には、認証要求に含まれる暗号情報は、正当な被認証装置1の共通鍵暗号の鍵で暗号化されているため、復号することができる。したがって、図6で示される時刻t22, t24, t25, t27, t28, t30にそれぞれ送信された認証要求は、認証装置2の受信部21によって受信され、その認証要求に含まれる暗号情報が、復号部23によって復号され、復号後の復号情報が、攻撃者の装置とは異なる被認証装置1のID、及び受信時刻に対応付けられて記憶部22に蓄積されることになる（ステップS201, S202）。

[0100] そして、認証部24による認証が開始されると（ステップS203）、復号情報がすべて同じであるため、復号情報に重複が存在すると判断され、攻撃者の装置は、正当な被認証装置1ではないと判断される（ステップS209）。このように、1個の正当な認証要求が攻撃に用いられたとしても、攻撃者の装置は認証されないことになる。また、この場合には、復号情報がユ

ニーク情報に整合しないため、そのことによって、被認証装置 1 が正当ではないと判断することができる。

[0101] [複数の認証要求の後からの送信]

正当な被認証装置 1 から送信されたすべての認証要求を受信した攻撃者の装置が、その複数の認証要求を、認証装置 2 に送信した場合について説明する。攻撃者の装置は、時刻 $t_1 \sim t_{10}$ に正当な被認証装置 1 から送信された認証要求をそれぞれ受信し、図 7 で示されるように、正当な被認証装置 1 から送信される認証要求の認証期間が終了した後の時刻 t_{21} から、同様の時間間隔で、その複数の認証要求をそれぞれ認証装置 2 に送信したとする。この場合には、認証要求に含まれる暗号情報は、正当な被認証装置 1 の共通鍵暗号の鍵で暗号化されているため、復号することができる。したがって、図 7 で示される時刻 t_{22} , t_{24} , t_{25} , t_{27} , t_{28} , t_{30} にそれぞれ送信された認証要求は、認証装置 2 の受信部 21 によって受信され、その認証要求に含まれる暗号情報が、復号部 23 によって復号され、復号後の復号情報が、攻撃者の装置とは異なる被認証装置 1 の ID、及び受信時刻に対応付けられて記憶部 22 に蓄積されることになる（ステップ S201, S202）。

[0102] そして、認証部 24 による認証が開始され、復号情報に重複がなく、受信回数「6」も閾値「7」を超えておらず、認証要求の受信間隔にも、確率が閾値より低い受信間隔が含まれていないと判断されたとする（ステップ S203～S206）。しかしながら、この場合には、復号情報に含まれる時刻と、受信時刻との差が、あらかじめ決められていた閾値より大きかったとする。そのため、認証部 24 は、複数の復号情報がユニーク情報に整合しないことにより、攻撃者の装置が、正当な被認証装置 1 ではないと判断する（ステップ S207, S209）。このように、複数の正当な認証要求が攻撃に用いられたとしても、攻撃者の装置は認証されないことになる。

[0103] [受信した認証要求のリレー送信]

正当な被認証装置 1 から送信された認証要求を受信した攻撃者の装置が、

その認証要求を、認証装置2に即座に送信した場合について説明する。攻撃者の装置は、時刻 t_3 , t_6 , t_9 に正当な被認証装置1から送信された認証要求を受信し、図8で示されるように、その認証要求を認証装置2に中継（リレー）して送信したとする。この場合には、攻撃者の装置からの認証要求に含まれる暗号情報は復号できるため、復号後の復号情報が記憶部22に蓄積されることになる（ステップS201, S202）。

[0104] ここで、図8で示されるように、攻撃者の装置は、偶然、認証装置2で受信されていない認証要求を、認証装置2の受信期間に送信できたとする。すると、認証の処理において、復号情報に重複は存在しないことになり、重複によって不正を検出することはできないことになる（ステップS203, S204）。一方、この場合には、正当な被認証装置1からの認証要求と、攻撃者の装置からの認証要求とが認証装置2で受信されることになり、認証要求の受信回数「9」が閾値「7」を超えることになる（ステップS205）。したがって、認証部24は、受信回数が多いことによって、認証要求を送信した装置が正当でないと判断することができることになる。

