

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6120526号  
(P6120526)

(45) 発行日 平成29年4月26日(2017.4.26)

(24) 登録日 平成29年4月7日(2017.4.7)

(51) Int.Cl.

F I

HO 4W 36/18	(2009.01)	HO 4W 36/18	
HO 4W 8/24	(2009.01)	HO 4W 8/24	
HO 4W 92/18	(2009.01)	HO 4W 92/18	
HO 4W 84/10	(2009.01)	HO 4W 84/10	1 1 0

請求項の数 20 (全 17 頁)

(21) 出願番号 特願2012-241099 (P2012-241099)  
 (22) 出願日 平成24年10月31日(2012.10.31)  
 (65) 公開番号 特開2014-93567 (P2014-93567A)  
 (43) 公開日 平成26年5月19日(2014.5.19)  
 審査請求日 平成27年10月21日(2015.10.21)

(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 100076428  
 弁理士 大塚 康德  
 (74) 代理人 100112508  
 弁理士 高柳 司郎  
 (74) 代理人 100115071  
 弁理士 大塚 康弘  
 (74) 代理人 100116894  
 弁理士 木村 秀二  
 (74) 代理人 100130409  
 弁理士 下山 治  
 (74) 代理人 100134175  
 弁理士 永川 行光

最終頁に続く

(54) 【発明の名称】 通信装置、その制御方法、及びプログラム

(57) 【特許請求の範囲】

【請求項 1】

通信装置であって、

第1の通信方式により通信する第1の通信インタフェースと、

第2の通信方式により通信する第2の通信インタフェースと、

前記第1の通信インタフェースを用いて接続した相手方装置から、前記第1の通信インタフェースを用いて、前記第2の通信インタフェースによるネットワークにおいて相手方装置を識別する識別情報を取得する取得手段と、

前記取得手段によって取得された情報に基づいて、前記第2の通信インタフェースを用いて既に確立されている第1の通信路を用いて、前記相手方装置との通信が可能かを判定する判定手段と、を有し、

前記第2の通信インタフェースは、前記第1の通信路を用いて前記相手方装置との通信が可能であると前記判定手段により判定された場合、前記第1の通信路を介して前記相手方装置と通信し、

前記第2の通信インタフェースは、前記第1の通信路を用いて前記相手方装置との通信が可能であると前記判定手段により判定されなかった場合、前記相手方装置から前記第1の通信インタフェースを用いて取得した無線設定情報に基づいて確立される第2の通信路を介して前記相手方装置と通信する、

ことを特徴とする通信装置。

【請求項 2】

10

20

前記取得手段により取得される情報は、前記相手方装置のＭＡＣアドレスである、  
ことを特徴とする請求項１に記載の通信装置。

【請求項３】

前記第２の通信インタフェースは、前記第２の通信路を確立する場合、前記第１の通信路を切断して当該第２の通信路を確立し、前記第２の通信路を切断する場合、前記第１の通信路へ接続を戻す、

ことを特徴とする請求項１又は２に記載の通信装置。

【請求項４】

前記第１の通信インタフェースを用いて前記相手方装置と近接しているかを検知する検知手段をさらに有し、

前記第２の通信インタフェースは、前記第２の通信路を確立していた場合において、前記検知手段が前記相手方装置と近接していないことを検知した場合、前記第２の通信インタフェースを用いて確立する通信路を、前記第１の通信路へと戻す、

ことを特徴とする請求項１から３のいずれか１項に記載の通信装置。

【請求項５】

前記第２の通信インタフェースを用いた通信の利用状況を観測する観測手段をさらに有し、

前記第２の通信インタフェースは、前記第２の通信路を確立していた場合において、前記検知手段が前記相手方装置と近接していないことを検知した場合であって、前記利用状況が、規定時間以上のデータ通信パケットの未検出または上位アプリケーションからのセッション確保継続要求がないことを示す場合、前記第２の通信インタフェースを用いて確立する通信路を、前記第１の通信路へと戻す、

ことを特徴とする請求項４に記載の通信装置。

【請求項６】

前記取得手段は、前記第２の通信インタフェースによるネットワークにおいて前記相手方装置を識別する識別情報を取得し、

前記判定手段は、前記第２の通信インタフェースによる通信相手の識別情報記憶テーブルに、前記相手方装置の識別情報が含まれている場合、前記第１の通信路を用いて前記相手方装置への接続が可能であると判定する、

