

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6890504号
(P6890504)

(45) 発行日 令和3年6月18日 (2021.6.18)

(24) 登録日 令和3年5月27日 (2021.5.27)

(51) Int. Cl.

F I

H O 2 J 50/10 (2016.01)

H O 2 J 50/10

H O 2 J 50/80 (2016.01)

H O 2 J 50/80

H O 2 J 7/00 (2006.01)

H O 2 J 7/00 3 O 1 D

請求項の数 37 (全 27 頁)

(21) 出願番号 特願2017-163671 (P2017-163671)
 (22) 出願日 平成29年8月28日 (2017.8.28)
 (65) 公開番号 特開2019-41541 (P2019-41541A)
 (43) 公開日 平成31年3月14日 (2019.3.14)
 審査請求日 令和2年8月25日 (2020.8.25)

早期審査対象出願

(73) 特許権者 000001007
 キヤノン株式会社
 東京都大田区下丸子3丁目30番2号
 (74) 代理人 110003281
 特許業務法人大塚国際特許事務所
 (72) 発明者 七野 隆広
 東京都大田区下丸子3丁目30番2号 キ
 ヤノン株式会社内

審査官 高野 誠治

最終頁に続く

(54) 【発明の名称】 送電装置、受電装置、無線電力伝送システムおよびそれらの制御方法

(57) 【特許請求の範囲】

【請求項 1】

Authenticationが規定されたWPC (Wireless Power Consortium) 規格に対応した受電装置であって、

前記WPC規格におけるDigital Pingを送電装置から受けたことに基づいて、当該受電装置が前記Authenticationに対応していることを示す情報を含む、前記WPC規格におけるConfigurationのパケットを、前記送電装置に送信する送信手段と、

前記送信手段が前記Configurationのパケットを送信した前記送電装置から無線で電力を受電する受電手段と、

前記送電装置と前記Authenticationに関する処理を行う認証手段と、

前記認証手段による前記Authenticationの結果に基づいて、当該受電装置の負荷への出力電力に関して保障される電力値に関する交渉を前記送電装置と行う交渉手段と、を有し、

前記交渉手段は、前記Authenticationに成功した場合は、前記Authenticationに失敗した場合よりも、当該受電装置の負荷への出力電力に関して保障される電力値を大きい値にするように交渉することができることを特徴とする受電装置。

【請求項 2】

前記送信手段が前記Configurationのパケットを前記送電装置に送信した後に、前記認証手段は、前記送電装置と前記Authenticationに関する処理を開始することを特徴とする請求項 1 に記載の受電装置。

10

20

【請求項 3】

前記ConfigurationのパケットのBank2のbit6に、当該受電装置が前記Authenticationに対応していることを示す情報が格納されることを特徴とする請求項 1 又は 2 に記載の受電装置。

【請求項 4】

当該受電装置が前記Authenticationに対応していることを示す情報は「1」であり、当該受電装置が前記Authenticationに対応していないことを示す情報は「0」であることを特徴とする請求項 1 乃至 3 のいずれか 1 項に記載の受電装置。

【請求項 5】

前記Authenticationにおいて、前記送電装置と当該受電装置との間でやりとりされる第 1 のパケットと次の第 2 のパケットの間の第 1 の時間は、当該受電装置の負荷への出力電力に関して保障される電力値に関する交渉において、前記送電装置と当該受電装置との間でやりとりされる第 3 のパケットと次の第 4 のパケットの間の第 2 の時間よりも長いことを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の受電装置。

10

【請求項 6】

前記第 1 のパケット又は前記第 2 のパケットは、前記WPC規格におけるGET_DIGEST、GET_CERTIFICATE、CHALLENGEのいずれかに関するパケットであることを特徴とする請求項 5 に記載の受電装置。

【請求項 7】

前記第 3 のパケット又は前記第 4 のパケットは、前記WPC規格におけるSpecific Requestに関するパケットであることを特徴とする請求項 5 又は 6 に記載の受電装置。

20

【請求項 8】

前記Authenticationは、送電装置と受電装置の間で装置の正当性を確認するための処理であることを特徴とする請求項 1 乃至 7 のいずれか 1 項に記載の受電装置。

【請求項 9】

前記送信手段は、前記WPC規格におけるDigital Pingを送電装置から受けたことに基づいて、当該受電装置の識別情報を含む、前記WPC規格におけるIdentificationのパケットを、前記送電装置に送信することを特徴とする請求項 1 乃至 8 のいずれか 1 項に記載の受電装置。

【請求項 10】

30

前記送電装置から送信された、前記WPC規格におけるPower Transmitter Capabilityのパケットに基づいて、前記送電装置が前記Authenticationに対応しているか否かを判断する判断手段をさらに有することを特徴とする請求項 1 乃至 9 のいずれか 1 項に記載の受電装置。

【請求項 11】

前記Authenticationの要求に対する前記送電装置からの応答に基づいて、前記送電装置が前記Authenticationに対応しているか否かを判断する判断手段をさらに有することを特徴とする請求項 1 乃至 9 のいずれか 1 項に記載の受電装置。

【請求項 12】

前記交渉手段は、前記送電装置が前記Authenticationに対応しているか否かの前記判断手段による判断結果に基づいて、当該受電装置の負荷への出力電力に関して保障される電力値に関する交渉を前記送電装置と行うことを特徴とする請求項 10 又は 11 に記載の受電装置。

40

【請求項 13】

請求項 1 乃至 12 のいずれか 1 項に記載の受電装置の少なくとも前記送信手段、前記認証手段及び前記交渉手段としてコンピュータを機能させるためのプログラム。

【請求項 14】

Authenticationが規定されたWPC (Wireless Power Consortium) 規格に対応した送電装置であって、

受電装置からの要求に基づいて、当該送電装置が前記Authenticationに対応しているこ

50

とを示す情報を含む、前記WPC規格におけるPower Transmitter Capabilityのパケットを前記受電装置に送信する送信手段と、

前記送信手段が前記Power Transmitter Capabilityのパケットを送信した前記受電装置に無線で電力を送電する送電手段と、

前記受電装置と前記Authenticationに関する処理を行う認証手段と、

前記認証手段による前記Authenticationの結果に基づいて、前記受電装置の負荷への出力電力に関して保障される電力値に関する交渉を前記受電装置と行う交渉手段と、を有し、

前記交渉手段は、前記Authenticationに成功した場合は、前記Authenticationに失敗した場合よりも、前記受電装置の負荷への出力電力に関して保障される電力値を大きい値にすることを許容することを特徴とする送電装置。

10

【請求項 1 5】

前記送信手段が前記Power Transmitter Capabilityのパケットを前記受電装置に送信した後に、前記認証手段は、前記受電装置と前記Authenticationに関する処理を開始することを特徴とする請求項 1 4 に記載の送電装置。

【請求項 1 6】

前記Power Transmitter CapabilityのパケットのBank2のbit7からbit2のいずれかに、当該送電装置が前記Authenticationに対応していることを示す情報が格納されることを特徴とする請求項 1 4 又は 1 5 に記載の送電装置。

【請求項 1 7】

20

当該送電装置が前記Authenticationに対応していることを示す情報は「1」であり、当該送電装置が前記Authenticationに対応していないことを示す情報は「0」であることを特徴とする請求項 1 4 乃至 1 6 のいずれか 1 項に記載の送電装置。

【請求項 1 8】

前記Authenticationにおいて、前記受電装置と当該送電装置との間でやりとりされる第1のパケットと次の第2のパケットの間の第1の時間は、前記受電装置の負荷への出力電力に関して保障される電力値に関する交渉において、前記受電装置と当該送電装置との間でやりとりされる第3のパケットと次の第4のパケットの間の第2の時間よりも長いことを特徴とする請求項 1 4 乃至 1 7 のいずれか 1 項に記載の送電装置。

【請求項 1 9】

30

前記Authenticationは、送電装置と受電装置の間で装置の正当性を確認するための処理であることを特徴とする請求項 1 4 乃至 1 8 のいずれか 1 項に記載の送電装置。

【請求項 2 0】

前記受電装置から送信された、前記WPC規格におけるConfigurationのパケットに基づいて、前記受電装置が前記Authenticationに対応しているか否かを判断する判断手段をさらに有することを特徴とする請求項 1 4 乃至 1 9 のいずれか 1 項に記載の送電装置。

【請求項 2 1】

前記交渉手段は、前記受電装置が前記Authenticationに対応しているか否かの前記判断手段による判断結果に基づいて、前記受電装置の負荷への出力電力に関して保障される電力値に関する交渉を前記受電装置と行うことを特徴とする請求項 2 0 に記載の送電装置。

40

【請求項 2 2】

請求項 1 4 乃至 2 1 のいずれか 1 項に記載の送電装置の少なくとも前記送信手段、前記認証手段及び前記交渉手段としてコンピュータを機能させるためのプログラム。

【請求項 2 3】

Authenticationが規定されたWPC (Wireless Power Consortium) 規格に対応した受電装置の制御方法であって、

前記WPC規格におけるDigital Pingを送電装置から受けたことに基づいて、当該受電装置が前記Authenticationに対応していることを示す情報を含む、前記WPC規格におけるConfigurationのパケットを前記送電装置に送信する送信工程と、

前記送信工程で前記Configurationのパケットを送信した前記送電装置から無線で電力

50

を受電する受電工程と、

前記送電装置と前記Authenticationに関する処理を行う認証工程と、

前記認証工程における前記Authenticationの結果に基づいて、当該受電装置の負荷への出力電力に関して保障される電力値に関する交渉を前記送電装置と行う交渉工程と、を有し、

前記交渉工程において、前記Authenticationに成功した場合は、前記Authenticationに失敗した場合よりも、当該受電装置の負荷への出力電力に関して保障される電力値を大きい値にするように交渉することができることを特徴とする受電装置の制御方法。

【請求項 2 4】

前記送信工程で、前記Configurationのパケットを前記送電装置に送信した後に、
前記認証工程で、前記送電装置と前記Authenticationに関する処理を開始することを特徴とする請求項 2 3 に記載の受電装置の制御方法。

10

【請求項 2 5】

前記ConfigurationのパケットのBank2のbit6に、当該受電装置が前記Authenticationに対応していることを示す情報が格納されることを特徴とする請求項 2 3 又は 2 4 に記載の受電装置の制御方法。

【請求項 2 6】

当該受電装置が前記Authenticationに対応していることを示す情報は「1」であり、当該受電装置が前記Authenticationに対応していないことを示す情報は「0」であることを特徴とする請求項 2 3 乃至 2 5 のいずれか 1 項に記載の受電装置の制御方法。

20

【請求項 2 7】

前記Authenticationにおいて、前記送電装置と当該受電装置との間でやりとりされる第 1 のパケットと次の第 2 のパケットの間の第 1 の時間は、当該受電装置の負荷への出力電力に関して保障される電力値に関する交渉において、前記送電装置と当該受電装置との間でやりとりされる第 3 のパケットと次の第 4 のパケットの間の第 2 の時間よりも長いことを特徴とする請求項 2 3 乃至 2 6 のいずれか 1 項に記載の受電装置の制御方法。

【請求項 2 8】

前記第 1 のパケット又は前記第 2 のパケットは、前記WPC規格におけるGET_DIGEST、GET_CERTIFICATE、CHALLENGEのいずれかに関するパケットであることを特徴とする請求項 2 7 に記載の受電装置の制御方法。

30

【請求項 2 9】

前記第 3 のパケット又は前記第 4 のパケットは、前記WPC規格におけるSpecific Requestに関するパケットであることを特徴とする請求項 2 7 又は 2 8 に記載の受電装置の制御方法。

【請求項 3 0】

前記Authenticationは、送電装置と受電装置の間で装置の正当性を確認するための処理であることを特徴とする請求項 2 3 乃至 2 9 のいずれか 1 項に記載の受電装置の制御方法。

【請求項 3 1】

前記送信工程において、前記WPC規格におけるDigital Pingを送電装置から受けたことに基づいて、当該受電装置の識別情報を含む、前記WPC規格におけるIdentificationのパケットを、前記送電装置に送信することを特徴とする請求項 2 3 乃至 3 0 のいずれか 1 項に記載の受電装置の制御方法。

