審決

不服２０２０－　　８１８４

（省略）
請求人　　ローズマウント インコーポレイテッド

（省略）
代理人弁理士　　特許業務法人 津国

特願２０１８－５５１２９７「ＮＦＣ対応無線プロセス通信ゲートウェイ」拒絶査定不服審判事件〔平成２９年１０月　５日国際公開、ＷＯ２０１７／１７２４０３、令和　１年　６月２０日国内公表、特表２０１９－５１７１７２〕について、次のとおり審決する。

結　論

本件審判の請求は、成り立たない。

理　由

第１　手続の経緯

本願は、２０１７年（平成２９年）３月２１日（パリ条約による優先権主張外国庁受理　２０１６年３月３１日　米国）を国際出願日とする出願であって、その手続の経緯は以下のとおりである。

令和　元年　９月２０日付け：拒絶理由通知書
令和　元年１２月１７日　　：意見書、手続補正書の提出
令和　２年　２月　５日付け：拒絶査定
令和　２年　６月１２日　　：拒絶査定不服審判の請求、手続補正書の提出
令和　３年　２月　４日　　：上申書の提出

第２　令和２年６月１２日にされた手続補正についての補正の却下の決定

［補正の却下の決定の結論］

令和２年６月１２日にされた手続補正（以下、「本件補正」という。）を却下する。

［理由］

１　本件補正について（補正の内容）

（１）本件補正後の特許請求の範囲の記載

本件補正により、特許請求の範囲の請求項１の記載は，次のとおり補正された。（下線は，補正箇所である。）
「　フィールドデバイスが無線プロセス通信ネットワークに接続される方法であって、
無線フィールドデバイスが無線ゲートウェイの近距離無線通信（ＮＦＣ）の範囲内に近接されることと、
前記無線ゲートウェイのＮＦＣトランシーバと前記無線フィールドデバイスのＮＦＣタグとの間の通信接続が確立されることと、
自動的に前記無線フィールドデバイスを前記無線プロセス通信ネットワークにアクセスさせることができる接続キーを、自動的に前記無線フィールドデバイスにロードさせるために、前記無線ゲートウェイと前記無線フィールドデバイスとの間に近距離無線通信が生成されることと、
前記無線フィールドデバイスが、前記無線プロセス通信ネットワーク上で通信することを可能にするために、前記接続キーが使用されることと、
を含む方法。」

（２）本件補正前の特許請求の範囲
本件補正前の、令和元年１２月１７日にされた手続補正により補正された特許請求の範囲の請求項１の記載は次のとおりである。
「　フィールドデバイスが無線プロセス通信ネットワークに接続される方法であって、
無線フィールドデバイスが無線ゲートウェイの近距離無線通信（ＮＦＣ）の範囲内に近接されることと、
前記無線ゲートウェイのＮＦＣトランシーバと前記無線フィールドデバイスのＮＦＣタグとの間の通信接続が確立されることと、
前記無線フィールドデバイスを前記無線プロセス通信ネットワークにアクセスさせることができる接続キーを前記無線フィールドデバイスにロードさせるために、前記無線ゲートウェイと前記無線フィールドデバイスとの間に近距離無線通信が生成されることと、
前記無線フィールドデバイスが前記無線プロセス通信ネットワーク上で通信することを可能にするために前記接続キーが無線で使用されることと、
を含む方法。」

２　補正の適否
本件補正は、本件補正前の請求項１に記載された発明を特定するために必要な事項である「前記無線フィールドデバイスを前記無線プロセス通信ネットワークにアクセスさせること」との事項について、「自動的に」との限定を付加し、また、本件補正前の請求項１に記載された発明を特定するために必要な事項である「前記無線フィールドデバイスにロードさせるために、」

との事項について，「自動的に」との限定を付加することを含むものであって、本件補正前の請求項１に記載された発明と本件補正後の請求項１に記載される発明の産業上の利用分野及び解決しようとする課題が同一であるから、特許法１７条の２第５項２号の特許請求の範囲の減縮を目的とするものに該当する。
　そこで、本件補正後の請求項１に記載される発明（以下「本件補正発明」という。）が同条第６項において準用する同法第１２６条第７項の規定に適合するか（特許出願の際独立して特許を受けることができるものであるか）について、以下、検討する。