ことを特徴とする請求項１から５のいずれか１項に記載の通信装置。

【請求項７】

通信装置であって、

第１の通信方式により通信する第１の通信インタフェースと、

第２の通信方式により通信する第２の通信インタフェースと、

前記第１の通信インタフェースを用いて接続した相手方装置から、前記第１の通信インタフェースを用いて、前記第２の通信インタフェースによるネットワークにおいて相手方装置を識別する識別情報と、前記相手方装置において前記第２の通信方式を用いて既に確立されている他の装置を介する通信路に関する情報との少なくともいずれかを取得する取得手段と、

前記取得手段によって取得された情報に基づいて、前記第２の通信インタフェースを用いて既に確立されている第１の通信路を用いて、前記相手方装置との通信が可能かを判定する判定手段と、を有し、

前記相手方装置において前記第２の通信方式を用いて既に確立されている他の装置を介する通信路に関する情報は、当該通信路を介する前記相手方装置の通信相手を識別する識別情報を含み、

前記判定手段は、前記相手方装置の通信相手の識別情報記憶テーブルに、前記通信装置の識別情報が含まれている場合、前記第１の通信路を用いて前記相手方装置への接続が可能であると判定し、

前記第２の通信インタフェースは、前記第１の通信路を用いて前記相手方装置との通信が可能であると前記判定手段により判定された場合、前記第１の通信路を介して前記相手

10

20

30

40

50

方装置と通信し、

前記第 2 の通信インタフェースは、前記第 1 の通信路を用いて前記相手方装置との通信が可能であると前記判定手段により判定されなかった場合、前記相手方装置から前記第 1 の通信インタフェースを用いて取得した無線設定情報に基づいて確立される第 2 の通信路を介して前記相手方装置と通信する、

ことを特徴とする通信装置。

【請求項 8】

通信装置であって、

第 1 の通信方式により通信する第 1 の通信インタフェースと、

第 2 の通信方式により通信する第 2 の通信インタフェースと、

前記第 1 の通信インタフェースを用いて接続した相手方装置から、前記第 1 の通信インタフェースを用いて、前記第 2 の通信インタフェースによるネットワークにおいて相手方装置を識別する識別情報と、前記相手方装置において前記第 2 の通信方式を用いて既に確立されている他の装置を介する通信路に関する情報との少なくともいずれかを取得する取得手段と、

前記取得手段によって取得された情報に基づいて、前記第 2 の通信インタフェースを用いて既に確立されている第 1 の通信路を用いて、前記相手方装置との通信が可能かを判定する判定手段と、を有し、

前記通信装置において前記第 2 の通信方式を用いて既に確立されている他の装置を介する通信路に関する情報は、当該通信路を介する前記通信装置の通信相手を識別する識別情報を含み、

前記判定手段は、前記通信装置の通信相手の識別情報記憶テーブルに、前記相手方装置の識別情報が含まれている場合、前記第 1 の通信路を用いて前記相手方装置への接続が可能であると判定し、

前記第 2 の通信インタフェースは、前記第 1 の通信路を用いて前記相手方装置との通信が可能であると前記判定手段により判定された場合、前記第 1 の通信路を介して前記相手方装置と通信し、

前記第 2 の通信インタフェースは、前記第 1 の通信路を用いて前記相手方装置との通信が可能であると前記判定手段により判定されなかった場合、前記相手方装置から前記第 1 の通信インタフェースを用いて取得した無線設定情報に基づいて確立される第 2 の通信路を介して前記相手方装置と通信する、

ことを特徴とする通信装置。

【請求項 9】

通信装置であって、

第 1 の通信方式により通信する第 1 の通信インタフェースと、

第 2 の通信方式により通信する第 2 の通信インタフェースと、

前記第 1 の通信インタフェースを用いて接続した相手方装置から、前記第 1 の通信インタフェースを用いて、前記第 2 の通信インタフェースによるネットワークにおいて相手方装置を識別する識別情報と、前記相手方装置において前記第 2 の通信方式を用いて既に確立されている他の装置を介する通信路に関する情報との少なくともいずれかを取得する取得手段と、

前記取得手段によって取得された情報に基づいて、前記第 2 の通信インタフェースを用いて既に確立されている第 1 の通信路を用いて、前記相手方装置との通信が可能かを判定する判定手段と、を有し、