40

【請求項 3 2】

Authenticationが規定されたWPC (Wireless Power Consortium) 規格に対応した送電装置の制御方法であって、

受電装置からの要求に基づいて、当該送電装置が前記Authenticationに対応していることを示す情報を含む、前記WPC規格におけるPower Transmitter Capabilityのパケットを前記受電装置に送信する送信工程と、

前記送信工程で前記Power Transmitter Capabilityのパケットを送信した前記受電装置

50

に無線で電力を送電する送電工程と、

前記受電装置と前記Authenticationに関する処理を行う認証工程と、

前記認証工程における前記Authenticationの結果に基づいて、前記受電装置の負荷への出力電力に関して保障される電力値に関する交渉を前記受電装置と行う交渉工程と、を有し、

前記交渉工程において、前記Authenticationに成功した場合は、前記Authenticationに失敗した場合よりも、前記受電装置の負荷への出力電力に関して保障される電力値を大きい値にすることを許容することを特徴とする送電装置の制御方法。

【請求項 3 3】

前記送信工程で、前記Power Transmitter Capabilityのパケットを前記受電装置に送信した後に、

前記認証工程で、前記受電装置と前記Authenticationに関する処理を開始することを特徴とする請求項 3 2 に記載の送電装置の制御方法。

【請求項 3 4】

前記Power Transmitter CapabilityのパケットのBank2のbit7からbit2のいずれかに、当該送電装置が前記Authenticationに対応していることを示す情報が格納されることを特徴とする請求項 3 2 又は 3 3 に記載の送電装置の制御方法。

【請求項 3 5】

当該送電装置が前記Authenticationに対応していることを示す情報は「1」であり、当該送電装置が前記Authenticationに対応していないことを示す情報は「0」であることを特徴とする請求項 3 2 乃至 3 4 のいずれか 1 項に記載の送電装置の制御方法。

【請求項 3 6】

前記Authenticationにおいて、前記受電装置と当該送電装置との間でやりとりされる第1のパケットと次の第2のパケットの間の第1の時間は、前記受電装置の負荷への出力電力に関して保障される電力値に関する交渉において、前記受電装置と当該送電装置との間でやりとりされる第3のパケットと次の第4のパケットの間の第2の時間よりも長いことを特徴とする請求項 3 2 乃至 3 5 のいずれか 1 項に記載の送電装置の制御方法。

【請求項 3 7】

前記Authenticationは、送電装置と受電装置の間で装置の正当性を確認するための処理であることを特徴とする請求項 3 2 乃至 3 6 のいずれか 1 項に記載の送電装置の制御方法

。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は無線電力伝送システムに関するものである。

【背景技術】

【0002】

近年、無線電力伝送システムの技術開発は広く行われている。特許文献1では、非接触充電規格の標準化団体Wireless Power Consortium (WPC) が策定する規格(WPC規格)に準拠した送電装置および受電装置が開示されている。また、特許文献2には、非接触充電の送電装置および受電装置間の機器認証方法が開示されている。特許文献2によれば、送電装置はチャレンジデータを、送電コイルを介して受電装置に送信し、受電装置はそのチャレンジデータに対して認証用演算を施すことで作成されたレスポンスデータを、受電コイルを介して送電装置に送信する。そして送電装置が受電装置から受信したレスポンスデータを照合することで、機器認証プロトコルを実行する。

【先行技術文献】

【特許文献】

【0003】

【特許文献1】特開2016-007116号公報

【特許文献2】特開2010-104097号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

送電装置において、受電装置に無線で電力伝送を行うための電力を外部の電源（例えばＡＣアダプタ）からケーブル（例えばＵＳＢケーブル）を介して電力を受け取る構成が知られている。このようなＡＣアダプタやケーブルなどの外部の電源装置が正当なものではない場合、送電装置や受電装置に過剰な電力が供給され得る。したがって、ケーブルやＡＣアダプタについても正当性を確認するための機器認証を行い、機器認証により認証された正当性に応じた電力で無線電力伝送が行われることが望まれる。

【0005】

また、例えば、ＷＰＣ規格などの標準規格のバージョンアップでより大電力を送電する場合に、機器の正当性を認証するため新たな機器認証を導入することが考えられる。この場合、新たな機器認証を導入する前の規格に対応する装置とも互換性を保つことが望まれる。そして、例えば、機器認証で正当性が証明された装置間である場合は、より大きな電力で無線電力伝送を行い、古いバージョンで機器認証が実施できない場合であっても、この古いバージョン内で供給可能な電力で無線電力伝送を行うことが望まれる。

【0006】

本発明は上記の課題に鑑みてなされたものであり、機器の正当性の認証を実施可能な無線電力伝送において、その認証の実行可否の判定の結果を有効に利用できるようにすることを目的とする。

【課題を解決するための手段】

【0007】

本発明の一態様による受電装置は、
Authenticationが規定されたWPC（Wireless Power Consortium）規格に対応した受電装置であって、

前記WPC規格におけるDigital Pingを送電装置から受けたことに基づいて、当該受電装置が前記Authenticationに対応していることを示す情報を含む、前記WPC規格におけるConfigurationのパケットを、前記送電装置に送信する送信手段と、

前記送信手段が前記Configurationのパケットを送信した前記送電装置から無線で電力を受電する受電手段と、

前記送電装置と前記Authenticationに関する処理を行う認証手段と、

前記認証手段による前記Authenticationの結果に基づいて、当該受電装置の負荷への出力電力に関して保障される電力値に関する交渉を前記送電装置と行う交渉手段と、を有し、

前記交渉手段は、前記Authenticationに成功した場合は、前記Authenticationに失敗した場合よりも、当該受電装置の負荷への出力電力に関して保障される電力値を大きい値にするように交渉することができる。

【発明の効果】

【0008】

本発明によれば、機器の正当性の認証を実施可能な無線電力伝送において、その認証の実行可否の判定の結果を有効に利用できる。

【図面の簡単な説明】

【0009】

【図1】実施形態による送電装置の構成例を示すブロック図。

【図2】実施形態による受電装置の構成例を示すブロック図。

【図3】実施形態による非接触充電システムの構成例を示すブロック図。

【図4】ＵＳＢ認証とＷＰＴ認証を含む、非接触充電システムの動作シーケンス図。

【図5】送電装置の制御部による、ＧＰの設定処理を示すフローチャート。

【図6】機器認証の結果とＧＰの設定値の関係を示す図。

【図7】送電装置の制御部による電力伝送までの状態遷移を示すフローチャート。

【図 8 A】送電装置と受電装置の間の通信に関するシーケンス図。

【図 8 B】送電装置と受電装置の間の通信に関するシーケンス図。

【図 9 A】受電装置の制御部による電力伝送までの状態遷移を示すフローチャート。

【図 9 B】受電装置の制御部による電力伝送までの状態遷移を示すフローチャート。

【図 9 C】受電装置の制御部による電力伝送までの状態遷移を示すフローチャート。

【図 10】(a) は Configuration Packet の構成を示す図、(b) は Power Transmitter Capability Packet の構成を示す図。

【発明を実施するための形態】

【 0 0 1 0 】

以下、添付の図面を参照して、本発明の実施形態について説明する。以下に記載する実施形態では、送電装置の電源となる A C アダプタやケーブルについても正当性を確認するための機器認証について記載する。また、以下の実施形態では、送電装置の電源となる A C アダプタやケーブルが機器認証に対応していない場合であっても、安全性を担保しつつ無線電力伝送を行う仕組みについて記載する。また、電源との機器認証及び送電装置と受電装置が送電コイルおよび受電コイルを介した機器認証の複数種類の機器認証プロトコルを用いた好適な無線電力伝送に係る制御方法について記載する。

【 0 0 1 1 】

図 3 は、実施形態による無線電力伝送システムとしての非接触充電システムの構成例を示すブロック図である。図 3 において、送電装置 (以下、T X 1 0 0) は、A C アダプタ 3 0 1 から U S B ケーブル 3 0 0 を介して供給される電力を受電装置 (以下、R X 2 0 0) へ、無線により伝送する。R X 2 0 0 は、T X 1 0 0 から無線により伝送された電力を受け取り、例えばバッテリーを充電する。A C アダプタ 3 0 1 は、電源プラグ 3 0 2 を介して供給される商用電源の電力を T X 1 0 0 に適した電圧に変換して、T X 1 0 0 に供給する。

【 0 0 1 2 】

図 1 は、図 3 に示した非接触充電システムに適用可能な送電装置 (T X 1 0 0) の構成例を示すブロック図である。T X 1 0 0 は W P C 規格に準拠しており、さらに W P C 規格 v 1 . 2 . 2 に記載の機能を含む。本実施形態の T X 1 0 0 は同じく W P C 規格に対応した受電装置 (R X 2 0 0) の充電部に最大 1 5 ワットの電力を出力するだけの電力を供給する能力があるものとする。なお、本実施形態では T X 1 0 0 と R X 2 0 0 は W P C 規格に準拠しているものとして説明するが、それに限定されず、他の非接触充電規格であってもよい。

【 0 0 1 3 】

制御部 1 0 1 は、T X 1 0 0 全体を制御する。制御部 1 0 1 の一例は C P U (Central Processing Unit) である。電源部 1 0 2 は USB Power-Delivery 規格に対応しており、さらに接続された U S B 機器同士の機器認証を行う Authentication 規格にも対応している。電源部 1 0 2 は、A C アダプタ 3 0 1 から U S B ケーブル 3 0 0 を介して T X 1 0 0 の動作電源を受け、少なくとも制御部 1 0 1 および送電部 1 0 3 が動作する電源を供給する。送電部 1 0 3 は送電コイル 1 0 5 を介して受電装置 (R X 2 0 0) へ伝送する交流電圧および交流電流を発生させる。具体的には電源部 1 0 2 が供給する直流電圧を、F E T を使用したハーフブリッジもしくはフルブリッジ構成のスイッチング回路で交流電圧に変換する。送電部 1 0 3 は F E T の O N / O F F を制御するゲートドライバを含む。

【 0 0 1 4 】

通信部 1 0 4 は R X 2 0 0 (図 2 の通信部 2 0 4) との間で、W P C 規格に基づいた無線電力伝送の制御通信を行う。本実施形態では通信部 1 0 4 が実行する通信は送電部 1 0 3 が発生する交流電圧または電流を変調し、無線電力に通信を重畳するいわゆるインバンド通信とする。しかし、これに限られるものではなく、送電部 1 0 3 の周波数と異なる周波数を使用するアウトバンド通信でもよい。アウトバンド通信としては、たとえば、N F C、R F I D、Wi-Fi (I E E E 8 0 2 . 1 1 シリーズ)、Bluetooth (登録商標) などがあげられる。表示部 1 0 6 は、T X 1 0 0 自体の状態、もしくは図 3 に示すような T X 1

10

20

30

40

50

00、RX200、USBケーブル300、ACアダプタ301などの機器を含む非接触充電システムの状態を表示し、ユーザに報知する。本実施形態では、表示部106はLEDとして説明するが、これはユーザに上記状態を報知するものであれば他の構成でもよく、スピーカ、振動発生回路、ディスプレイであってもよい。

【0015】

メモリ107は、TX100および非接触充電システム(図3)の各要素および全体の状態を記憶する。第一認証部108は電源部102と、それに接続されるUSBケーブル300およびACアダプタ301について機器認証を行う。第一認証部108は、本実施形態ではUSB Authentication規格に対応しているものとして説明する。しかしこれは機器認証に対応している他の規格でもよく、Qualcomm社のQuick Charge規格でもよいし、それ以外の規格に対応していてもよい。第二認証部109は通信部104を介した通信によってTX100とRX200との間の機器認証を行う。第二認証部109が行う機器認証を本実施形態ではWireless Power Transfer認証(WPT認証)と呼ぶ。

10

【0016】

図1では制御部101、電源部102、送電部103、通信部104、メモリ107、第一認証部108、第二認証部109は別体として記載しているが、これらの内の任意の複数は、同一チップ内に実装されてもよい。例えば、Power-Deliveryに対応した電源部102とUSB Authentication規格に対応した第一認証部108をUSB関連チップとして同一チップ内に実装してもよい。その場合、制御部101とUSB関連チップとの間は、例えばGPIO(General Purpose Input/Output)やシリアル通信で接続するようにしてもよい。

20

【0017】

図2は、本実施形態による受電装置(RX200)の構成例を示すブロック図である。RX200はWPCが策定する規格に準拠しており、WPC規格v1.2.2に記載の機能を含む。