[0105] なお、図8において、攻撃者の装置から送信される認証要求の個数が1個であった場合には、認証要求の受信回数が閾値を超えていることによって不正を検出することはできないことになる。一方、その場合でも、攻撃者の装置から送信される認証要求は、正当な被認証装置1から送信される認証要求よりも遅れて送信されるため、認証装置2で受信される認証要求の受信間隔が、正当な被認証装置1から送信された認証要求の受信間隔とは異なったものとなり、その結果、その受信間隔に、確率が閾値より低い受信間隔が含まれる可能性が高くなる。したがって、そのような場合でも、認証部24は、認証要求の受信間隔を用いることによって、認証要求を送信した装置が正当でないと判断できる可能性もある（ステップS206）。

[0106] また、図8とは異なり、攻撃者の装置から送信された認証要求が、すでに認証装置2で受信されていた場合には、復号情報に重複が存在することになり、そのことによって、認証部24は、認証要求を送信した装置が正当でな

いと判断することができる（ステップS204）。

[0107] [受信した認証要求の異なる場所へのリレー送信]

正当な被認証装置1から送信された認証要求を受信した攻撃者の装置が、その認証要求を、他の攻撃者の装置を介して別の認証装置2に即座に送信した場合について説明する。攻撃者の装置が認証要求を中継することは、図8の場合と同様であるが、ここでは、中継された認証要求の送信先の認証装置2が、正当な被認証装置1の認証要求の送信先とは異なっているものとする。

[0108] 図9で示されるように、第1の場所において、正当な被認証装置1から送信された認証要求を攻撃者の第1の装置が受信し、その受信した認証要求を即座に、第2の場所に存在する攻撃者の第2の装置に送信し、攻撃者の第2の装置が、第2の場所において、第1の場所の認証装置2とは別の認証装置2に、受信した認証要求を即座に送信したとする。この場合には、復号情報の重複や受信回数が多いことによって、不正を検出することはできない。一方、第1の場所から第2の場所に認証要求を送信する場合には、その送信に関する伝送時間の揺らぎに起因して、第2の場所で受信される認証要求の受信間隔が、第1の場所における受信間隔とは異なるものとなる。したがって、第2の場所においては、認証要求の受信間隔に、確率が閾値より低い受信間隔が含まれる可能性が高くなり、そのことを利用して、第2の場所に存在する認証装置2の認証部24は、第2の場所において認証要求を送信した装置が正当でないと判断できる可能性もある（ステップS206）。

[0109] また、第2の場所における認証装置2の認証部24が、複数の復号情報について、復号情報である時刻と、その復号情報に対応する認証要求の受信時刻との差である時刻差をそれぞれ取得し、取得した複数の時刻差が一定でないときに、複数の復号情報がユニーク情報と整合しないと判断する場合には、伝送時間の揺らぎによって、複数の時刻差が一定にならないことによって、複数の復号情報がユニーク情報と整合しないと判断される可能性もあり、その結果、第2の場所において認証要求を送信した装置が正当ではないと判

断できる可能性もある（ステップS207）。

[0110] なお、第1の場所において取得された認証要求が、第2の場所で用いられる不正を検出できるようにするため、ユニーク情報に、被認証装置1の位置情報を含めてもよい。その位置情報は、その位置情報を含むユニーク情報が暗号化された暗号情報を含む認証要求が送信される際の被認証装置1の位置を示す位置情報であることが好適である。上記のように、ユニーク情報には、ユニーク部分と、非ユニーク部分とを含めることができるが、その非ユニーク部分として、被認証装置1の位置情報を含めるようにしてもよい。この場合には、被認証装置1は、その被認証装置1の位置を示す位置情報を取得するための位置取得部をさらに備えていてもよい。位置情報は、例えば、緯度・経度であってもよく、位置を示すその他の座標値等であってもよい。また、位置取得部による位置の取得は、例えば、GPS（Global Positioning System）を用いる方法や屋内GPSを用いる方法、最寄りの無線基地局を用いる方法などのように無線通信を用いて行われてもよく、SLAM（Simultaneous Localization and Mapping）で知られているように、周囲の物体までの距離の測定結果を用いて行われてもよく、Visual-SLAMで知られているように、周囲の画像を撮影することによって行われてもよく、位置を取得できるその他の方法を用いて行われてもよい。この場合には、認証要求を受信した認証装置2の認証部24は、復号情報に含まれる位置情報が、自装置の位置情報から所定の範囲内（例えば、20メートル以内や、10メートル以内、5メートル以内など）でないときに、復号情報がユニーク情報に整合していないと判断してもよい。また、この判断とは別に、復号情報に含まれるユニーク部分に対応する情報が、ユニーク情報のユニーク部分と整合するかどうかの判断も行われてもよい。そして、いずれかの判断において、整合していないと判断された場合には、認証要求を送信した被認証装置1が正当ではないと判断されてもよい。この場合には、認証装置2も、その認証装置2の位置を示す位置情報を取得するための位置取得部をさらに備えていてもよい。そして、その位置取得部によって取得された位置情報を用いて