前記相手方装置において前記第 2 の通信方式を用いて既に確立されている他の装置を介する通信路に関する情報は、前記第 2 の通信方式による接続先のネットワークの識別情報と、ネットワークにおいて互いに接続できる通信装置のグループの情報とを含み、

前記判定手段は、前記通信装置において前記第 2 の通信インタフェースによる接続先のネットワークの識別情報と、前記相手方装置の接続先のネットワークの識別情報とが同一であり、かつ、前記通信装置と前記相手方装置とが、1つの前記グループに含まれる場合

10

20

30

40

50

、前記第 1 の通信路を用いて前記相手方装置への接続が可能であると判定し、

前記第 2 の通信インタフェースは、前記第 1 の通信路を用いて前記相手方装置との通信が可能であると前記判定手段により判定された場合、前記第 1 の通信路を介して前記相手方装置と通信し、

前記第 2 の通信インタフェースは、前記第 1 の通信路を用いて前記相手方装置との通信が可能であると前記判定手段により判定されなかった場合、前記相手方装置から前記第 1 の通信インタフェースを用いて取得した無線設定情報に基づいて確立される第 2 の通信路を介して前記相手方装置と通信する、

ことを特徴とする通信装置。

【請求項 10】

前記第 1 の通信インタフェースは、前記相手方装置と近接した場合に通信を行う近接無線通信インタフェースである、

ことを特徴とする請求項 1 から 9 のいずれか 1 項に記載の通信装置。

【請求項 11】

前記近接無線通信インタフェースは、動作モードとして、Peer-to-Peer モードを含む、

ことを特徴とする請求項 10 に記載の通信装置。

【請求項 12】

前記近接無線通信インタフェースは、動作モードとして、タグモードとリーダ/ライタモードとを含み、前記通信装置がタグモードで動作する場合は前記相手方装置はリーダ/ライタモードとして動作し、前記通信装置がリーダ/ライタモードで動作する場合は前記相手方装置はタグモードとして動作する、

ことを特徴とする請求項 10 に記載の通信装置。

【請求項 13】

前記第 2 の通信インタフェースは無線 LAN インタフェースである、

ことを特徴とする請求項 1 から 12 のいずれか 1 項に記載の通信装置。

【請求項 14】

前記第 2 の通信路は、インフラストラクチャモード、アドホックモード、又は Wi-Fi ダイレクトモードに従って確立される、

ことを特徴とする請求項 13 に記載の通信装置。

【請求項 15】

前記第 2 の通信インタフェースは Bluetooth インタフェースである、

ことを特徴とする請求項 1 から 12 のいずれか 1 項に記載の通信装置。

【請求項 16】

前記無線設定情報は、Network Index、SSID、Authentication Type、Encryption Type、Network Key Index、Network Key、Mac Address、EAP Type、EAP Index、Key Provided Automatically、802.1x Enabled 及び Network key Shareable のうち少なくともいずれかを含む、

ことを特徴とする請求項 1 から 15 のいずれか 1 項に記載の通信装置。

【請求項 17】

通信装置であって、

第 1 の通信方式により通信する第 1 の通信インタフェースと、

第 2 の通信方式により通信する第 2 の通信インタフェースと、

前記第 1 の通信インタフェースを用いて接続した相手方装置から、前記第 1 の通信インタフェースを用いて、前記第 2 の通信インタフェースによるネットワークにおいて相手方装置を識別する識別情報と、前記相手方装置において前記第 2 の通信方式を用いて既に確立されている他の装置を介する通信路に関する情報との少なくともいずれかを取得する取得手段と、

10

20

30

40

50

前記取得手段によって取得された情報に基づいて、前記第２の通信インタフェースを用いて既に確立されている第１の通信路を用いて、前記相手方装置との通信が可能かを判定する判定手段と、を有し、

前記第２の通信インタフェースは、前記第１の通信路を用いて前記相手方装置との通信が可能であると前記判定手段により判定された場合、前記第１の通信路を介して前記相手方装置と通信し、

前記第２の通信インタフェースは、前記第１の通信路を用いて前記相手方装置との通信が可能であると前記判定手段により判定されなかった場合、前記相手方装置から前記第１の通信インタフェースを用いて取得した無線設定情報に基づいて確立される第２の通信路を介して前記相手方装置と通信し、