【0018】

RX200において、制御部201は、RX200の全体を制御する。制御部201の一例はCPUである。受電部203は、受電コイル205を介して受電した送電コイル105からの交流電圧および交流電流を制御部201および充電部206などが動作する直流電圧および直流電流に変換する。本実施形態の受電部203は、充電部206に最大15ワットの電力を出力する能力があるものとする。

30

【0019】

通信部204はTX100の通信部104との間で、WPC規格に基づいた非接触充電の制御通信を行う。この制御通信は、受電コイル205で受電した電磁波を負荷変調する、いわゆるインバンド通信である。しかしながら、これに限られるのではなく、送電部103の周波数と異なる周波数を使用するアウトバンド通信でもよい。アウトバンド通信としては、NFC、RFID、Wi-Fi(IEEE802.11シリーズ)、Bluetooth(登録商標)などがあげられる。

【0020】

充電部206は受電部203から供給される直流電圧と直流電流を利用してバッテリー207を充電する。認証部208は通信部204を介した通信によってTX100(第二認証部109)とRX200との間のWPT認証を行う。メモリ209はRX200および非接触充電システム(図3)の各要素および全体の状態を記憶する。なお、TX100またはRX200がWPT認証を含むWPC規格に対応していることを、以下ではWPC規格バージョンAに対応していると表現する。ここでWPC規格バージョンAとはWPCv1.2.2の後継の規格であり、少なくともWPT認証機能が追加されているものとする。

40

【0021】

表示部202は、電力の供給状態、充電状態などを表示する。本実施形態では、表示部202はLEDとして説明するが、これはユーザに上記状態を報知するものであれば他の構成でもよく、例えば、スピーカ、振動発生回路、ディスプレイであってもよい。なお、

50

図 2 では受電部 2 0 3、認証部 2 0 8、制御部 2 0 1、メモリ 2 0 9、通信部 2 0 4、充電部 2 0 6 を別体として記載しているが、これらの内の任意の複数が同一チップ内に実装されてもよい。

【 0 0 2 2 】

以上のような構成を備えた本実施形態の非接触充電システムにおいて、TX 1 0 0 の第一認証部 1 0 8 は、AC アダプタ 3 0 1 および USB ケーブル 3 0 0 と、第一の通信プロトコル（例えば、USB ケーブルを介した USB 認証）を使用して機器認証を行う。また、TX 1 0 0 の第二認証部 1 0 9 は、第一の通信プロトコルが通信に使用する媒体とは異なる媒体（例えば、送電コイル 1 0 5 および受電コイル 2 0 5）を使用する第二の通信プロトコルを使用して RX 2 0 0 と機器認証を行う。

10

【 0 0 2 3 】

図 3 に示される本実施形態の非接触充電システムにおいて、AC アダプタ 3 0 1、USB ケーブル 3 0 0、TX 1 0 0（電源部 1 0 2）は USB 機器である。USB 機器が USB 認証に対応しかつ USB 認証に成功するということは、それらに USB 認証で定められた電力を印加したとしても過度の発熱などのリスクがないことを意味する。つまり、USB 認証に成功した場合、定められた電力を AC アダプタ 3 0 1 から USB ケーブル 3 0 0 を介して TX 1 0 0 の電源部 1 0 2 に供給したとしても、TX 1 0 0 の電源部 1 0 2、USB ケーブル 3 0 0、AC アダプタ 3 0 1 が過度に発熱することはない。

【 0 0 2 4 】

仮に TX 1 0 0 の送電部 1 0 3 に供給される電力の通り道である、TX 1 0 0 の電源部 1 0 2、USB ケーブル 3 0 0、AC アダプタ 3 0 1 のいずれかが USB 認証に非対応である場合は、当然 USB 認証に成功しない。この場合、定められた電力を印加した場合に、USB 認証に非対応であるいずれかが過度に発熱するなどのリスクがある。ここで USB 認証に非対応とは、USB 認証規格が策定される以前の複数のバージョンの USB 規格のいずれかに対応していることを含む。本実施形態では USB 認証規格が策定される以前の複数のバージョンの USB 規格のいずれかに対応した USB 機器をレガシーの USB 機器と呼ぶことにする。

20

【 0 0 2 5 】

また、TX 1 0 0 の電源部 1 0 2、USB ケーブル 3 0 0、AC アダプタ 3 0 1 のいずれかが USB 認証に失敗した場合は、これも USB 認証に成功しない為、上記の定められた電力を印加した場合に、上記のリスクがある。ここで、USB 認証に失敗するとは、USB ケーブル 3 0 0 と AC アダプタ 3 0 1 のいずれかまたは両方が、一見 USB 認証に対応しているように見えるが、実際は USB 認証に対応していないというような悪意のある USB 機器の可能性があるという場合を含む。

30

【 0 0 2 6 】

また、RX 2 0 0 と TX 1 0 0 が WPC 規格バージョン A に対応しており、かつ WPT 認証に成功した場合は、RX 2 0 0 と TX 1 0 0 が所定の電力のやり取りをしたとしても、それらが過度に発熱するなどのリスクがないことを意味する。一方、RX 2 0 0 と TX 1 0 0 のいずれかまたは両方が WPC 規格バージョン A に非対応である場合は、WPT 認証に成功しない。この場合、上記の定められた電力が印加された場合に、WPC 規格バージョン A に非対応である装置が過度に発熱するなどのリスクがある。ここで WPC 規格バージョン A に非対応とは、WPC 規格バージョン A より前の複数のバージョンの WPC 規格のいずれかに対応していることを含む。本実施形態では WPC 規格バージョン A より前の複数のバージョンの WPC 規格のいずれかに対応した TX もしくは RX をレガシーの TX もしくは RX と呼ぶ。

40

【 0 0 2 7 】

また、TX 1 0 0 と RX 2 0 0 が WPT 認証に失敗した場合は、一見 WPT 認証に対応しているように見えるが、実際は対応していないというような悪意のある RX または TX である可能性がある（WPT 認証に対応していれば、認証は必ず成功する為）。この場合も、WPT 認証に成功しない為、上述の定められた電力を印加した場合に、過度の発熱な

50

どの上記したリスクがある。

【 0 0 2 8 】

本実施形態では、U S B ケーブル 3 0 0 および A C アダプタ 3 0 1 が U S B 認証に成功し、かつ R X 2 0 0 および T X 1 0 0 が W P T 認証に成功した場合に、安全に所定の電力を供給することが可能であると判断される。すなわち、R X 2 0 0 の受電部 2 0 3 が負荷（本実施形態では充電部 2 0 6）に所定の電力（15ワット）を供給したとしても、過度の発熱などのリスクがない。他方、T X 1 0 0（電源部 1 0 2）、U S B ケーブル 3 0 0、A C アダプタ 3 0 1 のいずれかが U S B 認証に成功しない、または R X 2 0 0 と T X 1 0 0 のいずれかが W P T 認証に成功しない場合は、安全に所定の電力を供給できない可能性がある。すなわち、R X 2 0 0 の受電部 2 0 3 が負荷に 15ワットの所定の電力を供給した場合に、過度の発熱などのリスクがある。以下では、そのようなリスクを回避するために、認証に成功しない場合に、受電部 2 0 3 が供給する電力を所定の電力（例えば 15ワット）より小さい電力（例えば 5ワット以下）に制限するものとする。

10

【 0 0 2 9 】

従来、上述のように U S B 認証と W P T 認証など複数の機器認証プロトコルが存在するシステムにおいて、これら複数の認証を考慮した制御方法については何等提案されていない。

【 0 0 3 0 】

図 4 は本実施形態による U S B 認証と W P T 認証を含むシーケンス図である。図 5 は本実施形態における Guaranteed Power（以下、G P）の設定に関する送電装置（T X 1 0 0）の制御部 1 0 1 の動作を示すフローチャートである。G P とは、T X 1 0 0 と R X 2 0 0 の位置関係がずれて、送電コイル 1 0 5 と受電コイル 2 0 5 の間の送電効率が低下しても、受電部 2 0 3 の負荷への出力電力に関して保障される電力値を意味する。受電部 2 0 3 の負荷とは、受電部 2 0 3 が電源を供給する対象であり、少なくとも充電部 2 0 6 を含む。例えば、G P が 5ワットの場合、送受電コイルの位置関係がずれて、コイル間の送電効率が低下したとしても、受電部 2 0 3 が 5ワットを出力することができるよう、T X 1 0 0 は送電部 1 0 3 を制御する。図 4、図 5 に示される動作（G P の決定動作）については、図 6 の説明の後で述べる。

20

【 0 0 3 1 】

図 6 は U S B 認証および W P T 認証の結果によって、後述する Negotiation において用いられる G P の制限値の例を示す図である。

30

【 0 0 3 2 】

列 6 0 0 の「U S B 認証非対応」とは、T X 1 0 0 の電源部 1 0 2、U S B ケーブル 3 0 0、A C アダプタ 3 0 1 の少なくともいずれかが U S B 認証に対応していない（ただし、U S B 認証に対応している機器は認証に成功している）こと示す。列 6 0 1 の「U S B 認証失敗」とは、T X 1 0 0 の電源部 1 0 2、U S B ケーブル 3 0 0、A C アダプタ 3 0 1 のいずれかが、U S B 認証に対応しているが U S B 認証に失敗したことを示す。列 6 0 2 の「U S B 認証成功」とは T X 1 0 0 の電源部 1 0 2、U S B ケーブル 3 0 0、A C アダプタ 3 0 1 のすべてが U S B 認証に成功したことを示す。また、行 6 0 3 は R X 2 0 0 が W P T 認証に対応していないことを、行 6 0 4 は R X 2 0 0 が W P T 認証に対応しているが W P T 認証に失敗したことを、行 6 0 5 は R X 2 0 0 が W P T 認証に対応しており W P T 認証に成功したことを示す。なお、テーブル中の「0, 2.5, 5」の 3 種類の G P の電圧値が記載されている欄については、予めそれらのうちの 1 つを採用するように決定しておく。

40

【 0 0 3 3 】

図 6 によれば U S B 認証に非対応（列 6 0 0）である場合は、W P T 認証の結果によらず、G P を 5ワットに制限することで、過度の発熱などのリスクを回避しつつ、送電を行うことができる。また、列 6 0 0 のうち、W P T 認証に失敗した場合（行 6 0 4）は、0ワット（送電しない）、2.5ワットなど（5ワットより小）、W P T 認証に非対応の場合（行 6 0 3）と比較して小さい値に制限してもよい。なぜかという、W P T 認証に失

50

敗したということはW P T 認証を実装してはいるが正確には実装していない悪意のある R X (例えばW P C 規格をみたしていない偽物)の可能性があるからである。過度の発熱などの上記リスクの観点では、G P を5ワットに制限すればよいが、W P T 認証非対応であるが正確に規格を実装しているレガシーの R X よりも低いG P (0ワットまたは2.5ワット)に制限することは、偽物を排除できるというメリットがある。

【0034】

同様に、U S B 認証に失敗した場合(列601)は、W P T 認証の結果にかかわらず0ワット(送電しない)、2.5ワットなど(5ワットより小)U S B 認証に非対応の場合(列600)と比較して小さい値に制限してもよい。U S B 認証に失敗したということはU S B 認証を実装してはいるが正確には実装していない悪意のあるU S B 機器の可能性が

10

【0035】

また、U S B 認証に成功した場合(列602)は、図3のシステムでU S B に関連するT X 100の電源部102、U S B ケーブル300、A C アダプタ301に関して、R X 200が負荷へ15ワットを供給したとしても上記リスクがないことを意味する。よってT X 100はW P C 認証の結果に基づいてG P の設定を行う。W P T 認証非対応の場合(行603)は前述の理由によりG P は5ワットとし、W P T 認証に失敗した場合(行604)はより低いG P (0ワットまたは2.5ワット)に制限される。U S B 認証に成功し

20

【0036】

<非接触充電システム起動から送電までのシーケンス>

図3の非接触充電システムの起動から送電までのシーケンスについて、図4および図5を使用して説明する。T X 100はU S B 認証およびW P T 認証において、認証の対象となる機器のうち認証に非対応もしくは認証に失敗した機器が1つでもあれば送電電力を制