、復号情報に含まれる位置情報が、認証装置 2 の位置情報から所定の範囲内であるかどうか判断されてもよい。認証装置 2 が有する位置取得部や、その位置取得部によって取得される位置情報も、上記説明と同様のものであり、その説明を省略する。

[0111] また、暗号鍵が共通鍵暗号の鍵ではなく、公開鍵暗号の公開鍵である場合であっても、ユニーク情報の種類について知ることができなければ、攻撃者は、ユニーク情報を生成して暗号化することはできず、上記のように、正当な被認証装置 1 から送信された認証要求をコピーして用いることしかできないことになる。そして、そのような状況では、共通鍵暗号の鍵を用いた場合と同様に不正を検出することができる。

[0112] また、取得部 11 によって取得されるユニーク情報に重複が存在し、その結果として、同じ暗号情報を含む複数の認証要求が送信される場合には、上記のように、認証部 24 は、複数の復号情報に、所定数以上の重複が存在するときに、被認証装置 1 が正当でないと判断してもよい。具体的には、時刻であるユニーク情報が、100ミリ秒の精度の時計を用いて50ミリ秒ごとに取得される場合には、ユニーク情報の重複数は2個であり、ユニーク情報は2個ごとに異なる値となる。そのような場合であっても、3個以上の復号情報が同じであるときには、攻撃者からも認証要求が送信されたことを検出することができることになる。また、認証装置 2 が間欠的な受信を行っており、上記の状況において、正当な被認証装置 1 から送信される、同じユニーク情報に対応する2個の認証要求のうち、一方の認証要求しか受信されない場合には、認証部 24 は、複数の復号情報に重複が存在するときに、攻撃者からも認証要求が送信されたことを検出することができる。

[0113] 最後に、本実施の形態による認証装置 2 を実装した装置やシステムなどの例について簡単に説明する。

認証装置 2 は、自動改札機に組み込まれていてもよい。そして、自動改札機は、認証要求の送信指示であるビーコンを定期的に発信していてもよい。ユーザが有する被認証装置 1 は、そのビーコンである送信指示を受信すると

、上記のようにして複数の認証要求を自動改札機の認証装置 2 に送信する。認証装置 2 が、その複数の認証要求を用いて、被認証装置 1 が正当であると判断すると、自動改札機のゲートが開き、ユーザは、改札内に入ったり、改札外に出たりすることができる。また、ユーザが改札内に入る際に、または改札外に出る際に、ユーザへの課金が行われる。このようにして、例えば、ユーザは被認証装置 1 であるスマートフォン等を操作することなく、電車等に乗ることができるようになる。

[0114] 認証装置 2 は、飲み物などの自動販売機に組み込まれてもよい。そして、自動販売機の購入ボタンをユーザが操作すると、自動販売機は、認証要求の送信指示を発信してもよい。ユーザが有する被認証装置 1 は、その送信指示を受信すると、上記のようにして複数の認証要求を自動販売機の認証装置 2 に送信する。認証装置 2 が、その複数の認証要求を用いて、被認証装置 1 が正当であると判断すると、ユーザが操作した購入ボタンに応じた飲み物などの商品が自動販売機から出てくることになり、ユーザは、その商品を受け取ることができる。また、その処理に応じて、適宜、ユーザへの課金が行われる。このようにして、例えば、ユーザは被認証装置 1 であるスマートフォン等を操作することなく、自動販売機で商品を購入することができるようになる。