10

前記第２の通信インタフェースは、前記第２の通信路を確立する場合、前記第１の通信路を切断して当該第２の通信路を確立し、前記第２の通信路を切断する場合、前記第１の通信路へ接続を戻す、

ことを特徴とする通信装置。

【請求項１８】

第１の通信方式により通信する第１の通信インタフェースと、第２の通信方式により通信する第２の通信インタフェースと、を有する通信装置の制御方法であって、

前記第１の通信インタフェースを用いて接続した相手方装置から、前記第１の通信インタフェースを用いて、前記第２の通信インタフェースによるネットワークにおいて相手方装置を識別する識別情報を取得する取得工程と、

20

前記取得工程において取得した情報に基づいて、前記第２の通信インタフェースを用いて既に確立されている第１の通信路を用いて、前記相手方装置との通信が可能かを判定する判定工程と、

前記第１の通信路を用いて前記相手方装置との通信が可能であると前記判定工程において判定された場合、前記第２の通信インタフェースを用いて、前記第１の通信路を介して前記相手方装置と通信する工程と、

前記第１の通信路を用いて前記相手方装置との通信が可能であると前記判定工程において判定されなかった場合、前記第２の通信インタフェースを用いて、前記相手方装置から前記第１の通信インタフェースを用いて取得した無線設定情報に基づいて確立される第２の通信路を介して前記相手方装置と通信する工程と、

30

を有することを特徴とする制御方法。

【請求項１９】

通信方法であって、

第１の通信方式を用いて、第２の通信方式によるネットワークにおいて第１通信装置を識別する識別情報を前記第１通信装置から第２通信装置に提供し、

前記第１通信装置と前記第２通信装置とが前記第２の通信方式により既に確立されている第１の通信路を用いて通信が可能であると、前記識別情報に基づいて判定された場合、前記第１通信装置と前記第２通信装置は、前記第１の通信路を介して通信し、

前記第１通信装置と前記第２通信装置とが前記第１の通信路を用いて通信が可能であると、前記識別情報に基づいて判定されなかった場合、前記第１通信装置と前記第２通信装置は、前記第１の通信方式を用いて共有された無線設定情報に基づいて確立される第２の通信路を介して通信する、

40

ことを特徴とする通信方法。

【請求項２０】

コンピュータを請求項１から１７のいずれか１項に記載の通信装置が備える各手段として機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は複数インタフェース間のハンドオーバー技術に関する。

50

## 【背景技術】

## 【0002】

非特許文献1には、図12に示すように、低速の近接無線通信インタフェースの近接を契機として高速無線通信インタフェースの接続を設定し、低速通信パスから、設定した高速通信パスへP2P通信セッションをハンドオーバーさせる技術が記載されている。なお、近接無線通信インタフェースは、例えばNFCであり、高速無線通信インタフェースは、例えば、無線LANインタフェース、Bluetooth（登録商標）インタフェースである。

## 【0003】

また、特許文献1には、P2P通信セッションのハンドオーバー先である高速無線通信用の媒体の候補が複数ある場合、近接低速無線通信の通信パスを介してサービス能力等の情報を交換し、適切な高速無線通信媒体にハンドオーバーする方法が記載されている。また、特許文献2には、端末が、高速無線通信インタフェースを介して享受しているネットワークサービスの実行手順を、近接無線通信インタフェースを介して他の端末へ通知することで、他の端末に同一のサービスを享受させる方法が記載されている。

10

## 【先行技術文献】

## 【特許文献】

## 【0004】

【特許文献1】特開2010-279042号公報

【特許文献2】特開2010-219824号公報

20

【特許文献3】特開2008-131175号公報

## 【非特許文献】

## 【0005】

【非特許文献1】「NFC Connection Handover 1.2 Technical Specification」、NFC Forum、2010年7月

## 【発明の概要】

## 【発明が解決しようとする課題】

## 【0006】

しかし、上述の技術では、既に高速無線通信インタフェースを介して他の通信機器と通信を実行している場合、図13に示すように、接続設定処理（1ホップ目の無線接続先変更）に伴い、既存の通信路が切断されてしまうという課題があった。

30

## 【0007】

これに対し、特許文献3には、近接無線通信インタフェースを介して、他の装置の個別識別情報を読み出した後、高速無線通信路を介してその識別情報を用いた機器探索処理を実行し、高速無線通信路の設定変更の必要性を判定する方法が記載されている。