30

【0037】

T X 100の電源部102にU S B ケーブル300とA C アダプタ301が接続されると(400)、T X 100の制御部101はU S B 認証を行う(401、S501)。U S B 認証において、制御部101は、第一認証部108を動作させ、認証対象であるすべてのU S B 機器(実施形態ではU S B ケーブル300とA C アダプタ301の両方)がU S B 認証に対応しているかを判断する。第一認証部108は、すべてのU S B 機器についてU S B 認証を実行し、実行したすべてのU S B 認証に成功した場合に、「U S B 認証成功」と判定する。また、本実施形態では、すべてのU S B 認証に成功しなかった場合の認証結果として「U S B 認証非対応」と「U S B 認証失敗」を設けている。U S B 認証に

40

【0038】

例えば、A C アダプタ301のU S B 認証に成功したが、U S B ケーブル300がU S B 認証に対応していない場合、「U S B 認証非対応」と判定される。また、例えば、A C アダプタ301のU S B 認証に成功し、U S B ケーブル300はU S B 認証に対応しているものの認証に失敗した場合、「U S B 認証失敗」と判定される。また、例えば、A C アダプタ301とU S B ケーブル300の両方がU S B 認証に成功した場合、「U S B 認証成功」と判定される。制御部101は、このようなU S B 認証結果をメモリ107に保持

50

しておく(S 5 0 2)。

【 0 0 3 9 】

次に、制御部 1 0 1 は USB PD (USB-Power Delivery 規格) のシーケンスに基づいて A C アダプタ 3 0 1 との間で A C アダプタ 3 0 1 から供給される電圧および電流に関する電源仕様を決定する (4 0 2)。電源電圧は T X 1 0 0 の内部構成により決まっているので、この場合は電流値に関して決定する。図 3 のシステムにおける電源部 1 0 2 の電圧は 1 5 V であるとし、電源部 1 0 2 の出力電流は最大 3 A であるとする。ここで、T X 1 0 0 の制御部 1 0 1 は電流値を下げるにあたって、図 6 に示されるように判断する。例えば、U S B 認証非対応の場合、図 6 の列 6 0 0 に基づいて、W P C 規格の Negotiation フェーズ (後述) による交渉における G P の最大値は 5 ワットと決定される。

10

【 0 0 4 0 】

そして、制御部 1 0 1 は T X 1 0 0 内部のロスを考慮して電流値を決定する。たとえば送受電コイルの位置が変化し、コイル間効率が一番低くなった時に G P である 5 ワットを R X 2 0 0 が出力したときのシステム効率を 5 0 % であるとする。この場合、電源部 1 0 2 が送電部 1 0 3 や制御部 1 0 1 に供給する電力は 1 0 ワット (5 W × 2) である。電源電圧が 1 5 V なので、出力電流は 0 . 6 7 A である。本実施形態では、U S B 機器が U S B 認証に非対応であった場合、リスクを回避する為には G P を 5 ワットに制限すればよいとした。ゆえに、電源部 1 0 2 が USB PD のシーケンスに基づいて A C アダプタ 3 0 1 と交渉して決定すべき電流値は 0 . 6 7 A 程度であればよい。この決定すべき電流値に基づいて、T X 1 0 0 の制御部 1 0 1 は A C アダプタ 3 0 1 との間で電源仕様を決定する。他方、U S B 認証に成功した場合は、1 5 ワットの G P 値に対応できるように、電源仕様を 2 . 0 A (1 5 W × 2 / 1 5 V) に決定する。

20

【 0 0 4 1 】

T X 1 0 0 の制御部 1 0 1 は送電部 1 0 3 を起動する (4 0 3)。送電部 1 0 3 を起動することとは、電源部 1 0 2 から制御部 1 0 1 と送電部 1 0 3 と通信部 1 0 4 の少なくともいずれかに電源を投入するいわゆるパワーオンリセットでもよい。または第一認証部 1 0 8 が T X 1 0 0 の制御部 1 0 1 と送電部 1 0 3 と通信部 1 0 4 の少なくともいずれかに図示しないリセット信号 (L O : 約 0 V) を入力することで制御部 1 0 1 と送電部 1 0 3 と通信部 1 0 4 の少なくともいずれかにリセットをかけてもよい。この場合、電源仕様が決まり、G P の値が決定したのちに、第一認証部 1 0 8 は、リセット信号を H I (例えば 3 . 3 V) にすることで、リセットを解除する。

30

【 0 0 4 2 】

送電部 1 0 3 が起動すると、T X 1 0 0 は W P C 規格に準拠した動作を開始する。本実施形態では、W P C 規格に準拠したフェーズに加え、W P T 認証を行うフェーズとして Authentication フェーズを定義する。Authentication フェーズでは T X と R X は W P T 認証に基づいた機器認証を実施する。T X および R X の両方が Authentication フェーズに対応している場合、T X と R X は、Selection フェーズ、Ping フェーズ、Identification & Configuration フェーズ (I & C フェーズ)、Authentication フェーズ、Negotiation フェーズ、Calibration フェーズ、Power Transfer フェーズ (P T フェーズ) の順に遷移する。

【 0 0 4 3 】

40

具体的には、まず Selection フェーズにおいて、送電部 1 0 3 は送電コイル 1 0 5 を介して Analog Ping を送電する (4 0 5)。Analog Ping とは送電コイル 1 0 5 の近傍に存在する物体を検出する為の微小な電力の信号である。T X 1 0 0 は Analog Ping を送電した時の送電コイルの電圧値または電流値を検出し、電圧がある閾値を下回るもしくは電流値がある閾値を超える場合に物体が存在すると判断し、Ping フェーズに遷移する。

【 0 0 4 4 】

Ping フェーズでは T X 1 0 0 は Analog Ping より大きい Digital Ping を送電する。Digital Ping の大きさは、送電コイル 1 0 5 の近傍に存在する R X 2 0 0 の制御部 2 0 1 が起動するのに十分な電力である。R X 2 0 0 の制御部 2 0 1 は、受電コイル 2 0 5 を介して受電した Digital Ping により起動すると、受電電圧の大きさを T X 1 0 0 へ通知し (4 0

50

7)、I & C フェーズへ遷移する。TX 100 は受電電圧値の通知を受けると、I & C フェーズに遷移する。続いてRX 200 はID PacketおよびConfiguration PacketをTX 100へ送信する(408、409)。

【0045】

続いて、第二認証部109はAuthenticationフェーズでWPT認証処理を実施する(410、S503)。認証対象は、無線電力伝送システムにおける受電装置としてのRX 200である。制御部101は、このWPT認証の結果をメモリ107に保持する(S504)。そして、制御部101は、S502でメモリ107に保持したUSB認証の結果とS504でメモリ107に保持したWPT認証の結果と図6に基づいてNegotiationフェーズで用いるGPの最大値を決定する(404、S505)。Authenticationフェーズの詳細は、図8(e)により後述する。

10

【0046】

その後、TX 100の制御部101はNegotiationフェーズでRX 200との交渉によりGPを決定する(411)。ここでは、送電電力が、第一認証部108(USB認証)と第二認証部109(WPT認証)による機器認証の結果に基づいて制限されたGP値(404)、すなわち許容される送電電力以下となるように交渉が行われる。例えば、USB認証の結果が「USB認証成功」かつWPT認証の結果が「WPT認証成功」の場合は、図6に示されるようにGPの設定が15ワットまで許容される。一方、USB認証の結果が「USB認証非対応」であれば、GPは5ワットまたはそれ未満に制限される。この場合、Negotiationフェーズにおいて、RX 200の制御部201から5ワットを超えるGPを要求された場合は、TX 100の制御部101は当該要求に対してNAKを送信する。他方、制限値以下のGPが要求されれば、制御部101はアクノリッジ(ACK)を送信する。

20

【0047】

以上のように、TX 100の制御部101はUSB認証およびWPT認証の両方の結果に基づいてGPを設定するので、複数の認証のうちいずれかの認証が失敗した際はGPの大きさが制限され、過度の発熱などのリスクを回避することができる。また、全ての認証が成功した場合のみ、送電部103の能力の最大値をGPに設定することができる。

【0048】

続いてTX 100の制御部101はGPを制限した理由をRX 200の制御部201へ通知する理由通知を送信する(412)。理由通知により、第一認証部108および第二認証部109による機器認証の結果が受電装置であるRX 200に通知される。この理由通知は、後述のRESULTパケット(図8Bの(e)の820)であってもよい。本実施形態では、TX 100の制御部101は、RESULTパケットに、WPT認証の結果と、TX 100の電源部102に関するUSB認証の結果を格納してRX 200の制御部201に送信する。例えば、制御部101は、RESULTパケットの中にWPT認証結果を格納する1ビットを設け、WPT認証が成功すれば「1」を、そうでなければ「0」を格納する。また、制御部101は、RESULTパケットにACアダプタ301およびUSBケーブル300とのUSB認証結果を格納する1ビットを設け、全てのUSB認証が成功すれば「1」を、そうでなければ「0」を格納する。制御部101は、こうして機器認証の結果が格納されたRESULTパケットを送信する。

30

40

【0049】

その後、TX 100の制御部101およびRX 200の制御部201はCalibrationフェーズの処理を実行し(413)、PTフェーズへ遷移する。PTフェーズにおいて、RX 200は負荷へ電力を供給する(414)。RX 200の制御部201は、理由通知(412)に基づいて表示部202に電力が制限されていることを表示してもよい(416)。同様にTX 100の制御部101は、機器認証の結果(理由通知)に基づいて表示部106に電力が制限されていることを表示してもよい(415)。例えば、前記RESULTパケットのUSB認証結果ないしWPT認証結果を示すビットにもとづいて、「USB認証に成功しない為(USB機器が原因で)、低速充電中です」という表示をしてもよい。このような表

50

示により、ユーザは、充電に、電力が制限されない場合よりも長い時間がかかることを知ることができる。前記表示はWPT認証の結果について言及してもよく、同様の効果があることは明らかである。また、当該表示は電力が制限されない場合異なるLEDの色もしくは点灯パターンで表示してもよい。また、電力が制限されない場合と異なる音や振動でユーザに報知するようにしても同様の効果を得ることができる。

【0050】

また、本実施形態ではUSB認証において送電電力を制限するか否かを判断した後に、WPCの送電装置を起動するようにした。しかしこれは、USBとWPCを同時に起動してUSB認証とWPC認証を非同期に実施し、WPCが送電を開始した後に、USB認証による送電電力の制限が判明した場合、WPCの送電電力を再度Negotiationにより制限しても同様の効果を与えることができる。しかし、本実施形態のようにUSB認証において送電電力を制限するか否かを判断した後に、WPCの送電装置を起動するようにすれば、さらなる効果を期待できる。TX100がNegotiationフェーズ(411)でGPを決定する時には、すでにUSB認証において送電電力を制限するか否かが決定している為、前記再度Negotiationする処理が発生しない効果がある。

【0051】

<WPT認証の動作と後方互換性>

WPC規格でより大きな電力を送電するようになり、前記リスクを回避する為にレガシーのWPC規格にWPT認証機能を追加する必要がある。ここでWPT認証機能を有したTXは同じくWPT認証機能を有するRXのみならず、レガシーのRXとも後方互換性を確保しなければならない。同様にWPT認証機能を有したRXはレガシーのTXとも後方互換性を確保しなければならない。しかしながら、レガシーのWPC規格に準拠しながらWPT認証機能を加え後方互換も考慮した技術は提案されていないという課題がある。

【0052】

そこで、以下では、無線電力伝送の標準規格に新たな機器認証を追加した場合に、新たな機器認証を有さないバージョンの標準規格と互換性を保つ形態を説明する。

【0053】

図7は本実施形態のTX100の制御部101の動作を示すフローチャートである。図8A～8Bは、バージョンAのTX100あるいはRX200による後方互換性を説明するシーケンス図である。本実施形態のWPT認証は、USB認証と同様に電子証明書を用いたチャレンジ・レスポンス型の機器認証として説明するが、WPT認証はこれに限定されない。TX100がRX200に対してチャレンジテキストを送信するイニシエータとして動作し、RX200はチャレンジテキストを暗号化してTX100に送信するレスポンドとして動作する。図9A～9CはRX200の制御部201の動作を示すフローチャートである。図10(a)はWPC規格によるConfiguration Packetのビット構成例を示す図である。図10(b)はWPC規格によるPower Transmitter Capability Packetのビット構成例を示す図である。なお図中の同一の構成に関しては、同一の符号を付与している。