[0115] 認証装置 2 は、コンサートやスポーツの試合、セミナーなどのイベントの会場、美術館、博物館、テーマパーク、スポーツクラブ、会員制のラウンジなどの入り口付近に設置されてもよい。この場合には、共通鍵暗号の鍵が、イベント等のチケットや、会員証となってもよい。そして、認証装置 2 は、認証要求の送信指示であるビーコンを定期的に発信してもよい。ユーザが有する被認証装置 1 は、そのビーコンである送信指示を受信すると、上記のようにして複数の認証要求を会場の入り口付近の認証装置 2 に送信する。認証装置 2 が、その複数の認証要求を用いて、被認証装置 1 が正当であると判断すると、例えば、認証要求の電波の強度などを用いて被認証装置 1 の位置を特定し、その特定した位置に、共通鍵暗号の鍵に対応するチケット

等の情報（例えば、チケットの種類の情報や、あらかじめ登録されているチケットの所有者の情報など）を表示する出力を行ってもよい。そして、その表示を見ることによって、イベント等のスタッフは、入り口から入ってくる人のうち、チケットや会員証を持っていない人を特定することができる。なお、チケット等を持っていない人については、スタッフがチケット等の提示を求めるようにしてもよい。このようにして、例えば、ユーザは被認証装置 1 であるスマートフォン等を操作することなく、イベントの会場や、美術館、スポーツクラブ等に入ることができるようになる。

[0116] 認証装置 2 は、店舗のキャッシュレジスタに組み込まれてもよい。そして、例えば、キャッシュレジスタの支払いボタンをユーザや店員が操作すると、キャッシュレジスタは、認証要求の送信指示を発信してもよい。ユーザが有する被認証装置 1 は、その送信指示を受信すると、上記のようにして複数の認証要求をキャッシュレジスタの認証装置 2 に送信する。認証装置 2 が、その複数の認証要求を用いて、被認証装置 1 が正当であると判断すると、共通鍵暗号の鍵に対応付けられて登録されている支払い手段（例えば、クレジットカードや電子マネーなど）に対して、購入金額に応じた課金が行われることによって、ユーザは、商品等の購入対象を受け取ることができてもよい。このようにして、例えば、ユーザは被認証装置 1 であるスマートフォン等を操作することなく、店舗で商品等を購入することができるようになる。

[0117] 認証装置 2 は、P C (Personal Computer) や A T M (Automated Teller Machine) などの本人認証が必要な装置に組み込まれてもよい。そして、例えば、P C や A T M などの装置をユーザが操作すると、その装置は、認証要求の送信指示を発信してもよい。ユーザが有する被認証装置 1 は、その送信指示を受信すると、上記のようにして複数の認証要求をその装置の認証装置 2 に送信する。認証装置 2 が、その複数の認証要求を用いて、被認証装置 1 が正当であると判断すると、共通鍵暗号の鍵に対応付けられて登録されているユーザに関して、例えば、P C へのログインが行われてもよく、P C で操作しているウェブサイトへのログインが行われてもよく、A T M での現金の引

き出しなどが行われてもよい。このようにして、例えば、ユーザは暗証番号の入力等を行うことなく、P CやA T Mなどの装置における本人認証を行うことができ、その装置を操作することができるようになる。

[0118] また、本実施の形態による被認証装置1及び認証装置2は、上記した以外の状況においても用いることができる。例えば、カーシェアリングや、レンタカー、飛行機の搭乗手続等における認証に用いられてもよい。また、例えば、パソコンなどの機器を操作する際のユーザ認証等に用いられてもよい。

[0119] 以上のように、本実施の形態による被認証装置1及び認証要求送信方法によれば、ユニーク情報が暗号化された暗号情報を含む複数の認証要求を、認証装置2に送信することができる。また、例えば、暗号化が共通鍵暗号の鍵を用いて行われる場合には、より高速に暗号化を行うことができるようになる。また、ユニーク情報が、乱数値やカウンタ値、時刻等を含むものである場合には、低負荷でユニーク情報を生成することができるというメリットもある。また、そのようなユニーク情報を用いることによって、ユニーク情報の情報量を少なくすることもでき、その結果として、認証要求に含まれる情報量を少なくすることもできる。したがって、例えば、B L E通信などのように、ペイロード長に制限のある通信規格でも、認証要求を送信できるようになる。また、上記説明のように、ユーザによる操作を介することなく、認証を行うこともでき、ユーザの利便性を向上させることができる。