## 【0009】

本発明は上記先行技術らの課題に鑑みなされたものであり、複数のインタフェース間のハンドオーバーを、既存の通信路の切断を防ぎながら、高速に実行する技術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】

40

## 【0010】

上記目的を達成するため、本発明による通信装置は、第1の通信方式により通信する第1の通信インタフェースと、第2の通信方式により通信する第2の通信インタフェースと、前記第1の通信インタフェースを用いて接続した相手方装置から、前記第1の通信インタフェースを用いて、前記第2の通信インタフェースによるネットワークにおいて相手方装置を識別する識別情報を取得する取得手段と、前記取得手段によって取得された情報に基づいて、前記第2の通信インタフェースを用いて既に確立されている第1の通信路を用いて、前記相手方装置との通信が可能かを判定する判定手段と、を有し、前記第2の通信インタフェースは、前記第1の通信路を用いて前記相手方装置との通信が可能であると前記判定手段により判定された場合、前記第1の通信路を介して前記相手方装置と通信し、

50

前記第 2 の通信インタフェースは、前記第 1 の通信路を用いて前記相手方装置との通信が可能であると前記判定手段により判定されなかった場合、前記相手方装置から前記第 1 の通信インタフェースを用いて取得した無線設定情報に基づいて確立される第 2 の通信路を介して前記相手方装置と通信する、ことを特徴とする。

【発明の効果】

【0011】

本発明によれば、複数のインタフェース間のハンドオーバを、既存の通信路の切断を防ぎながら、高速に実行することができる。

【図面の簡単な説明】

【0012】

【図 1】確立中の高速無線通信インタフェースを利用する P 2 P 通信パスの通信メディアハンドオーバ制御の概念図。

【図 2】通信メディアハンドオーバを実行する通信装置の機能構成例を示すブロック図。

【図 3】通信メディアハンドオーバを実行する通信装置の機能構成例を示すブロック図。

【図 4】P 2 P 通信パスの通信メディアハンドオーバに係る IP 接続設定の要否判断処理を示すフローチャート。

【図 5】P 2 P 通信パスの通信メディアハンドオーバの動作を示すシーケンス図。

【図 6】回線設定用情報の一例を示す図。

【図 7】確立中の高速無線通信インタフェースを利用する P 2 P 通信パスの通信メディアハンドオーバ制御のもう 1 つの概念図。

【図 8】確立中の高速無線通信インタフェースを利用できない場合の P 2 P 通信パスの通信メディアハンドオーバ制御の概念図。

【図 9】実施形態 2 に係る P 2 P 通信パスの通信メディアハンドオーバに係る IP 接続設定の要否判断処理を示すフローチャート。

【図 10】実施形態 2 に係る P 2 P 通信パスの通信メディアハンドオーバの動作を示すシーケンス図。

【図 11】実施形態 3 に係る P 2 P 通信パスの通信メディアハンドオーバに係る IP 接続設定の要否判断処理を示すフローチャート。

【図 12】従来の P 2 P 通信パスの通信メディアハンドオーバ制御の概念図。

【図 13】従来の P 2 P 通信パスの通信メディアハンドオーバ制御の課題の一例を示す図

。

【発明を実施するための形態】

【0013】

以下、添付図面を参照して本発明の実施の形態を詳細に説明する。

【0014】

< 実施形態 1 >

図 1 は、本実施形態に係る通信メディアハンドオーバの概念を示す図である。本実施形態に係る通信メディアハンドオーバでは、第 1 通信装置 10 と第 2 通信装置 11 とが第 1 の通信インタフェースで論理通信セッション 100 を確立し、その後、確立済みの第 2 の通信インタフェースの P 2 P 通信パス 110 にハンドオーバ ( 120 ) する。ここで、例えば、第 1 の通信インタフェースは低速な近接無線通信インタフェースであり、第 2 の通信インタフェースは高速無線通信インタフェースである。また、近接無線通信インタフェースは例えば NFC であり、通信装置と相手方通信装置とが互いに近接したことを検知すると、通信セッションを確立するインタフェースである。また、高速無線通信インタフェースは、例えば、無線 LAN インタフェース、Bluetooth インタフェースであり、「確立済み」とは、第 1 通信装置 10 と第 2 通信装置 11 とが接続を試みる時点において確立されていることを意味する。なお、以下の説明では高速無線通信インタフェースとして無線 LAN インタフェースを用いる場合について説明するが、これに代えて Bluetooth インタフェース等を利用してもよい。