【0054】

シーケンス図およびフローチャートの説明に先立って、WPC規格v1.2.2に基づいたTXおよびRXのカテゴリについて説明する。GPが5ワットであるTXおよびRXはBasic Power Profile(BPP)にカテゴリ化される。また、GPが5ワットより大きく15ワット以下であるTXおよびRXはExtended Power Profile(EPF)にカテゴリ化される。さらにWPC規格v1.2.2ではGPに関してTXとRX間で交渉(Negotiation)する機能が追加されている。EPFにカテゴリ化されたTXおよびRXはNegotiation機能を有する。BPPにカテゴリ化されたTXおよびRXは、Negotiation機能に対応したものとそうでないものにさらにカテゴリ化される。RXがNegotiation機能を有するかどうかは、TXがRXの設定情報が記載されているConfiguration Packet(図10(a))のNeg bit(Bank4, bit7)によって判断できる。Neg bitが「1」であればN

egotiation機能を有しており、「0」であればそれを有していない。本実施形態では、特に指定がない限り、レガシーのTXおよびRXはNegotiation機能を有しており、NegotiationはNegotiationフェーズで実施されるものとして説明する。

【0055】

WPT認証に対応したWPC規格バージョンAのTXおよびRXは、WPC規格v1.2.2に対応したレガシーのRXおよびTXとそれぞれ後方互換をとらなければならない。つまり、WPC規格バージョンAに対応したTXは、バージョンAより前のWPC規格に対応したRXに対しても矛盾なく動作する必要がある。同様にバージョンAに対応したRXはバージョンAより前のWPC規格に対応したTXに対しても矛盾なく動作する必要がある。

10

【0056】

そこで、図7、図8A～8B、図9A～9Cを参照して本実施形態に示すバージョンAに対応したTX100およびRX200がWPC規格v1.2.2との後方互換があることについて説明する。WPC規格v1.2.2のレガシーのEPPに対応したTXおよびRXは、Selectionフェーズ、Pingフェーズ、I&Cフェーズ、Negotiationフェーズ、Calibrationフェーズ、PTフェーズの順で状態遷移する。また、レガシーのTXおよびRXのうち少なくとも片方がNegotiation機能を有しないBPPの機器である場合は、TXおよびRXは、Selectionフェーズ、Pingフェーズ、I&Cフェーズ、PTフェーズの順で状態遷移する。

【0057】

20

上述のように、TXおよびRXの両方がAuthenticationフェーズに対応している場合、TXとRXは、Selectionフェーズ、Pingフェーズ、I&Cフェーズ、Authenticationフェーズ、Negotiationフェーズ、Calibrationフェーズ、PTフェーズの順に遷移する。ここで、AuthenticationフェーズはNegotiationフェーズに先立って実施されるべきである。その理由は次のとおりである。図6においてWPT認証の結果によってGPの値が変わることを説明した。仮にNegotiationフェーズにおいてTXとRXが交渉によりGPを決定した後でAuthenticationフェーズに遷移した場合を考える。この場合、Authenticationフェーズの結果によって上記リスクを回避するために、既に決定したGPが再度変更される可能性がある。このようなGPの再変更には、PTフェーズに遷移するまでの手順が煩雑になる、より時間がかかるなどの課題がある。Negotiationフェーズに先立ってAuthenticationフェーズを実施することにより、AuthenticationフェーズでGPに関する制限をかけ、制限されたGPを前提にNegotiationフェーズでGPを決定することができる。このように、Negotiationフェーズに先立ってAuthenticationフェーズでGPに制限をかけることにより、PTフェーズに遷移するまでのGPの再変更が発生せず、速やかにPTフェーズに遷移することができる。

30

【0058】

<TX100、RX200ともにレガシーの場合>

まず、TX100、RX200ともにレガシーのEPPに対応している場合のWPC規格v1.2.2におけるシーケンスである図8Aの(a)について説明する。なお、以降の説明では、TX100によるUSBケーブル300およびACアダプタ301とのUSB認証は成功したものとする。図7、図9AのフローチャートについてはレガシーのEPPに関する部分のみが用いられる。すなわち、レガシーのTXでは図7のS703～S708の処理は存在せず、レガシーのRXでは図9AのS903～S905、S908の処理が存在しない。なお、図8Aの(a)では後方互換に関係するI&Cフェーズ以降のシーケンスのみを示している。

40

【0059】

TX100とRX200との間でSelectionフェーズとPingフェーズの処理が行われた後、I&Cフェーズへ遷移する(S701)。I&CフェーズにおいてRX200はTX100に対してIdentification Packet(ID Packet)を送信する(800、S901)。ID packetには、自身の個体識別情報のほかに、対応しているWPC規格のバージョン(

50

この場合 v 1.2.2) がわかる情報要素が格納される。つづいて R X 2 0 0 は Configuration Packet を T X 1 0 0 へ送信する (8 0 1、S 9 0 1)。W P C 規格 v 1.2.2 の Configuration Packet は R X 2 0 0 が負荷に供給できる最大電力の具体的な値である Maximum Power Value、Negotiation 機能を有するか否かを示すビットである Neg bit を含む。ここで、R X 2 0 0 は Neg bit を「1」に設定し、Negotiation 機能を有することを示す。

【 0 0 6 0 】

T X 1 0 0 は R X 2 0 0 から ID Packet および Configuration Packet を受信すると (S 7 0 2)、R X 2 0 0 が Negotiation 機能を有するかを判断する (S 7 0 4)。R X 2 0 0 は Negotiation 機能を有するので (S 7 0 4 で Y E S)、T X 1 0 0 は Configuration Packet に対して ACK を送信し (S 7 1 3、8 0 2)、Negotiation フェーズに遷移する (S 7 0 9)。なお、R X 2 0 0 が Negotiation に対応していない B P P (Neg bit が 0) の場合は、T X 1 0 0 は ACK を送信せずに P T フェーズに遷移する (S 7 1 2)。また、T X 1 0 0 自身が B P P でありかつ Negotiation に対応していない場合も同様に、T X 1 0 0 は ACK を送信せずに P T フェーズに遷移する。この場合、G P は 5 ワットに制限される。

【 0 0 6 1 】

R X 2 0 0 は ACK を受信すると (S 9 0 2 で Y E S)、T X 1 0 0 が Negotiation 機能に対応していることがわかり、Negotiation フェーズへ遷移する (S 9 0 6)。そして、R X 2 0 0 は、自身が必要な電力 (例えば 15 ワット) を要求する Specific Request パケットを送信する。この場合、R X 2 0 0 は Specific Request パケットの情報要素として、G P として 15 ワットを要求することを示す Specific Request (15W) を T X 1 0 0 に送信する (8 0 3)。ここで、W P C 規格 v 1.2.2 の R X 2 0 0 は Configuration Packet 送信後、15 m s 以内に ACK を受信しなければ (S 9 0 2 で N O)、T X 1 0 0 が Negotiation 機能を有しない B P P であると判断する (S 9 0 9)。そして、R X 2 0 0 は P T フェーズへ遷移する (S 9 1 0)。

【 0 0 6 2 】

T X 1 0 0 は Specific Request (15 W) を受信すると、自身の送電能力と 15 ワットを比較し、送電可能であれば肯定を意味する ACK を、そうでなければ要求を拒否することを示す NAK を R X 2 0 0 に送信する。ここでは、15 ワットを送電可能と判断して、G P を 15 ワットと決定し (S 7 1 0)、ACK を送信する (8 0 4)。そして T X 1 0 0 は Calibration フェーズに遷移する。R X 2 0 0 は Specific Request (8 0 3) に対して T X 1 0 0 から ACK を受信すると Calibration フェーズへ遷移する (S 9 0 7)。Calibration フェーズでは、T X 1 0 0 が R X 2 0 0 に送電した電力について T X 1 0 0 の内部で測定した値と、R X 2 0 0 の内部で測定した受電電力の値との相関に基づいて T X 1 0 0 が調整を行う。Calibration フェーズが終了すると、T X 1 0 0 と R X 2 0 0 は P T フェーズへ遷移し、無線電力伝送を開始する (S 7 1 2、S 9 1 0)。

【 0 0 6 3 】

以上のように、W P C 規格 v 1.2.2 の T X 1 0 0 は、Neg bit によって R X 2 0 0 が Negotiation 機能を有する E P P ないし B P P か、もしくは Negotiation 機能を有しない B P P かを判断する。そして、前者の場合は Negotiation フェーズへ遷移し、後者の場合は P T フェーズへ遷移する。

【 0 0 6 4 】

また、W P C 規格 v 1.2.2 の R X 2 0 0 は、Configuration Packet 送信から 15 m s 以内に ACK を受信するかを判断基準として、ACK を受信すれば Negotiation フェーズに遷移し、そうでなければ P T フェーズへ遷移する。

【 0 0 6 5 】

以上の動作により、W P C 規格 v 1.2.2 では Negotiation 機能を持つ T X 1 0 0 および R X 2 0 0 とそうでない T X 1 0 0 および R X 2 0 0 の互換性が確保されている。

【 0 0 6 6 】

< T X 1 0 0 がバージョン A、R X 2 0 0 がレガシーの場合 >

T X 1 0 0 がバージョン A に対応し、R X 2 0 0 がレガシーの場合について、図 8 A の

10

20

30

40

50

(b)、図6、図7、図9Aを用いて説明する。なお、以降の説明では、TX100によるUSBケーブル300およびACアダプタ301とのUSB認証は成功したものとする。なお、以降のすべての説明はWPC規格の後方互換に関する説明の為、TX100が第一認証部を持たない構成であっても適応可能なことは明らかである。

【0067】

まず、Configuration Packet内のAuth bitについて定義する。図10(a)にWPC規格v1.2.2のConfiguration Packetの構成を示す。なお、本発明と関連がない部分の説明は省略する。Configuration Packetには複数のReserved領域がある。例えば、Bank2のbit4からbit6のReserved領域1001、Bank1のbit0からbit7のReserved領域1000、Bank4のbit2からbit0のReserved領域1002である。本実施形態では、Auth bitをBank2のbit6に配置する。但し、Auth bitの配置はこれに限られるものではなく、他のReserved領域に配置してもよい。なお、WPC規格v1.2.2ではReserved領域のビットはいずれも0である。RX200は自身がWPT認証に対応していればAuth bitに「1」を、そうでない場合は「0」を格納する。

【0068】

TX100はConfiguration PacketのAuth bitにより、RX200がWPT認証に対応しているかを判断する(S703)。RX200はレガシーであるためAuth bitは「0」である。TX100は、RX200がWPT認証に対応していないと判断し(S703でNO)、Negotiationフェーズに移移する。ここで、RX200からGPとして15ワットの要求を受信した場合、要求を拒否する旨を示すNAKをRX200に送信する(805)。

【0069】

RX200はNAKにより要求が拒否されたので、TX100が設定可能なGPの値を知ることが目的に、WPC規格v1.2.2に定義されたGeneral Requestを送信する。ここでGeneral Requestのうち、Transmitter Capability Packetを要求するメッセージを、本実施形態ではGeneral Request(capability)と表す。Transmitter Capability Packetとは、設定可能なGPの値を含み、WPC規格v1.2.2で定義されたパケットである。

【0070】

TX100はGeneral Request(capability)を受信すると(806)、既に説明した図6に基づいて、WPT認証非対応(行603)でUSB認証成功(列602)に該当する5ワットをGPとすると決定する。そして、TX100は、Power Transmitter Capability PacketのGuaranteed Power Valueに5ワットを示す情報を格納して、これをRX200に送信する(807)。

【0071】

以上のように、本実施形態で定義したAuth bitによって、WPC規格バージョンAに対応したTX100は、バージョンAより前のWPC規格に対応したレガシーRXに対して矛盾なく動作する。

【0072】

<TX100、RX200ともにバージョンAの場合>

次に、TX100とRX200がともにWPT認証処理に対応している場合について、図6、図7、図8Bの(e)、図9Aを使って説明する。なお、以降の説明では、TX100によるUSBケーブル300およびACアダプタ301とのUSB認証は成功したものとする。説明に先立ってWPT認証に対応したバージョンAのTX100とRX200の動作について説明する。