[0120] また、本実施の形態による認証装置2及び認証方法によれば、被認証装置1から送信された複数の認証要求を用いることによって、簡単な処理により、セキュアな認証を実現することができる。暗号情報において、ユニーク情報が共通鍵暗号の鍵を用いて暗号化されている場合には、その暗号情報を復号する処理を高速に行うことができる。また、共通鍵暗号の鍵が漏洩していない場合や、ユニーク情報の種類が知られていない場合には、攻撃者の装置は、正当な被認証装置1から受信した認証要求を認証装置2に送信することによって攻撃を行うことしかできないことになる。そのため、例えば、複数の復号情報に所定数以上の重複が存在するかどうかの判断処理や、所定の期

間の受信回数が閾値を超えているかどうかの判断処理、認証要求の受信間隔に、確率が閾値より低い間隔が含まれているかどうかの判断処理、認証要求から取得された復号情報がユニーク情報に整合するかどうかの判断処理などの簡単な処理によって、認証要求の送信元に攻撃者の装置が含まれているかどうかを検出することができるようになる。このようにして、なりすましによる攻撃に対応することができるようになり、セキュアな認証を実現することができる。また、複数の認証要求を用いて被認証装置 1 が正当であるかどうかを判断するため、1 個の認証要求だけでは検出することができない不正についても、検出することができるようになり、安全性を向上させることができる。また、認証装置 2 が、BLE 通信のように、間欠的に認証要求を受信する場合においても、上記認証を適切に行うことができる。また、そのような間欠的な認証要求の受信を行うことによって、認証装置 2 における消費電力を低減することもできる。

[0121] なお、本実施の形態では、認証部 24 が、復号情報の重複に関する判断、認証要求の受信回数に関する判断、認証要求の受信間隔に関する判断、復号情報とユニーク情報との整合性に関する判断によって被認証装置 1 が正当であるかどうか判断する場合について説明したが、認証部 24 は、それらの判断のうち、少なくとも 1 個以上の判断によって被認証装置 1 が正当であるかどうかを判断してもよい。

[0122] 例えば、共通鍵暗号の鍵が 1 回の認証にのみ用いられる場合（例えば、共通鍵暗号の鍵が入場券等に対応している場合など）であって、送信される認証要求ごとに、異なるユニーク情報が暗号化された暗号情報が含まれている場合には、認証部 24 は、復号情報に重複が存在するかどうかの判断のみによって、被認証装置 1 の正当性を判断してもよい。そのような場合には、攻撃者の装置が、正当な被認証装置 1 から送信された認証要求を、別の場所や機会に使用することはできず、また、攻撃者の装置から送信された認証要求が認証装置 2 で受信されることによって、複数の復号情報に重複が存在することになるからである。

- [0123] また、例えば、共通鍵暗号の鍵が1回の認証にのみ用いられる場合には、認証部24は、所定の期間における認証要求の受信回数が閾値を超えているかどうか判断のみによって、被認証装置1の正当性を判断してもよい。そのような場合には、攻撃者の装置が、正当な被認証装置1から送信された認証要求を、別の場所や機会に使用することはできず、また、攻撃者の装置から送信された認証要求が認証装置2で受信されることによって、受信回数があらかじめ決められた回数を超えることになるからである。
- [0124] また、例えば、認証要求の受信が間欠的ではなく、連続して行われる場合であって、共通鍵暗号の鍵が1回の認証にのみ用いられる場合であって、正当な被認証装置1からの認証要求の送信間隔があらかじめ規定されている場合には、認証部24は、認証期間における認証要求の受信間隔に、確率が閾値より低い受信間隔が含まれるかどうかの判断のみによって、被認証装置1の正当性を判断してもよい。そのような場合には、攻撃者の装置が、正当な被認証装置1から送信された認証要求を、別の場所や機会に使用することはできず、また、攻撃者の装置から認証要求が送信されることによって、認証要求の受信間隔に、通常とは異なる、確率が閾値より低い受信間隔が含まれることになるからである。
- [0125] また、例えば、共通鍵暗号の鍵が1回の認証にのみ用いられる場合には、認証部24は、複数の復号情報がユニーク情報と整合するかどうかの判断のみによって、被認証装置1の正当性を判断してもよい。そのような場合には、攻撃者の装置が、正当な被認証装置1から送信された認証要求を、別の場所や機会に使用することはできず、また、攻撃者の装置から送信された認証要求が認証装置2で受信されることによって、複数の復号情報とユニーク情報とが整合しなくなるからである。
- [0126] また、上記実施の形態では、被認証装置1と認証装置2との間でユーザの操作を介することなく認証の処理が行われる場合について主に説明したが、そうでなくてもよい。例えば、被認証装置1において、ユーザの操作に応じて、認証要求の送信が開始されてもよい。