【0015】

本実施形態では、第1通信装置10と第2通信装置11とが通信を行う際に、近接無線通信インタフェースにより、確立済みの高速無線通信インタフェースを用いて互いに通信可能な状態にあるかを判定する。この判定には、例えばMACアドレスのような識別情報を用い、高速無線通信インタフェースでの通信が可能な相手方装置の識別情報のリストに、相手方装置の識別情報が含まれているかを判定する。例えば、通信装置が有するリストに相手方装置のMACアドレスが含まれるか、相手方装置が有するリストに通信装置のMACアドレスが含まれるかの、少なくともいずれかの場合に、確立済みの高速無線通信インタフェースを利用可能と判断する。そして、確立済みの高速無線通信インタフェースを利用可能な場合、それに接続を切り替えることにより、既に確立された高速無線通信インタフェースを切断することなく、ハンドオーバを実行することが可能となる。また、本実施形態に係る方法では、相手方装置の識別情報が近接無線通信により分かるため、相手方装置の探索処理を行う必要がない。このため、高速にハンドオーバを実行することが可能となる。

10

#### 【0016】

以下、装置構成と処理について、図2～図8を用いて詳細に説明する。

#### 【0017】

(通信装置の構成)

図2及び図3に、図1における第1通信装置10及び第2通信装置11の機能構成例を示すブロック図を示す。図2は、NFCの動作モードが、第1通信装置10及び第2通信装置11の双方共に、Peer-to-Peerモード(P2Pモード)で動作する場合の、第1通信装置10及び第2通信装置11の構成例である。一方、図3は、NFCの動作モードが、第1通信装置10がタグモード(Card Emulationモード)、第2通信装置11がR/Wモード(リーダ/ライタモード)で動作する場合の、第1通信装置10及び第2通信装置11の構成例である。

20

#### 【0018】

図2において、第2通信装置11は、NFC通信路でのP2P通信100を司る近接無線通信部201と、無線LAN通信路でのP2P通信110を司る無線IP通信部211と、双方の通信部を統括制御する通信制御部202とを含む。また、第2通信装置11は、通信制御部202上に通信ミドルウェア203を有する。そして、通信ミドルウェア203は、通信パスの切換え要否の判定制御を司るメディアハンドオーバー選択部214と、確立済みの無線LANネットワークに関する設定情報213と、確立済みの無線LAN内のARP情報テーブル212とを含む。ここで、ARPは、Address Resolution Protocolの略であり、ARPテーブルは、無線LAN通信路での通信相手のIPアドレスとMACアドレスとの対照表であり、通信相手の識別情報を記憶する識別情報記憶テーブルである。

30

#### 【0019】

第1通信装置10も同様に、NFC通信路でのP2P通信100を司る近接無線通信部205と、無線LAN通信路でのP2P通信110を司る無線IP通信部215と、双方の通信部を統括制御する通信制御部206とを含む。そして、第1通信装置10も通信制御部206上に通信ミドルウェア207を有する。そして、通信ミドルウェア207は、通信パスの切換え要否の判定制御を司るメディアハンドオーバー要求部218と、確立済みの無線LANネットワークに関しての設定情報216と、確立済みの無線LAN内のARP情報テーブル212とを含む。

40

#### 【0020】

図3において、第2通信装置11は、NFC通信路での無線タグ用通信路100を介した情報アクセスを司る近接無線通信部301と、無線LAN通信路でのP2P通信110を司る無線IP通信部311とを含む。また、第2通信装置11は、双方の通信部を統括制御する通信制御部302とを含む。さらに、第2通信装置11は、通信制御部302上に通信ミドルウェア304を有する。そして、通信ミドルウェア304は、通信パスの切換え要否の判定制御を司るメディアハンドオーバー選択部314と、確立済みの無線LAN