【0073】

バージョンAのRX200はAuth Bitに「1」を格納したConfiguration PacketをTX100に送信する。バージョンAのTX100はConfiguration PacketのAuth Bitによって、RX200がWPT認証に対応していると判断すると(S703でYES)、ACK(auth)をRX200に送信する(S705、802)。ACK(auth)は、ACKとは区別可能なア

10

20

30

40

50

クノリッジであり、ACKとは異なるビットパターンで構成され、Configuration Packetに対するアクノリッジと、TX 1 0 0がWPT認証に対応していることを示すパケットである。

【0074】

こうして、TX 1 0 0はRX 2 0 0がWPT認証に対応していることがわかると、ACK(auth)を送信してAuthenticationフェーズへ遷移する(S 7 0 6)。一方、RX 2 0 0はACK(auth)を受信すると(S 9 0 3でYES)、TX 1 0 0がWPT認証に対応していると判断し(S 9 0 4)、Authenticationフェーズへ遷移する(S 9 0 5)。

【0075】

図8Bの(e)の814から820は、本実施形態のWPT認証の例である。まずTX 1 0 0はGET_DIGESTメッセージをRX 2 0 0に送信する(814、S 7 0 7)。GET_DIGEST Packetは、RX 2 0 0が持つ電子証明書に関する情報を要求するPacketである。RX 2 0 0はGET_DIGEST Packetに応答してDIGESTを送信する(815)。DIGESTとはRX 2 0 0が所有する電子証明書に関する情報である。TX 1 0 0は続いて、電子証明書に関する詳細な情報を要求するGET_CERTIFICATE PacketをRX 2 0 0に送信する(816)。RX 2 0 0はGET_CERTIFICATE Packetに応答してCERTIFICATEを送信する(817)。

【0076】

次に、TX 1 0 0はチャレンジテキストを含むCHALLENGEメッセージをRXに送信し(818)、RX 2 0 0はチャレンジテキストを暗号化したRESPONSEをTX 1 0 0に送信する(819)。TX 1 0 0はRESPONSEの正当性が確認されれば、RESULT(success)をRXに送信し(820、S 7 0 8)、Negotiationフェーズに遷移する(S 7 0 9)。RESULT(success)パケットは、RESPONSEの結果、WPT認証が成功したことを意味する。RX 2 0 0はRESULT(success)を受信すると、Negotiationフェーズに遷移する(S 9 0 6)。

【0077】

Negotiationフェーズでは、既に説明した図6に基づいて、TX 1 0 0は、WPT認証成功(行605)でUSB認証成功(列602)に該当する15ワットをGPとすると決定し、Negotiationを行う。TX 1 0 0は、GPとして15ワットをRX 2 0 0から要求され(803)、自身は図6を参照して交渉の際のGPの値は15ワットとした。従って、要求を認めるACKをRX 2 0 0に送信する(804)。また、TX 1 0 0はRESPONSEの結果、認証に失敗すると、失敗したことを示すRESULT(fail)をRESULT(success)に代えてRX 2 0 0に送信する。そして図6に基づいて、後続するNegotiationフェーズにおいてGPの値を決定する。もしくは、TX 1 0 0は、RESULT(fail)を送信した後、送電部103を停止してもよい。

【0078】

以上のように、本実施形態のTX 1 0 0はバージョンAより前のWPC規格に対応したRXに対してだけでなく、バージョンAに対応したRXに対しても矛盾なく動作する。

【0079】

ここで、GET_DIGESTS(814)からRESULT(success)(820)までのパケット間の時間間隔について補足する。RX 2 0 0のパケットに対するTX 1 0 0の応答について、例えばWPC規格v1.2.2のNegotiationフェーズでは、RX 2 0 0のパケットの後端からTX 1 0 0の応答パケットの先端まで10ms以内と規定されている。しかしAuthenticationフェーズのイニシエータ(TX 1 0 0)はRX 2 0 0が送信する電子証明書に関連するパケット(DIGEST、CERTIFICATE、RESPONSE)の正当性を確認する為に暗号化・複合化の処理が必要である。その為、Authenticationフェーズでは応答に時間がかかる。そこでAuthenticationフェーズでは、他のフェーズにおける応答時間(Response time)と比較して長い応答時間を設ける。本実施形態では、この応答時間を50msとする。つまり、図8Bの(e)において、応答時間はDIGESTからGET_CERTIFICATE、CERTIFICATEからCHALLENGE、RESPONSEからRESULT(success)までの時間である。応答時間を長くすることで、TX 1 0 0の制御部101が高速に動作する必要性が低下し、制御部101の消費電力の低減や低速なCPUの使用により低コスト化を実現できるという効果がある。

【 0 0 8 0 】

なお、TX 1 0 0はConfiguration PacketのAuth bitによって受電装置がW P T 認証対応かどうか判断したが、これはID Packetのバージョン情報で判断してもよい。バージョン情報がバージョン A (かそれ以降のバージョン) であればW P T 認証に対応していると判断し、バージョン情報がバージョン A より前であればW P T 認証に非対応と判断しても同様の効果を得られる。

【 0 0 8 1 】

< TX がレガシー、RX がバージョン A の場合 1 >

TX 1 0 0 がレガシーであり、RX 2 0 0 がバージョン A に対応している場合について、図 8 A の (c)、図 6、図 9 A を用いて説明する。なお、以降の説明では、TX 1 0 0 によるUSBケーブル3 0 0およびACアダプタ3 0 1とのUSB認証は成功したものとする。まず、バージョン A に対応したRX 2 0 0の動作について説明する。

10

【 0 0 8 2 】

RX 2 0 0はConfiguration Packetで自身がW P T 認証に対応していることをTX 1 0 0に通知する(8 0 0、8 0 1)。しかしTX 1 0 0はレガシーであるため、Auth bitを無視する。そして、TX 1 0 0は、RX 2 0 0がNegotiation機能に対応しているのでACKを送信して、自身はNegotiationフェーズへ遷移する(S 7 0 4でYES、S 7 1 3、S 7 0 9)。

【 0 0 8 3 】

RX 2 0 0はACKを受信すると(8 0 2、S 9 0 2でYES)、TX 1 0 0がW P T 認証に非対応であり、レガシーのTXであると判断する(S 9 0 8)。なぜなら、自身がW P T 認証に対応しているため、TX 1 0 0がW P T 認証対応であれば、ACK(auth)を受信するからである。なお、RX 2 0 0がConfiguration Packet送信から1 5 m s以内にACKを受信せず(S 9 0 2でNO)、かつACK(auth)も受信しない場合は(S 9 0 3でNO)、処理はS 9 0 9へ進む。この場合、RX 2 0 0は、TX 1 0 0がB P PでありかつNegotiation機能に対応してないと判断し(S 9 0 9)、P Tフェーズへ遷移する(S 9 1 0)。

20

【 0 0 8 4 】

RX 2 0 0はNegotiationフェーズにおいてGPの交渉を行うが、図 6 で説明したように、RX 2 0 0は上記のリスクを回避するために1 5 ワットを受信するべきでないと判断する。そして、RX 2 0 0はW P T 認証非対応(行 6 0 3)でUSB認証成功(列 6 0 2)に該当する5ワットをGPとして交渉すると判断し、Specific Request(5 W)を送信する(8 0 9)。そして、RX 2 0 0はTX 1 0 0からACKを受信し(8 1 0)、Negotiationフェーズを終了する。そして、RX 2 0 0はCalibrationフェーズへ遷移し(S 9 0 7)、所定の処理を実行した後、P Tフェーズへ遷移する(S 9 1 0)。

30

【 0 0 8 5 】

以上のように、W P C 規格バージョン A に対応したRX 2 0 0は、バージョン A より前のW P C 規格に対応したTX 1 0 0に対しても矛盾なく動作することができる。さらに、図 8 B の (e) で説明したように、RX 2 0 0はTX 1 0 0がW P T 認証に対応している場合でも矛盾なく動作できる。

40

【 0 0 8 6 】

< TX がレガシー、RX がバージョン A の場合 2 >

上記では、RX 2 0 0 がバージョン A に対応している場合に、Configuration Packetに対するTX 1 0 0からの応答に基づいてTX 1 0 0がW P T 認証に対応しているか否か、Negotiation機能に対応しているか否かを判断した。より具体的には、Configuration Packetの送信から1 5 m s以内に、ACKまたはACK(auth)のどちらを受信したのか、または、いずれも受信していないのか、によって上記判断をする例について説明した。ここでは、TX 1 0 0 がバージョン A に対応しているか否かの判断を行う別の例について、図 8 B の (d)、図 9 C を使用して説明する。なお、以降の説明では、TX 1 0 0 によるUSBケーブル3 0 0およびACアダプタ3 0 1とのUSB認証は成功したものとする。

50

【 0 0 8 7 】

R X 2 0 0 は、Configuration Packetに対してACKを受信すると、W P T 認証の実行を要求するためにAuth Reqを送信する (S 9 1 2、8 1 0)。Auth Reqは、Authentication フェーズへ遷移することを T X 1 0 0 に要求する認証要求のパケットであり、W P C 規格 v 1 . 2 . 2 でパケットタイプが規定されていないReserved Packetである。本実施形態では、Reserved Packetの内、パケットヘッダが 0 x 4 0 のパケットをAuth Reqパケットとして定義する。バージョン A に対応した T X は、Configuration Packetに対してACKを返した後、Auth Reqパケットの受信に応じてAuthenticationフェーズへ遷移し、W P T 認証を開始する。

【 0 0 8 8 】

一方、バージョン A に非対応の T X では次のように動作する。W P C 規格 v 1 . 2 . 2 ではNegotiationフェーズにおいて、T X 1 0 0 は、パケットタイプを見て、自身が対応していないPacketを受信すると、Not-Defined Response (ND Resp) パケットを送信するように規定されている。但し、I & C フェーズでは、T X 1 0 0 は、対応していないPacketを受信しても何も応答しないように規定されている。T X 1 0 0 はConfiguration Packetに対するACK (8 0 2) を送信している為、Negotiationフェーズになっている。よってレガシーである T X 1 0 0 はAuth Reqのパケットに回答してND Respを R X 2 0 0 へ送信する (8 1 1)。R X 2 0 0 はND Respを受信すると (S 9 1 3 で Y E S)、T X 1 0 0 が W P T 認証非対応であると判断し (S 9 0 8)、W P T 認証は行わず、Negotiationフェーズへ遷移する (S 9 0 6)。

【 0 0 8 9 】

ここで、R X 2 0 0 がAuth Reqに対して、ND Respを受信せず (S 9 1 3 で N O)、ACKを受信した場合 (S 9 1 4 で Y E S)、処理は S 9 0 4 へ進む。この場合、R X 2 0 0 は T X 1 0 0 が W P T 認証対応であると判断し (S 9 0 4)、Authenticationフェーズへ遷移する (S 9 0 5)。なお、Auth Reqに対して、R X 2 0 0 がND RespもACKも受信しない場合は (S 9 1 4 で N O) R X 2 0 0 は T X 1 0 0 に対して送電の停止を要求し、Selectionフェーズに戻る (S 9 1 5)。送電の停止の要求は、たとえばEnd of Transmission Packet (E T P) を送信することにより行われる。T X 1 0 0 に対して送電の停止を要求することにより、T X 1 0 0 の故障や T X 1 0 0 と R X 2 0 0 との間の通信品質の劣化によってW P C シーケンスを継続できない場合に、システムを元の状態に戻せるという効果がある。

【 0 0 9 0 】

また、R X 2 0 0 がND RespもACKも受信しない場合に、R X 2 0 0 はAuth Reqを再送するしてもよい。これは、T X 1 0 0 がAuth Reqを正しく受信できなかった可能性があるからである。そして、W P C 規格 v 1 . 2 . 2 では、T X 1 0 0 がNegotiationフェーズにおいてパケットを正しく受信できない場合は、T X 1 0 0 はNegotiationフェーズにとどまることが規定されている。よってAuth Reqを再送することで、T X 1 0 0 が正しくパケットを受信し、ACKもしくはND Respを受信でき、シーケンスを継続できる可能性があるからである。そして、Auth Reqが数回 (3 回など) 連続してACKもND Respも受信しない場合に E P T を送信するようにしてもよい。

【 0 0 9 1 】

以上のように、T X 1 0 0 が自身が対応できないパケットに対して応答 (ND Resp) を返す状態であるNegotiationフェーズの時に、R X 2 0 0 は T X 1 0 0 が W P T 認証に対応するか否かがわかるパケットを送信するようにした。故に R X 2 0 0 はAuth Reqに対する応答によって T X 1 0 0 が W P T 認証対応か否かを判断し、W P T 認証非対応の T X に対して矛盾なく動作することができる。