（１）本件補正発明
　本件補正発明は、上記１（１）に記載したとおりのものである。

（２）引用文献の記載事項
ア　引用文献２
（ア）原査定の拒絶の理由に引用された本願の優先日前に頒布された又は電気通信回線を通じて公衆に利用可能となった文献である、特表２０１１-５０４６８４号公報（以下、「引用文献２」という。）には、図面とともに次の記載がある。（下線は当審で付与した。）
「【００１９】
　図１は、ホストコンピュータ１２、高速ネットワーク１４、無線メッシュネットワーク１６（ゲートウェイ１８および無線フィールドデバイスまたはノード２０ａ～２０ｉを含む）、構成デバイス３０、およびネットワークコンピュータ３２を備える、プロセス制御／監視システム１０を示している。ゲートウェイ１８は、高速ネットワーク１４を介してメッシュネットワーク１６とホストコンピュータ１２とのインターフェースとなる。メッセージは、ネットワーク１４を介してホストコンピュータ１２からゲートウェイ１８に伝送することができ、次いで、複数の異なる経路のうちの１つの経路を経由してメッシュネットワーク１６の選択されたノードに送信される。同様に、メッシュネットワーク１６の個別のノードからのメッセージは、それらがゲートウェイ１８に到達し、次いで、高速ネットワーク１４を介してホスト１２に送信されるまで、複数の経路のうちの１つの経路を介してノードツーノードからメッシュネットワーク１６を通じてルーティングされる。
【００２０】
　加入プロセスを使用して、新しい無線フィールドデバイスをネットワーク１６に追加することができる。一実施形態では、ネットワーク１６内のセキュリティは、対称加入鍵機構に基礎を置いている。デバイスが他のフィールドデバイスによって、またゲートウェイによって受け入れられるように、正しい加入鍵をフィールドデバイス内にロードしなければならない。加入鍵は

、安全にロードされなければならないので、範囲内にある他の無線デバイスは、加入鍵を受信して、場合によっては間違って使用することはできない。加入鍵は、手動でそれぞれの新しいフィールドデバイス内にロードできるが、手動ロードは、誤りを起こしがちであり、人間のオペレータに暗号材料を曝すおそれがある。
【００２１】
　目標は、鍵などの暗号材料を安全な方法で新しいフィールドデバイス内にロードすることである。これは、ゲートウェイ１８と新しいフィールドデバイスと間の安全な無線通信経路（図２Ａおよび２Ｂに関して後で説明されるような）または安全な有線通信経路（図３に関して説明されているような）を通じて実現されうる。両方の場合において、構成デバイス３０は、例えば、ウェブブラウザを含むことができるグラフィカルユーザインターフェース（ＧＵＩ）を備えるネットワークコンピュータ３２とともに、ネットワーク１４に接続される。構成デバイス３０とコンピュータ３２上のＧＵＩとを使用することで、技術者は、ネットワークセキュリティマネージャ（例えば、ゲートウェイ１８またはホストコンピュータ１２上で実行されているアプリケーションプログラムであってもよい）に問い合わせを行い、新しいフィールドデバイスに対する正しい加入鍵（または他の暗号材料）を取得し、加入鍵を新しいフィールドデバイス内に安全にロードすることができる。加入鍵および他の必要な情報がロードされた後、新しいフィールドデバイスをフィールド内にインストールすることができ、そこで、格納されている加入鍵を加入プロセスの一部として使用して、無線ネットワーク１６の一部になることができる。」

（イ）上記記載及び当業者の技術常識を考慮すると、引用文献２には、次の技術事項が記載されているものと認められる。
ａ　上記段落【００１９】には、「図１は、ホストコンピュータ１２、高速ネットワーク１４、無線メッシュネットワーク１６（ゲートウェイ１８および無線フィールドデバイスまたはノード２０ａ～２０ｉを含む）、・・・を備える、プロセス制御／監視システム１０を示している。」との記載がある。
　そうすると、引用文献２には「無線フィールドデバイスを含む無線メッシュネットワークを備える、プロセス制御／監視システム」が記載されているといえる。
ｂ　上記段落【００２０】には、「加入プロセスを使用して、新しい無線フィールドデバイスをネットワーク１６に追加することができる。」、「デバイスが・・・ゲートウェイによって受け入れられるように、正しい加入鍵をフィールドデバイス内にロードしなければならない。」との記載、上記段落【００２１】には、「加入鍵を新しいフィールドデバイス内に安全にロード

することができる。加入鍵および他の必要な情報がロードされた後、新しいフィールドデバイスをフィールド内にインストールすることができ、そこで、格納されている加入鍵を加入プロセスの一部として使用して、無線ネットワーク１６の一部になることができる。」との記載がある。ここで，上記段落【００２１】に記載された「新しいフィールドデバイス」が、段落【００２０】に記載された「新しい無線フィールドデバイス」と同じものを表すことは明らかである。