50



ネットワークに関する設定情報 3 1 3 と、確立済みの無線 LAN 内の ARP 情報テーブル 3 1 2 とを含む。

【 0 0 2 1 】

第 1 通信装置 1 0 は、NFC 通信路での無線タグ用通信路 1 0 0 を介した情報アクセスを司る近接無線通信タグ 3 0 5 と、無線 LAN 通信路での P 2 P 通信 1 1 0 を司る無線 IP 通信部 3 1 5 と、無線 IP 通信部を制御する通信制御部 3 0 6 とを含む。また、近接無線通信タグ 3 0 5 は、通信パスの切換え要否の判定制御を司る、既存無線 LAN ネットワークに関する設定情報 3 1 8 と、既存無線 LAN ハードウェアの MAC アドレス情報 3 1 8 の情報アクセスエリアとを含む。

【 0 0 2 2 】

( 通信装置の動作 )

続いて、図 4 及び図 5 を用いて、第 1 通信装置 1 0 及び第 2 通信装置 1 1 の動作について説明する。図 4 は、第 2 通信装置 1 1 において、NFC を介して接続された P 2 P の論理通信セッション 1 0 0 の、既存の無線 LAN の P 2 P 通信パス 1 1 0 へのハンドオーバー 1 2 0 の可否を、MAC アドレスを基準として判定する処理の一例を示すフローチャートである。この判定処理は、第 2 通信装置 1 1 のメディアハンドオーバー選択部 2 1 4 又は 3 1 4 において実行される。また、図 5 に、第 1 通信装置 1 0 及び第 2 通信装置 1 1 において実行される、近接無線通信インタフェースから高速無線通信インタフェースへのメディアハンドオーバーの処理手順の一例を示すシーケンスチャートを示す。

【 0 0 2 3 】

P 2 P 通信を実施する第 2 通信装置 1 1 は、NFC 通信機能部を起動中 ( S 4 0 1 ) に第 1 通信装置 1 0 が近接することで、相手方装置の近接を検知し、NFC の設定を行う ( F 5 0 1 )。そして、その後、第 1 通信装置 1 0 側の NFC 通信の動作開始を判定する ( S 4 0 2 )。

【 0 0 2 4 】

第 2 通信装置 1 1 は、NFC 通信路を介して、第 1 通信装置 1 0 の MAC アドレスを第 1 通信装置 1 0 から取得する ( S 4 0 3 )。第 2 通信装置 1 1 は、入手した MAC アドレスを指標として用いて、無線 IP 通信部 2 1 1 又は 3 1 1 に対応した ARP 情報テーブル 2 1 2 又は 3 1 2 を確認する ( S 4 0 4 )。第 1 通信装置 1 0 の無線 IP 通信部 2 1 5 ( 3 1 5 ) の MAC アドレスが ARP 情報テーブル 2 1 2 ( 3 1 2 ) に登録されている場合 ( S 4 0 4 で YES )、既存の無線 LAN 接続の接続先により第 1 通信装置との IP 通信が可能と判断できる。したがって、第 2 通信装置 1 1 は、この場合、1 ホップ目の接続先の変更は不要と判断し、無線 LAN 接続先の変更 ( 5 0 0、S 4 0 8 ) を実行せずに、1 処理単位を終了する。

【 0 0 2 5 】

MAC アドレスの登録が確認できない場合 ( S 4 0 4 で NO )、第 2 通信装置 1 1 は、続いて、NFC 1 0 0 を介して第 1 通信装置 1 0 の通信ミドルウェアと双方向通信が可能な通信モードであるかを判定する ( S 4 0 5 )。NFC 1 0 0 を介した双方向通信が可能な通信モードである場合 ( S 4 0 5 で YES )、第 2 通信装置 1 1 は、第 1 通信装置 1 0 の無線 IP 通信部 2 1 5 に対応した ARP 情報テーブル 2 1 7 を確認する ( F 5 0 2、S 4 0 6 )。そして、第 2 通信装置 1 1 は、ARP 情報テーブル 2 1 7 内に、自機 ( 第 2 通信装置 1 1 ) の無線 IP 通信部 2 1 1 の MAC アドレスが登録されているかを判定する ( S 4 0 7 )。ARP 情報テーブル 2 1 7 内に無線 IP 通信部 2 1 1 の MAC アドレスが登録されている場合 ( S 4 0 7 で YES )、既存の無線 LAN 接続の接続先で、第 2 通信装置との IP 通信が可能と判断できる。したがって、この場合、第 2 通信装置 1 1 は、無線 LAN 接続先の変更 ( 5 0 0、S 4 0 8 ) を実行せずに、1 処理単位を終了する。