【 0 0 9 2 】

また、Auth Reqはレガシーの T X 1 0 0 からの応答 (ND Resp) が期待されるパケットであればよい。したがって、W P C 規格 v 1 . 2 . 2 で規定されている、応答が期待されるパケットのうち、Packet typeがまだ定義されていないReserved Packetでもよい。応答が

期待されるパケットとしては、例えばGeneral Request Packet、Specific Request Packetがある。具体的には、Specific Request PacketのRequestフィールドがReserved (0x05から0xEF)であるパケットでもよい。この場合は、TX 1 0 0がWPT認証非対応であればTX 1 0 0はND Respを送信し、RX 2 0 0はこれを受信する。また、General Request PacketのRequestフィールドがReservedであるパケットでもよい。この場合は、TX 1 0 0がWPT認証非対応であれば、ND Respと同様に、TX 1 0 0はRequestに 응답して対応できない旨を示す、Power Transmitter Data Not Available Packetを送信し、RX 2 0 0はこれを受信する。

【0093】

また、Auth Reqを送信する前に、WPT認証対応かどうかを知るためのパケットをやり取りするようにしてもよい。例えば、RX 2 0 0は、General Request PacketでTX 1 0 0の個体識別情報や規格バージョンが格納されるPower Transmitter Identification Packetを要求してもよい。その場合、RX 2 0 0は、Auth Reqに先立って、General Request PacketによりTX 1 0 0の規格バージョンを取得する。RX 2 0 0は、取得したバージョンがバージョンA以降であればTX 1 0 0がWPT認証対応であると判断してAuth Reqを送信し、そうでなければTX 1 0 0はWPT認証に非対応であると判断することが可能である。

【0094】

また、Power Transmitter Identification Packetの要求は、同じGeneral Request PacketでTX 1 0 0の能力情報が格納されるPower Transmitter Capability Packetを要求してもよい。Power Transmitter Capability Packetは、送電装置であるTX 1 0 0が送電能力を通知するためのパケットであり、これにWPT認証を実行可能である旨の情報を含ませることができる。その場合、WPC規格v 1.2.2のPower Transmitter Capability Packet (図10(b))でReservedとなっているBank1のbit7かbit6、もしくはBank2のbit7からbit2のいずれかのビットをAuth bitとしてバージョンAで定義する。Auth bitには、「1(WPT認証対応)」か「0(WPT認証非対応)」が書き込まれる。バージョンAに対応したTX 1 0 0は、Power Transmitter Capability PacketのAuth bitに「1(WPT認証対応)」を書き込む。

【0095】

また、RX 2 0 0はReserved Packetに対する応答を受信する為に、TX 1 0 0がNegotiationフェーズにいるときに、Reserved Packetを送信するようにした。これにより、応答がND-RespであるかACKであるかによりTX 1 0 0がレガシーなのか、WPT認証に対応しているのかを判断することが可能となる。同一のパケットをI & Cフェーズで送信したとしても、WPC規格v 1.2.2ではReserved Packetに対してTX 1 0 0が応答しない為、上記の判断ができない。

【0096】

<TXがレガシー、RXがバージョンAの場合3>

TX 1 0 0がWPT認証に対応しているか否かをACK(auth)もしくはAuth Reqに対する応答によってRX 2 0 0が判断する例について説明した。以下では、他の例について図9Bを使用して説明する。なお、以降の説明では、TX 1 0 0によるUSBケーブル300およびACアダプタ301とのUSB認証は成功したものとする。RX 2 0 0は、Configuration Packetに対するACKを受信しNegotiationフェーズに移行してから、一定時間の間にAuthenticationフェーズにおいてTX 1 0 0が送信する特定のパケットを受信したか否かを判断する。上記一定時間以内に特定のパケットを受信した場合、RX 2 0 0はTX 1 0 0がWPT認証に対応していると判断し、受信しなかった場合、TX 1 0 0がWPT認証に対応していないと判断する。

【0097】

説明に先立ち、WPT認証に対応したTX 1 0 0の動作について説明する。TX 1 0 0はConfiguration PacketによってRX 2 0 0がWPT認証に対応していると判断したら、Authenticationフェーズに遷移する。すなわち、TX 1 0 0は、Configuration Packetに

10

20

30

40

50

対するACKの後端から一定時間以内にGET_DIGESTパケットの先頭をRX200に対して送信する。

【0098】

TX100がレガシーの場合は、RX200は一定時間以内にGET_DIGESTパケットの先頭を受信しないので(S911でNO)、TX100がWPT認証非対応であると判断し(S908)、Negotiationフェーズに遷移する。このように、RX200はレガシーのTX100に対して矛盾なく動作する。また、TX100がWPT認証に対応していた場合、RX200は一定時間以内にGET_DIGESTパケットの少なくとも先頭を受信する(S911でYES)。よって、RX200はTX100がWPT認証対応であると判断し(S904)、Authenticationフェーズに遷移する(S905)。

10

【0099】

ここで、上述の一定時間を本実施形態では6msとする。WPC規格v1.2.2ではRX200はACKを受信した後の6msの間はいかなるパケットの先頭も送信してはならないと規定されている。よって、TX100が少なくとも6ms以内にGET_DIGESTパケットの先頭を送信すれば、RX200がNegotiationフェーズで送信しうるパケット(例えば、Specific Requestなど)を送信する前に、RX200をAuthenticationフェーズに遷移させることができる。

【0100】

以上のように本実施形態のRX200は、TX100がレガシーである場合およびWPT認証に対応している場合に矛盾なく動作することができる。

20

【0101】

<RXがWPT認証のイニシエータになる場合>

図8Bの(e)はTX100がイニシエータになる例について説明したが、これに限られるものではなく、RX200がイニシエータであってもよい。その場合、RX200はACK(auth)を受信すると、TX100がWPT認証に対応していると判断するので、Authenticationフェーズに遷移する。そしてRX200はTX100に対してGET_DIGESTパケットをTX100に送信する。GET_DIGESTパケットの送信およびこれ以降の認証処理は(814から820まで)、図8Bの(e)に示されるパケットの矢印の向きを逆にしたものとなる。RX200はRESULT(success)を送信するとNegotiationフェーズに遷移する。同様にTX100はRESULT(success)を受信するとNegotiationフェーズに遷移する。以上

30

【0102】

また、Authenticationフェーズにおいて、TX100が所定のパケット以外のパケットをRX200から受信した場合は、送電部103の送電を停止し、Selectionフェーズに遷移してもよい。所定のパケットとは、814から820のパケットであり、GET_DIGEST、DIGEST、GET-CERTICARTE、CERTIFICATE、CHALLENGE、RESPONSE、RESULTである。Authenticationフェーズにおいて、受電した電圧の電圧値を示すSignal Strength Packet、電圧値の増減を要求するControl Error Packet、ID Packet、Configuration Packetなどを受信したら、TX100は送電を停止し、Selectionフェーズに戻る。このようにTX100は、Authenticationフェーズにおいて、RX200の故障などにより所定のパケット以外

40

のパケットを受信した場合に送電を停止することでシステムが予期せぬ動作をすることを防止することができる。

【0103】

以上のように本実施形態の非接触充電システムでは、電力供給源である電源装置(ACアダプタ301)と送電装置との間でUSBプロトコルを用いた機器認証が行われ、送電装置と受電装置との間でWPCプロトコルを用いた機器認証が行われる。そして、USBの機器認証結果とWPCの機器認証結果とに基づいて、WPCの送電装置が送電電力を制御するようにした。この構成により電源供給の経路に存在する機器の過度の発熱のリスクのない好適な送電装置の制御を実現できる。

【0104】

50

また、W P C の送電装置が受電装置に送電を開始するのに先立って、U S B の認証結果に基づいてW P C の送電装置の送電電力を制限するようにした。この構成により、W P C による送電開始後に、U S B 認証の結果に基づく送電電力の制限による送電電力の再交渉などが発生せず、高速な制御が実現できる。

【 0 1 0 5 】

< その他の実施形態 >

本発明に係る無線電力伝送システムの電力伝送方式は特に限定はしない。T X の共振器（共鳴素子）と、R X の共振器（共鳴素子）との間の磁場の共鳴（共振）による結合によって電力を伝送する磁界共鳴方式でもよい。また電磁誘導方式、電界共鳴方式、マイクロ波方式、レ - ザ - 等を利用した電力伝送方式を用いてもよい。

10

【 0 1 0 6 】

また、本発明は上述の実施形態の 1 以上の機能を実現するプログラムを、ネットワーク又は記憶媒体を介してシステム又は装置に供給し、そのシステム又は装置のコンピュータにおける 1 つ以上のプロセッサ - がプログラムを読み出し実行する処理でも実現可能である。また、1 以上の機能を実現する回路（例えば、A S I C）によっても実現可能である。

【 0 1 0 7 】

また、T X および R X は例えば、撮像装置（カメラやビデオカメラ等）やスキャナ等の画像入力装置であってもよいし、プリンタやコピー機、プロジェクタ等の画像出力装置であってもよい。また、ハードディスク装置やメモリ装置などの記憶装置であってもよいし、パーソナルコンピュータ（P C）やスマートフォンなどの情報処理装置であってもよい。

20

【 0 1 0 8 】

また、図 5、図 7、図 9 A ~ 9 C に示すフローチャ - トは、制御部に電源が投入された場合に開始される。なお、図 5、図 7 に示される処理は T X 1 0 0 のメモリ 1 0 7 に記憶されたプログラムを制御部 1 0 1 が実行することで実現される。また、図 9 A ~ 9 C に示すフローチャ - トは、R X 2 0 0 のメモリ 2 0 9 に記憶されたプログラムを制御部 2 0 1 が実行することで実現される。

【 0 1 0 9 】

なお、図 5、図 7、図 9 A ~ 9 C のフローチャ - トで示される処理の少なくとも一部がハードウェアにより実現されてもよい。ハードウェアにより実現する場合、例えば、所定のコンパイラを用いることで、各ステップを実現するためのプログラムから F P G A 上に自動的に専用回路を生成すればよい。F P G A とは、Field Programmable Gate Array の略である。また、F P G A と同様にして Gate Array 回路を形成し、ハードウェアとして実現するようにしてもよい。

30

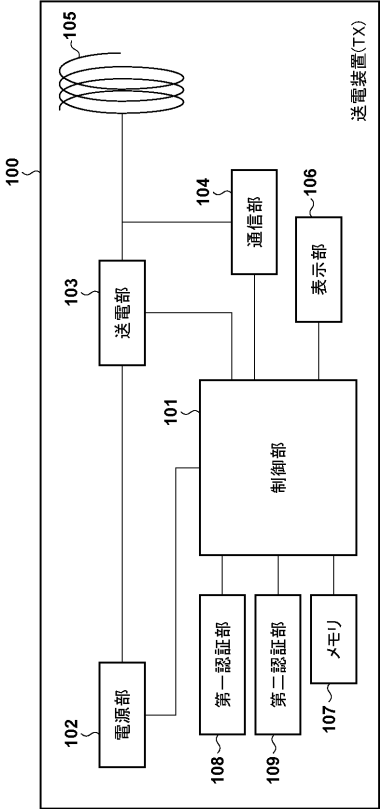
【 符号の説明 】

【 0 1 1 0 】

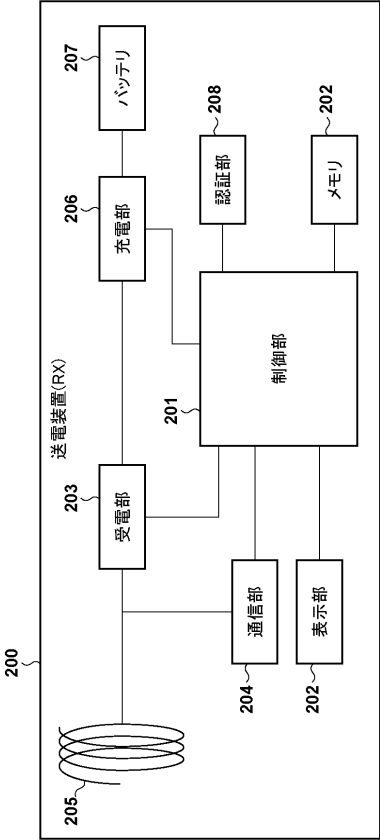
1 0 0 : T X、1 0 1 : 制御部、1 0 2 : 電源部、1 0 3 : 送電部、1 0 4 : 通信部、1 0 5 : 送電コイル、1 0 6 : 表示部、1 0 7 : メモリ、1 0 8 : 第一認証部、1 0 9 : 第二認証部、2 0 0 : R X、2 0 1 : 制御部、2 0 2 : 表示部、2 0 3 : 受電部、2 0 4 : 通信部、2 0 5 : 受電コイル、2 0 6 : 充電部、2 0 7 : バッテリ、2 0 8 : 認証部、2 0 9 : メモリ