そうすると、引用文献２には「加入鍵が新しい無線フィールドデバイスにロードされた後、格納されている加入鍵を加入プロセスの一部として使用し、無線フィールドデバイスをゲートウェイが受け入れられることによって、無線メッシュネットワークに追加する」ものが記載されているといえる。

ｃ　そして、上記「ａ」及び「ｂ」に摘記した内容から、引用文献２には「加入鍵を加入プロセスの一部として使用し、新しい無線フィールドデバイスを無線メッシュネットワークに追加する」という方法が記載されているといえる。

そうすると、引用文献２には「無線フィールドデバイスを無線メッシュネットワークに追加する方法」が記載されているといえる。

（ウ）上記（ア）及び（イ）から、引用文献２には，次の発明（以下，「引用発明」という。）が記載されていると認められる。

「　無線フィールドデバイスを無線メッシュネットワークに追加する方法であって、

無線フィールドデバイスを含む無線メッシュネットワークを備える、プロセス制御／監視システムにおいて、

加入鍵が新しい無線フィールドデバイスにロードされた後、格納されている加入鍵を加入プロセスの一部として使用し、無線フィールドデバイスをゲートウェイが受け入れられることによって、無線フィールドデバイスを無線メッシュネットワークに追加する、

方法。」

イ　引用文献１

（ア）同じく原査定の拒絶の理由に引用され、本願の優先日前に頒布された又は電気通信回線を通じて公衆に利用可能となった文献である、国際公開第２０１４／２０５２４３号（以下、「引用文献１」という。）には、図面とともに次の記載がある。（下線は当審で付与した。）

「[0002] Embodiments of the subject matter generally relate to the field of network devices, and, more particularly, to wireless setup between network devices.

[0003] Near field communication (hereinafter ”NFC”) technology is a

set of standards for allowing communication between compatible devic es initiated by bringing the compatible devices into close proximity of each other. NFC may be implemented using radio frequency (herein after RF) technology. NFC may be implemented actively or passively. Active NFC includes hardware that transmits an RF signal using a con nected power source. Passive NFC, on the other hand, does not have a connected power source, instead relying on power generated from a r eceived RF signal.
(中略)
[0042] FIG. 1 depicts an embodiment of a set of NFC-enabled wireless devices capable of utilizing NFC to securely facilitate network con figuration. FIG. 1 depicts the set of NFC- enabled devices, includin g a device 102 with passive NFC capability (hereinafter "client") an d an access point 104 with active NFC capability (hereinafter "AP"). The range within which a passive NFC capable client may trigger the NFC capabilities of the AP 104 is indicated by the dotted line 106. The client 102 and the AP 104 may each be associated with a public-private key pair (not depicted).
[0043] At stage A, the client 102 is moved into the range 106 within which the AP 104 NFC capabilities are triggered. The specific range 106 may vary between implementations. For example, in some implemen tations the range may be a few centimeters, while in some implementa tions the range 106 is small enough that the client 102 physically t ouches the AP 104. The range 106 may be defined by the particular NF C standard implemented or vary due to design considerations. For exa mple, if reducing power consumption is a design goal, the amount of power available to transmit a signal may be limited, thus reducing t he range 106. As a device with active NFC capabilities, the AP 104 g enerates an RF field that, once a passive NFC device is within range , provides power for the passive NFC device. Thus, when a passive NF C device, such as the client 102, enters the RF field generated by t he AP 104, the passive NFC device may communicate with the AP 104.
[0044] At stage B, the AP 104 reads the public key associated with t he client 102 from the client 102. To read data from a passive NFC d evice such as the client 102, the AP 104 encodes a command and trans mits the command using an RF signal. The client 102 receives the RF signal, and utilizing the power generated by the RF signal, decodes the command. Further using the power generated by the RF signal, the client 102 transmits the public key.