- [0127] また、上記実施の形態による被認証装置 1 や認証装置 2 は、他の認証方法を補完するために用いられてもよい。例えば、顔認証だけでは安全性に問題がある場合に、顔認証と、上記実施の形態における認証とを組み合わせで用いるようにしてもよい。従来、顔認証だけでは安全性に問題がある場合に、別途、ICカードを用いた認証などを併用することが行われていたが、上記実施の形態による認証と顔認証とを組み合わせで用いることによって、ICカード等を用いないでもよいことになり、ユーザの利便性が向上することになる。なお、上記実施の形態による被認証装置 1 や認証装置 2 は、例えば、顔認証以外の生体認証や、生体認証以外の認証と組み合わせで用いられてもよい。
- [0128] また、上記実施の形態において、被認証装置 1 は、例えば、ユーザが保持するものであってもよく、または、移動体に搭載されるものであってもよい。後者の場合には、例えば、移動体に関する認証を行うこともできるようになる。移動体は、例えば、走行する走行体や、飛行する飛行体であってもよい。
- [0129] また、上記実施の形態において、各処理または各機能は、単一の装置または単一のシステムによって集中処理されることによって実現されてもよく、または、複数の装置または複数のシステムによって分散処理されることによって実現されてもよい。
- [0130] また、上記実施の形態において、各構成要素間で行われる情報の受け渡しは、例えば、その情報の受け渡しを行う 2 個の構成要素が物理的に異なるものである場合には、一方の構成要素による情報の出力と、他方の構成要素による情報の受け付けとによって行われてもよく、または、その情報の受け渡しを行う 2 個の構成要素が物理的に同じものである場合には、一方の構成要素に対応する処理のフェーズから、他方の構成要素に対応する処理のフェーズに移ることによって行われてもよい。
- [0131] また、上記実施の形態において、各構成要素が実行する処理に関する情報、例えば、各構成要素が受け付けたり、取得したり、選択したり、生成し

たり、送信したり、受信したりした情報や、各構成要素が処理で用いる閾値や数式、アドレス等の情報等は、上記説明で明記していなくても、図示しない記録媒体において、一時的に、または長期にわたって保持されていてもよい。また、その図示しない記録媒体への情報の蓄積を、各構成要素、または、図示しない蓄積部が行ってもよい。また、その図示しない記録媒体からの情報の読み出しを、各構成要素、または、図示しない読み出し部が行ってもよい。

[0132] また、上記実施の形態において、各構成要素等で用いられる情報、例えば、各構成要素が処理で用いる閾値やアドレス、各種の設定値等の情報がユーザによって変更されてもよい場合には、上記説明で明記していなくても、ユーザが適宜、それらの情報を変更できるようにしてもよく、または、そうでなくてもよい。それらの情報をユーザが変更可能な場合には、その変更は、例えば、ユーザからの変更指示を受け付ける図示しない受付部と、その変更指示に応じて情報を変更する図示しない変更部とによって実現されてもよい。その図示しない受付部による変更指示の受け付けは、例えば、入力デバイスからの受け付けでもよく、通信回線を介して送信された情報の受信でもよく、所定の記録媒体から読み出された情報の受け付けでもよい。

[0133] また、上記実施の形態において、被認証装置 1 に含まれる 2 以上の構成要素が通信デバイスや入力デバイス等を有する場合に、2 以上の構成要素が物理的に単一のデバイスを有してもよく、または、別々のデバイスを有してもよい。認証装置 2 についても同様である。

[0134] また、上記実施の形態において、各構成要素は専用のハードウェアにより構成されてもよく、または、ソフトウェアにより実現可能な構成要素については、プログラムを実行することによって実現されてもよい。例えば、ハードディスクや半導体メモリ等の記録媒体に記録されたソフトウェア・プログラムを CPU 等のプログラム実行部が読み出して実行することによって、各構成要素が実現され得る。その実行時に、プログラム実行部は、記憶部や記録媒体にアクセスしながらプログラムを実行してもよい。なお、上記実施の