40

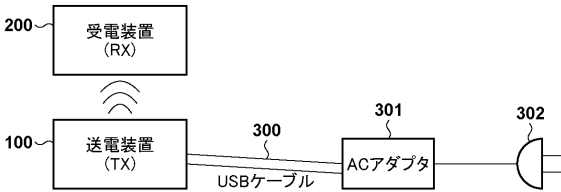
【図 1】



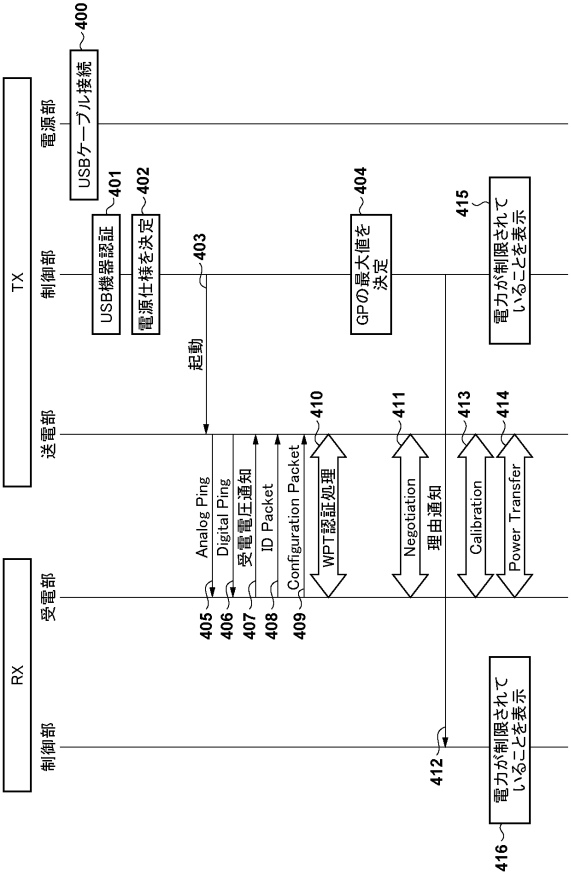
【図 2】



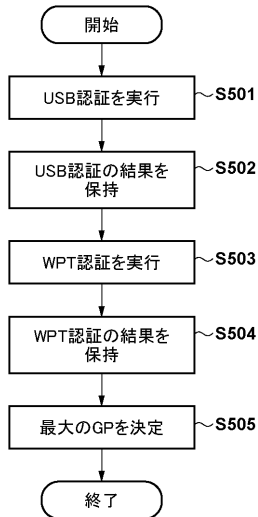
【図 3】



【図 4】



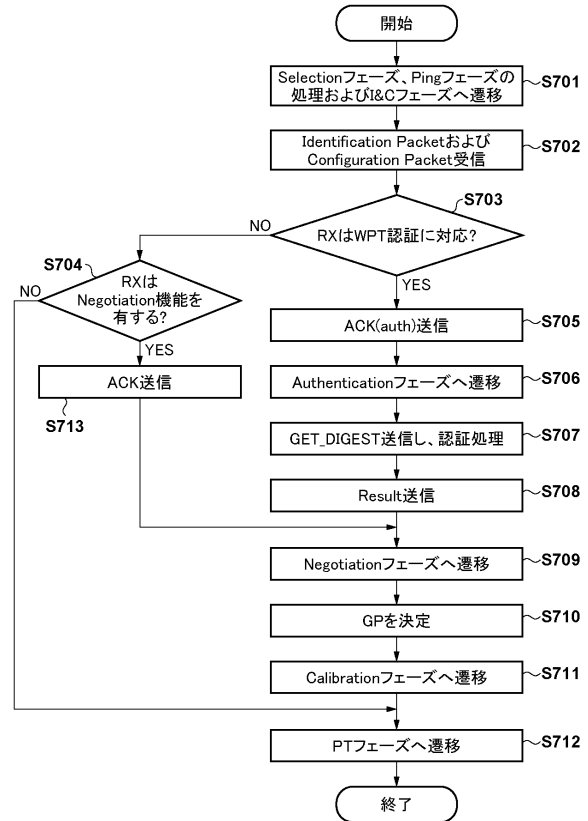
【図 5】



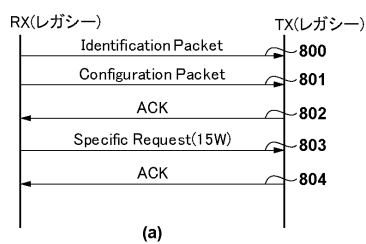
【図 6】

	600	601	602
	USB認証非対応	USB認証失敗	USB認証成功
603 WPT認証非対応	5	0, 2.5, 5	5
604 WPT認証失敗	0, 2.5, 5	0, 2.5, 5	0, 2.5, 5
605 WPT認証成功	5	0, 2.5, 5	15

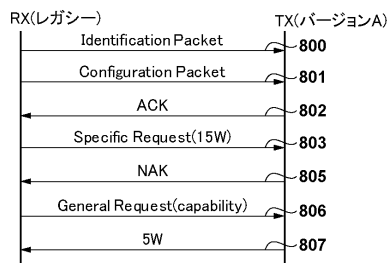
【図 7】



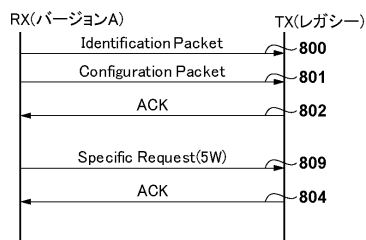
【図 8 A】



(a)

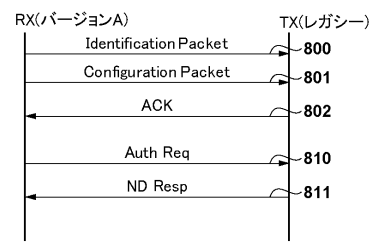


(b)

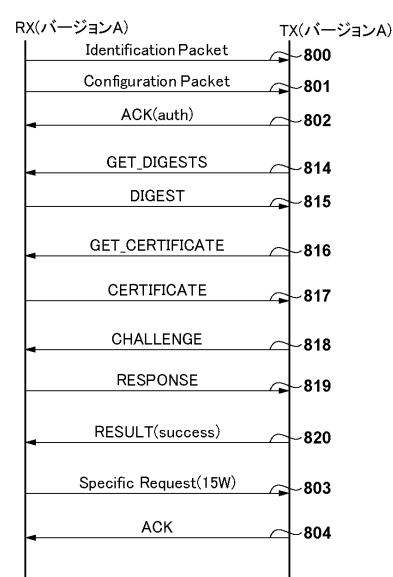


(c)

【図 8 B】

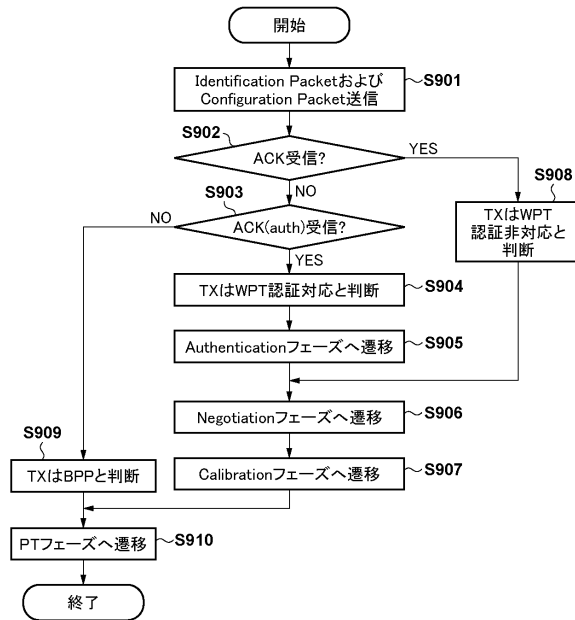


(d)

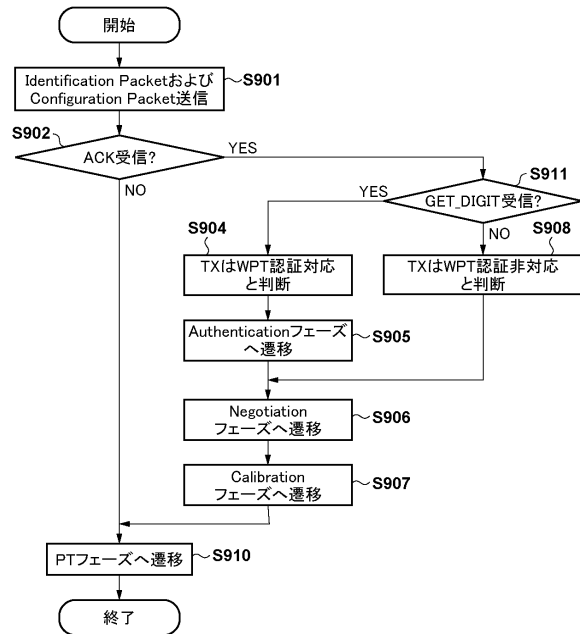


(e)

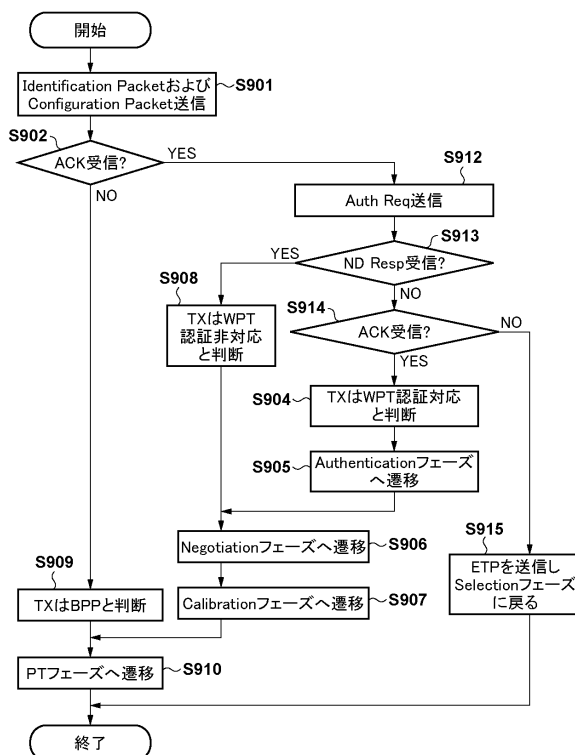
【図 9 A】



【図 9 B】



【図 9 C】



【図 10】

	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0	
Bank0	Power Class		Maximum Power Value						
Bank1	Reserved								1000
Bank2	Prop	Reserved			ZERO		Count		
Bank3	Window Size					Window Offset			
Bank4	Neg	Polarity		Depth		Reserved			1002

(a)

	bit7	bit6	bit5	bit4	bit3	bit2	bit1	bit0
Bank0	Power Class		Guaranteed Power Value					
Bank1	Reserved		Potential Power Value					
Bank2	Reserved						WPID	Not Res Sens

(b)

フロントページの続き

(56)参考文献 特開 2 0 1 7 - 1 1 2 8 2 5 (J P , A)
特開 2 0 1 6 - 0 7 7 1 4 2 (J P , A)
特開 2 0 1 6 - 0 1 0 0 7 0 (J P , A)
特開 2 0 1 4 - 1 0 7 9 7 1 (J P , A)

(58)調査した分野(Int.Cl. , D B 名)

H 0 2 J 5 0 / 0 0 - 5 0 / 9 0
H 0 2 J 7 / 0 0