[0045] At stage C, the AP 104 writes the public key associated with the AP 104 to the client 102. To write the AP 104 public key to the client 102, the AP 104 encodes a write command, as well as the data to write, and transmits the encoded command and data as an RF signal, or as a set of RF signals, to the client 102. The client 102 utilizes the power generated by the RF signal to decode the command and data, writing the AP 104 public key to memory accessible to the client 102.
[0046] At stage D, the client 102 and AP 104 perform a secure network configuration. The client 102 may be implemented such that the client 102 begins the secure network configuration in response to receiving the AP 104 public key. Thus, the receipt of the AP 104 public key may act as the indication that a secure network configuration set up can begin. In some implementations, another command transmitted by the AP 104 indicates that the secure network configuration can begin. In some implementations, the indication may come from another source, such as from a user interacting with a user interface associated with the client 102 or AP 104.」

（[当審仮訳]：
[0002]本主題の実施形態は、一般にネットワークデバイスの分野に関し、より詳細には、ネットワークデバイス間のワイヤレスセットアップに関する。
[0003]ニアフィールド通信（以下「ＮＦＣ」）技術は、互換デバイスを互いの極近傍にもってくることによって開始される互換デバイス間の通信を可能にするための規格のセットである。ＮＦＣは、無線周波数（以下ＲＦ）技術を使用して実装され得る。ＮＦＣはアクティブにまたはパッシブに実装され得る。アクティブＮＦＣは、接続された電源を使用してＲＦ信号を送信するハードウェアを含む。一方、パッシブＮＦＣは、接続された電源を有さず、代わりに、受信されたＲＦ信号から生成される電力に依拠する。
（中略）
[0042]図１に、ネットワーク構成をセキュアに可能にするためにＮＦＣを利用することが可能なＮＦＣ対応ワイヤレスデバイスのセットの実施形態を示す。図１は、パッシブＮＦＣ能力をもつデバイス１０２（以下「クライアント」）と、アクティブＮＦＣ能力をもつアクセスポイント１０４（以下「ＡＰ」）とを含む、ＮＦＣ対応デバイスのセットを示す。パッシブＮＦＣ対応クライアントがＡＰ１０４のＮＦＣ能力をトリガし得る範囲は点線１０６によって示される。クライアント１０２およびＡＰ１０４はそれぞれ公開秘密鍵ペア（図示せず）に関連し得る。

[0043]段階Ａにおいて、クライアント１０２は、ＡＰ１０４のＮＦＣ能力がトリガされる範囲１０６に移動される。特定の範囲１０６は実装形態間で異なり得る。たとえば、いくつかの実装形態では、範囲は数センチメートルであり得るが、いくつかの実装形態では、範囲１０６は、クライアント１０２がＡＰ１０４に物理的に接触するほど十分に小さい。範囲１０６は、実装される特定のＮＦＣ規格によって定義されるか、または設計要件により異なり得る。たとえば、電力消費を低減することが設計目的である場合、信号を送信するために利用可能な電力量は制限され、したがって範囲１０６は低減し得る。アクティブＮＦＣ能力をもつデバイスとして、ＡＰ１０４は、パッシブＮＦＣデバイスが範囲内にあると、パッシブＮＦＣデバイスのための電力を与える、ＲＦ電界を生成する。したがって、クライアント１０２など、パッシブＮＦＣデバイスが、ＡＰ１０４によって生成されたＲＦ電界に入ると、パッシブＮＦＣデバイスはＡＰ１０４と通信し得る。

[0044]段階Ｂにおいて、ＡＰ１０４は、クライアント１０２から、クライアント１０２に関連する公開鍵を読み取る。クライアント１０２などのパッシブＮＦＣデバイスからデータを読み取るために、ＡＰ１０４は、コマンドを符号化し、ＲＦ信号を使用してコマンドを送信する。クライアント１０２は、ＲＦ信号を受信し、ＲＦ信号によって生成される電力を利用して、コマンドを復号する。さらに、ＲＦ信号によって生成される電力を使用して、クライアント１０２は公開鍵を送信する。

[0045]段階Ｃにおいて、ＡＰ１０４は、ＡＰ１０４に関連する公開鍵をクライアント１０２に書き込む。ＡＰ１０４の公開鍵をクライアント１０２に書き込むために、ＡＰ１０４は、書込みコマンド、ならびに書き込むべきデータを符号化し、符号化されたコマンドおよびデータを、ＲＦ信号として、またはＲＦ信号のセットとして、クライアント１０２に送信する。クライアント１０２は、コマンドおよびデータを復号するためにＲＦ信号によって生成される電力を利用し、ＡＰ１０４の公開鍵を、クライアント１０２にとってアクセス可能なメモリに書き込む。

[0046]段階Ｄにおいて、クライアント１０２およびＡＰ１０４はセキュアネットワーク構成を実行する。クライアント１０２は、ＡＰ１０４の公開鍵を受信したことに応答してクライアント１０２がセキュアネットワーク構成を開始するように実装され得る。したがって、ＡＰ１０４の公開鍵の受信は、セキュアネットワーク構成セットアップが開始することができるという指示として働き得る。いくつかの実装形態では、ＡＰ１０４によって送信される別のコマンドは、セキュアネットワーク構成が開始することができることを示す。いくつかの実装形態では、指示は、クライアント１０２またはＡＰ１０４に関連するユーザインターフェースと対話しているユーザからなど、別のソースから来ることがある。）