形態における被認証装置 1 を実現するソフトウェアは、以下のようなプログラムである。つまり、このプログラムは、コンピュータに、ユニーク情報を取得するステップと、ユニーク情報を暗号鍵によって暗号化して暗号情報を生成するステップと、暗号情報を含む認証要求を、認証期間内に繰り返して認証装置に送信するステップと、を実行させ、複数のユニーク情報が暗号化された暗号情報をそれぞれ含む複数の認証要求が、認証期間内に送信される、プログラムである。

[0135] また、上記実施の形態における認証装置 2 を実現するソフトウェアは、以下のようなプログラムである。つまり、このプログラムは、コンピュータに、被認証装置から送信された、暗号鍵によって暗号化された暗号情報を含む認証要求を、認証期間内に繰り返して受信するステップと、暗号情報を復号して復号情報を取得するステップと、復号できた暗号情報を含む、認証期間内に受信された複数の認証要求を用いて、被認証装置が正当かどうかを判断するステップと、被認証装置が正当かどうかを判断するステップにおける判断結果を出力するステップと、を実行させ、正当な被認証装置は、複数のユニーク情報を暗号化した暗号情報をそれぞれ含む複数の認証要求を認証期間内に送信する、プログラムである。

[0136] なお、上記プログラムにおいて、情報を送信する送信ステップや、情報を受信する受信ステップ、情報を出力するステップなどでは、ハードウェアでしか行われない処理、例えば、送信ステップや受信ステップにおけるモデムやインターフェースカードなどで行われる処理は少なくとも含まれない。

[0137] また、このプログラムは、サーバなどからダウンロードされることによって実行されてもよく、所定の記録媒体（例えば、CD-ROMなどの光ディスクや磁気ディスク、半導体メモリなど）に記録されたプログラムが読み出されることによって実行されてもよい。また、このプログラムは、プログラムプロダクトを構成するプログラムとして用いられてもよい。

[0138] また、このプログラムを実行するコンピュータは、単数であってもよく、複数であってもよい。すなわち、集中処理を行ってもよく、または分散処理

を行ってもよい。

[0139] 図10は、上記プログラムを実行して、上記実施の形態による被認証装置1、認証装置2を実現するコンピュータシステム900の一例を示す図である。上記実施の形態は、コンピュータハードウェア及びその上で実行されるコンピュータプログラムによって実現されうる。

[0140] 図10において、コンピュータシステム900は、MPU (Micro Processing Unit) 911と、ブートアッププログラム等のプログラムや、アプリケーションプログラム、システムプログラム、及びデータが記憶されるフラッシュメモリ等のROM912と、MPU911に接続され、アプリケーションプログラムの命令を一時的に記憶すると共に、一時記憶空間を提供するRAM913と、タッチパネル914と、無線通信モジュール915と、MPU911、ROM912等を相互に接続するバス916とを備える。なお、無線通信モジュール915に代えて、有線通信モジュールを備えていてもよい。また、タッチパネル914に代えて、ディスプレイと、マウスやキーボード等の入力デバイスとを備えていてもよい。

[0141] コンピュータシステム900に、上記実施の形態による被認証装置1、認証装置2の機能を実行させるプログラムは、無線通信モジュール915を介してROM912に記憶されてもよい。プログラムは実行の際にRAM913にロードされる。なお、プログラムは、ネットワークから直接、ロードされてもよい。

[0142] プログラムは、コンピュータシステム900に、上記実施の形態による被認証装置1、認証装置2の機能を実行させるオペレーティングシステム(OS)、またはサードパーティプログラム等を必ずしも含んでいなくてもよい。プログラムは、制御された態様で適切な機能やモジュールを呼び出し、所望の結果が得られるようにする命令の部分のみを含んでいてもよい。コンピュータシステム900がどのように動作するのかについては周知であり、詳細な説明は省略する。

[0143] また、本発明は、以上の実施の形態に限定されることなく、種々の変更が

可能であり、それらも本発明の範囲内に包含されるものであることは言うまでもない。

産業上の利用可能性

[0144] 以上のように、本発明による被認証装置、認証装置、認証要求送信方法、認証方法、及びプログラムは、例えば、キャッシュレジスタや自動改札機等における支払いや、チケットの提示等における認証に用いることができる。