（イ）上記記載から、引用文献１には、次の技術事項が記載されているものと認められる。

ａ　上記段落[0042]には、「図１は、パッシブＮＦＣ能力をもつデバイス１０２（以下「クライアント」）と、アクティブＮＦＣ能力をもつアクセスポイント１０４（以下「ＡＰ」）とを含む、ＮＦＣ対応デバイスのセットを示す。」ことが、上記段落[0043]には、「クライアント１０２は、ＡＰ１０４のＮＦＣ能力がトリガされる範囲１０６に移動される。」と記載される一方で、「範囲は数センチメートルであり得るが、いくつかの実装形態では、範囲１０６は、クライアント１０２がＡＰ１０４に物理的に接触するほど十分に小さい。」と記載されていることから、上記「クライアント１０２は、ＡＰ１０４のＮＦＣ能力がトリガされる範囲１０６に移動される。」との記載は，クライアント１０２は、ＡＰ１０４のＮＦＣ能力がトリガされる範囲内に近接されることを表しているといえる。また、上記段落[0043]には、「ＡＰ１０４は、パッシブＮＦＣデバイスが範囲内にあると、パッシブＮＦＣデバイスのための電力を与える、ＲＦ電界を生成する。・・・クライアント１０２など、パッシブＮＦＣデバイスが、ＡＰ１０４によって生成されたＲＦ電界に入ると、パッシブＮＦＣデバイスはＡＰ１０４と通信し得る。」ことが記載されており，通信する際に，クライアントなどのパッシブＮＦＣデバイスはＡＰとの間で通信接続が確立されることは自明である。

　そうすると、引用文献１には「パッシブＮＦＣ能力をもつクライアントがアクティブＮＦＣ能力をもつＡＰの範囲内に近接されるとパッシブＮＦＣ能力をもつクライアントはアクティブＮＦＣ能力をもつＡＰとの間で通信接続が確立される」ことが記載されている。

ｂ　また、上記段落[0045]には、「ＡＰ１０４の公開鍵をクライアント１０２に書き込むために、ＡＰ１０４は、書込みコマンド、ならびに書き込むべきデータを符号化し、符号化されたコマンドおよびデータを、ＲＦ信号として、またはＲＦ信号のセットとして、クライアント１０２に送信する。」と記載され、上記段落[0046]には、「クライアント１０２およびＡＰ１０４はセキュアネットワーク構成を実行する。クライアント１０２は、ＡＰ１０４の公開鍵を受信したことに応答してクライアント１０２がセキュアネットワーク構成を開始するように実装され得る。・・・ＡＰ１０４の公開鍵の受信は、セキュアネットワーク構成セットアップが開始することができるという指示として働き得る。」と記載されている。そして、上記段落[0002]には「本主題の実施形態は、一般にネットワークデバイスの分野に関し、より詳細には、ネットワークデバイス間のワイヤレスセットアップに関する。」とあるから、上記段落[0046]の「セキュアネットワーク構成セットアップ」とはネットワークデバイス間のワイヤレスセットアップ、すなわち、クライアント１０２とＡＰ１０４とのワイヤレスセットアップであることは明らかであり、ワイヤレスセットアップの際は、クライアント１０２がＡＰ１０４にア

クセスすることは技術常識である。
　そうすると、引用文献１には「ＡＰ１０４の公開鍵をＲＦ信号としてクライアントに送信し、ＡＰ１０４の公開鍵の受信に応答してクライアントは、クライアント１０２とＡＰ１０４とのワイヤレスセットアップを開始するために、ＡＰ１０４にアクセスする」ことが記載されている。
ｃ　ここで、パッシブＮＦＣはＮＦＣタグ、アクティブＮＦＣはＮＦＣリーダ／ライターとも呼ばれることは技術常識であり、ＮＦＣリーダ／ライターは、ＮＦＣタグとの間で能動的に送受信を行うものであるからＮＦＣの送受信機、すなわちＮＦＣトランシーバであるともいえ、ＡＰのＮＦＣリーダ／ライターは、クライアントのＮＦＣタグに対し公開鍵の送信を行うのであるから、ＮＦＣタグをもつクライアントはＮＦＣトランシーバをもつＡＰの間で通信接続が確立されており、公開鍵はクライアントにロードされるといえる。
　また、クライアントがＡＰ１０４の公開鍵を受信することに応答してワイヤレスセットアップを開始するために、ＡＰにアクセスするのであるから、前記ＡＰ１０４の公開鍵は自動的にクライアントをＡＰにアクセスさせることができる接続キーであるといえる。
　そして、ＡＰのＮＦＣトランシーバとクライアントのＮＦＣタグとの間は、接続キーの受け渡しをＲＦ信号として行うのであるから、近距離無線通信が生成されることは自明であり、該近距離無線通信の生成は、クライアントのＮＦＣタグとＡＰのトランシーバが近接することによって行われ、公開鍵はクライアントに送信（ロード）されるのであるから、ＡＰのＮＦＣトランシーバとクライアントのＮＦＣタグとの間の近距離無線通信の生成は、自動的にクライアントに公開鍵（接続キー）をロードさせるために生成されるものといえる。
　そうすると、引用文献１には、「ＮＦＣタグをもつクライアントがＮＦＣトランシーバをもつＡＰの範囲内に近接されるとＮＦＣタグをもつクライアントはＮＦＣトランシーバをもつＡＰとの間で通信接続が確立されることと、自動的にクライアントをＡＰにアクセスさせることができる接続キーを、自動的にクライアントにロードさせるために、ＡＰのＮＦＣトランシーバとクライアントのＮＦＣタグとの間に近距離無線通信が生成される」技術が記載されていると認められる。

（３）対比・判断

　本件補正発明と引用発明とを対比すると，以下のことがいえる。

（ア）引用発明の「無線フィールドデバイス」は、本件補正発明の「フィールドデバイス」に含まれ、本件補正発明の「無線フィールドデバイス」に相

当する。また、引用発明の「無線メッシュネットワーク」は「プロセス制御／監視システム」が備えるものであるから、「無線メッシュネットワーク」は、プロセス制御／監視のための通信を行う無線ネットワーク、すなわち、本件補正発明の「無線プロセス通信ネットワーク」に相当する。そして、引用発明の「無線フィールドデバイスを無線メッシュネットワークに追加する」とは、無線フィールドデバイスを無線メッシュネットワークに接続することである。

そうすると、本件補正発明と引用発明は「フィールドデバイスが無線プロセス通信ネットワークに接続される方法」という点で一致する。

（イ）引用発明の「加入鍵」は、「無線フィールドデバイス」を「無線メッシュネットワークに追加する」際に使用されるものである。そして、該加入鍵が使用されることによって、無線フィールドデバイスをゲートウェイが受け入れられるようにするものであるから、引用発明の「加入鍵」は、本件補正発明の「接続キー」に相当する。そして、引用発明の「無線フィールドデバイス」を「無線メッシュネットワークに追加する」ことは、無線フィールドデバイスが無線メッシュネットワーク上で通信することを可能にするために行われることであることは明らかである。

そうすると、本件補正発明と引用発明は「前記無線フィールドデバイスが、前記無線プロセス通信ネットワーク上で通信することを可能にするために、接続キーが使用される」点で一致する。

以上のことから、本件補正発明と引用発明との一致点及び相違点は、次のとおりである。

（一致点）

「　フィールドデバイスが無線プロセス通信ネットワークに接続される方法であって、

前記無線フィールドデバイスが、前記無線プロセス通信ネットワーク上で通信することを可能にするために、接続キーが使用されること、

を含む方法。」

（相違点）

本件補正発明は「無線フィールドデバイスが無線ゲートウェイの近距離無線通信（ＮＦＣ）の範囲内に近接されることと、前記無線ゲートウェイのＮＦＣトランシーバと前記無線フィールドデバイスのＮＦＣタグとの間の通信接続が確立されることと、自動的に前記無線フィールドデバイスを前記無線プロセス通信ネットワークにアクセスさせることができる接続キーを、自動的に前記無線フィールドデバイスにロードさせるために、前記無線ゲートウ

ェイと前記無線フィールドデバイスとの間に近距離無線通信が生成されることと、」との発明特定事項を有するのに対し、引用発明は、当該発明特定事項を有していない点。

以下，上記各相違点について検討する。

上記（２）で説示したとおり、「ＮＦＣタグをもつクライアントがＮＦＣトランシーバをもつＡＰの範囲内に近接されるとＮＦＣタグをもつクライアントはＮＦＣトランシーバをもつＡＰとの間で通信接続が確立されることと、自動的にクライアントをＡＰにアクセスさせることができる接続キーを、自動的にクライアントにロードさせるために、ＡＰのＮＦＣトランシーバとクライアントのＮＦＣタグとの間に近距離無線通信が生成される」ことは公知技術である。