請求の範囲

- [請求項1] ユニーク情報を取得する取得部と、
前記ユニーク情報を暗号鍵によって暗号化して暗号情報を生成する暗号化部と、
前記暗号情報を含む認証要求を、認証期間内に繰り返して認証装置に送信する送信部と、を備え、
複数のユニーク情報が暗号化された暗号情報をそれぞれ含む複数の認証要求が、前記認証期間内に送信される、被認証装置。
- [請求項2] 前記ユニーク情報は、乱数値、カウンタ値、時刻のいずれかを含む、請求項1記載の被認証装置。
- [請求項3] 前記暗号鍵は、共通鍵暗号の鍵である、請求項1または請求項2記載の被認証装置。
- [請求項4] 被認証装置から送信された、暗号鍵によって暗号化された暗号情報を含む認証要求を、認証期間内に繰り返して受信する受信部と、
前記暗号情報を復号して復号情報を取得する復号部と、
復号できた暗号情報を含む、前記認証期間内に受信された複数の認証要求を用いて、前記被認証装置が正当かどうかを判断する認証部と、
前記認証部による判断結果を出力する出力部と、を備え、
正当な前記被認証装置は、複数のユニーク情報を暗号化した暗号情報をそれぞれ含む複数の認証要求を前記認証期間内に送信する、認証装置。
- [請求項5] 前記認証部は、複数の復号情報に所定数以上の重複が存在する場合に、前記被認証装置が正当でないと判断する、請求項4記載の認証装置。
- [請求項6] 前記認証部は、認証要求が所定の期間にあらかじめ決められた回数を超えて受信された場合に、前記被認証装置が正当でないと判断する、請求項4または請求項5記載の認証装置。
- [請求項7] 前記認証部は、前記認証期間における認証要求の受信間隔に、確率が

閾値より低い受信間隔が含まれる場合に、前記被認証装置が正当でないと判断する、請求項4から請求項6のいずれか記載の認証装置。

[請求項8] 前記認証部は、前記認証期間に受信された複数の認証要求からそれぞれ取得された複数の復号情報が、前記ユニーク情報と整合しない場合に、前記被認証装置が正当でないと判断する、請求項4から請求項7のいずれか記載の認証装置。

[請求項9] 前記受信部は、間欠的に認証要求を受信する、請求項4から請求項8のいずれか記載の認証装置。

[請求項10] 前記暗号鍵は、共通鍵暗号の鍵である、請求項4から請求項9のいずれか記載の認証装置。

[請求項11] ユニーク情報を取得するステップと、
前記ユニーク情報を暗号鍵によって暗号化して暗号情報を生成するステップと、
前記暗号情報を含む認証要求を、認証期間内に繰り返して認証装置に送信するステップと、を備え、
複数のユニーク情報が暗号化された暗号情報をそれぞれ含む複数の認証要求が、前記認証期間内に送信される、認証要求送信方法。

[請求項12] 被認証装置から送信された、暗号鍵によって暗号化された暗号情報を含む認証要求を、認証期間内に繰り返して受信するステップと、
前記暗号情報を復号して復号情報を取得するステップと、
復号できた暗号情報を含む、前記認証期間内に受信された複数の認証要求を用いて、前記被認証装置が正当かどうかを判断するステップと、
、
前記被認証装置が正当かどうかを判断するステップにおける判断結果を出力するステップと、を備え、
正当な前記被認証装置は、複数のユニーク情報を暗号化した暗号情報をそれぞれ含む複数の認証要求を前記認証期間内に送信する、認証方法。

- [請求項13] コンピュータに、
ユニーク情報を取得するステップと、
前記ユニーク情報を暗号鍵によって暗号化して暗号情報を生成するステップと、
前記暗号情報を含む認証要求を、認証期間内に繰り返して認証装置に送信するステップと、を実行させ、
複数のユニーク情報が暗号化された暗号情報をそれぞれ含む複数の認証要求が、前記認証期間内に送信される、プログラム。
- [請求項14] コンピュータに、
被認証装置から送信された、暗号鍵によって暗号化された暗号情報を含む認証要求を、認証期間内に繰り返して受信するステップと、
前記暗号情報を復号して復号情報を取得するステップと、
復号できた暗号情報を含む、前記認証期間内に受信された複数の認証要求を用いて、前記被認証装置が正当かどうかを判断するステップと、
、
前記被認証装置が正当かどうかを判断するステップにおける判断結果を出力するステップと、を実行させ、
正当な前記被認証装置は、複数のユニーク情報を暗号化した暗号情報をそれぞれ含む複数の認証要求を前記認証期間内に送信する、プログラム。