ここで、引用発明の無線フィールドデバイスが無線プロセス通信ネットワーク上で通信するための接続キーを使用するためには、そのための設定を行う必要があることは自明であり、設定作業の少なくとも一部を自動化することは、当業者が当然に追求すべき課題である。
また、引用発明は、加入鍵を使用し、無線フィールドデバイスをゲートウェイが受け入れられることによって、無線フィールドデバイスを無線メッシュネットワークに追加するものである、すなわち無線フィールドデバイスを無線メッシュネットワークにアクセスさせるものであるところ、引用文献１に記載される技術もクライアントをＡＰにアクセスさせること、すなわちクライアントというデバイスをＡＰを介してネットワークにアクセスさせるものであるから、自動的にデバイスをネットワークにアクセスさせる技術である点で共通する。

してみると、引用発明の「加入鍵が新しい無線フィールドデバイスにロードされ」る際、設定作業の少なくとも一部を自動化するために、公知技術である「ＮＦＣタグをもつクライアントがＮＦＣトランシーバをもつＡＰの範囲内に近接されるとＮＦＣタグをもつクライアントはＮＦＣトランシーバをもつＡＰとの間で通信接続が確立されることと、自動的にクライアントをＡＰにアクセスさせることができる接続キーを、自動的にクライアントにロードさせるために、ＡＰのＮＦＣトランシーバとクライアントのＮＦＣタグとの間に近距離無線通信が生成される」という技術事項を適用して、自動的に無線フィールドデバイスを無線メッシュネットワークにアクセスさせることは、当業者であれば容易になし得ることである。

そして、本件補正発明の作用効果も、引用発明及び引用文献１に記載され

た技術に基づいて当業者が予測できる範囲のものにすぎず、格別顕著なものとはいえない。

したがって、本件補正発明は、引用発明及び引用文献１に記載された技術に基づいて当業者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により、特許を受けることができない。

３　結語

したがって、本件補正は、本件補正発明が特許出願の際独立して特許を受けることができないものであるから、特許法第１７条の２第６項において準用する同法第１２６条第７項の規定に違反するので、同法第１５９条第１項において読み替えて準用する同法第５３条第１項の規定により却下すべきものである。

よって、上記補正の却下の決定の結論のとおり決定する。

第３　本願発明について
１　本願発明
令和２年６月１２日にされた手続補正は上記のとおり却下されたので、本願の請求項に係る発明は，令和元年１２月１７日にされた手続補正により補正された特許請求の範囲の請求項１ないし１１に記載された事項により特定されるものであるところ，その請求項１に係る発明は、上記「第２　令和２年６月１２日にされた手続補正についての補正の却下の決定」の項の「１　本件補正について（補正内容）」の項の「（２）本件補正前の特許請求の範囲」のとおりのもの（以下、「本願発明」という。）である。

２　原査定の拒絶の理由
原査定の拒絶の理由は、この出願の請求項１に係る発明は、本願の優先権主張の日前に頒布された又は電気通信回線を通じて公衆に利用可能となった下記の引用文献２に記載された発明及び引用文献１に記載された技術に基づいて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない、という理由を含むものである。

引用文献１：国際公開第２０１４／２０５２４３号
引用文献２：特表２０１１-５０４６８４号公報

３　引用発明等

原査定の拒絶の理由で引用された引用文献１及び２、並びにその記載事項は，上記「第２　令和２年６月１２日にされた手続補正についての補正の却下の決定」の項中の「２　補正の適否」の項中の「（２）引用文献の記載事項」の項に記載したとおりである。

４　対比・判断

本願発明は，本件補正発明から「無線フィールドデバイスの無線プロセス通信ネットワークへのアクセス」及び「接続キーの無線フィールドデバイスへのロード」に係る限定事項を省いたものである。そうすると、本願発明の発明特定事項を全て含み、さらに他の事項を付加したものに相当する本件補正発明が、上記「第２　令和２年６月１２日にされた手続補正についての補正の却下の決定」の項中の「２　補正の適否」の「（３）対比・判断」に記載したとおり、引用発明及び引用文献１に記載された技術に基いて当業者が容易に発明をすることができたものであるから、本願発明も同様の理由により、当業者が容易に発明をすることができたものである。

５　上申の内容について

審判請求人は、令和３年２月４日提出の上申書において、以下のとおりの補正案を作成するとともに、「審尋で引用される前置審査報告書のご指摘を解消するために補正を行う用意があります。これらの補正により独立特許要件を満足することができる請求項があるかどうかご審理いただきたく存じます。そのうえでさらなる補正の機会を賜ることができれば幸甚に存じます。」と述べている。

＜補正案（下線は補正箇所を示す。）＞

「　＜補正後の請求項１＞

フィールドデバイスが無線プロセス通信ネットワークに接続される方法であって、

無線フィールドデバイスが無線ゲートウェイの近距離無線通信（ＮＦＣ）の範囲内に近接されることと、

前記無線ゲートウェイが利用されて、前記無線ゲートウェイのＮＦＣトランシーバと前記無線フィールドデバイスのＮＦＣタグとの間の通信接続が確立されることと、

前記無線ゲートウェイが利用されて、前記ＮＦＣタグから得られた前記無線フィールドデバイスの識別子が前記ネットワーク上に提供されることと、

前記無線ゲートウェイが利用されて、前記無線フィールドデバイスを前記無線プロセス通信ネットワークに自動的にアクセスさせることができる接続キーが検索されることと、

前記無線ゲートウェイが利用されて、前記接続キーを前記無線フィールド

デバイスに自動的にロードさせるために、前記無線ゲートウェイと前記無線フィールドデバイスとの間に近距離無線通信が生成されることと、
前記無線フィールドデバイスが、前記無線プロセス通信ネットワーク上で通信することを可能にするために、前記接続キーが使用されることと、
を含む方法。
＜補正後の請求項５＞
無線プロセス通信ネットワーク上でフィールドデバイスと相互作用するように構成された無線ゲートウェイであって、
前記フィールドデバイスのＮＦＣタグを検出して前記ＮＦＣタグへ接続し、前記ＮＦＣタグから得られた前記無線フィールドデバイスの識別子を前記ネットワーク上に提供するように構成されたＮＦＣトランシーバと、
前記フィールドデバイスの前記ＮＦＣタグの検出に応じて、
自動的にプロセス環境ネットワークから、前記無線プロセス通信ネットワーク上のネットワーク接続キーを検索し、
自動的に前記ＮＦＣトランシーバを用いて、前記検索されたネットワーク接続キーを、前記フィールドデバイスへ提供する、
ように構成された制御装置と、
前記ネットワーク接続キーが利用されて、前記フィールドデバイスを前記無線プロセス通信ネットワーク上で通信させるための無線プロセス通信モジュールと、
を含むゲートウェイ。」
しかしながら、上記第２で説示したとおり本件補正は却下すべきものであり、かつ、上記第３の１ないし４で説示したとおり本願発明は原査定の拒絶の理由に引用された引用文献２及び引用文献１に記載された技術に基いて当業者が容易に発明をすることができたものであるから、補正の機会を再度与える合理的な理由を見出すことはできない。
なお、仮に請求項１の「自動的に」の係り先が明確でないとした場合、特許請求の範囲の請求項１の記載は特許法第３６条第６項第２号の規定に適合しないから、請求項１に係る発明は、独立して特許を受けることができる発明とはならないため、補正却下されるものとなる。そうすると、上記第３の１ないし４で説示したとおり本願発明は原査定の拒絶の理由に引用された引用文献２及び引用文献１に記載された技術に基いて当業者が容易に発明をすることができたものであるから、同じく補正の機会を再度与える合理的な理由を見出すことはできない。

第４　むすび
以上のとおり，本願発明は，引用発明及び引用文献１に記載された技術に基づいて，その出願の優先日前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから，特許法

第２９条第２項の規定により特許を受けることができない。
　したがって，他の請求項に係る発明について検討するまでもなく，本願は拒絶すべきものである。

　よって，結論のとおり審決する。

令和　３年　３月１１日

審判長　　特許庁審判官　廣川 浩
特許庁審判官　本郷 彰
特許庁審判官　國分 直樹

（行政事件訴訟法第４６条に基づく教示）
　この審決に対する訴えは、この審決の謄本の送達があった日から３０日（附加期間がある場合は、その日数を附加します。）以内に、特許庁長官を被告として、提起することができます。

審判長　廣川　浩
　出訴期間として在外者に対し９０日を附加する。

〔審決分類〕Ｐ１８　．５７５-Ｚ　（Ｈ０４Ｗ）
１２１

審判長	特許庁審判官	廣川　浩	9471
	特許庁審判官	國分　直樹	9070
	特許庁審判官	本郷　彰	4225