【 0 0 2 6 】

第 2 通信装置 1 1 の無線 IP 通信部 2 1 1 ( 3 1 1 ) の MAC アドレスが ARP 情報テーブル 2 1 7 に登録されていない場合 ( S 4 0 7 で NO )、第 2 通信装置 1 1 は、第 1 通信装置 1 0 の無線回線設定用情報 2 1 6 ( 3 1 8 ) を入手する ( F 5 0 3 )。なお、無線

10

20

30

40

50

回線設定用情報はC r e d e n t i a lと呼ばれ、例えばW i - F i（登録商標）アライアンスで規定されたC r e d e n t i a l情報は、図6のような構成要素を有する。第2通信装置11は、第1通信装置10の無線回線設定用情報216（318）の取得（F503）後、その情報を用いて、W P S - N F Cで規定のセットアップ手順を実行する（F504、F505、S408）。なお、W P S - N F Cは、N F Cを用いた無線LANの設定方式である。また、無線LANのセットアップに先立って、通信装置は、既に確立されている通信路において直接接続する（最初の1ホップ目の接続先である）他の装置（例えばA P）との接続を切断する。

#### 【0027】

その後、第2通信装置11は、無線LANのセットアップの成否を判定し（S409）、成功した場合（S409でY E S）は、そのまま1処理単位を終了する。一方、無線LANのセットアップに失敗した場合（S409でN O）は、P2P通信路の設定失敗を利用者に通知するための表示（S410）を行った後に、1処理単位を終了する。

#### 【0028】

上述の1処理単位にて、失敗表示（S410）がされていない状況においては、無線LAN経由で、第1通信装置10と第2通信装置11との間のP2P論理接続が可能である。したがって、この場合は、無線LAN上でP2P通信用の論理接続セッションを設定し（F506、F507）、P2P通信用通信路を確保する。

#### 【0029】

なお、上述の無線LAN接続先の変更（500、S408）は、例えば、無線LANのO u t - O f - B a n d（O O B）を用いた設定情報の変更に基づく、無線LANの動作モードの変更を含む。ここで、動作モードは、例えば、インフラストラクチャモード、アドホックモード、W i - F iダイレクトモードを含む。例えば、上述の例では、第1通信装置10又は第2通信装置11がインフラストラクチャモードでA Pに接続していた場合、接続先の変更に応じて、アドホックモードやW i - F iダイレクトモードへと移行する。

#### 【0030】

一方で、例えばB l u e t o o t hインタフェースを利用している場合、上述の接続先の変更（500、S408）は、N F C通信路を介した新規ペアリングに基づく、動作モードの変更を含む。ここで動作モードとは、例えば、スレーブ接続モードとマスタ接続モードである。このように、適切にモード変更することにより、接続先の変更を容易に行うことが可能となる。また、無線LANの場合はO O Bを用いた設定情報変更により、B l u e t o o t hの場合はN F C通信路を介した新規ペアリングにより、セキュリティを確保しながら通信路を確立することが可能となる。

#### 【0031】

以上の処理によるメディアハンドオーバの結果の例を図1、図7及び図8に示す。ここで、図1及び図7は、既存の無線LAN接続先を利用してメディアハンドオーバをした場合を示し、図8は既存の無線LANを利用できず、新たに無線LANによる直接接続を設定した場合を示している。上述の処理によれば、近接する相手方装置とのP2P通信路の設定の際に、既存の無線LAN接続先を利用するケース、すなわち図1又は図7に示すようなケースを増やすことが可能となる。これにより、図1及び図7に示す場合などにおいて、通信装置自身又は相手方装置内で動作中の他のアプリケーション（W e bアクセス等）への意図しない通信回線断などの影響を発生させるリスクを低減することができる。また、相手方装置の接続先として通信装置が登録されているか、又は通信装置の接続先として相手方装置が登録されているかに応じてハンドオーバを実行するか否かを決定するため、高速にハンドオーバを実行することができる。

#### 【0032】

##### < 実施形態2 >

実施形態1においては、既に確立され接続されている無線LANがある場合に、近接する機器との間でP2P論理通信路を設定できるかの判定条件として、無線LANインタフ

10

20

30

40

50

エースのMACアドレスを利用する例を示した。本実施形態では、P2P論理通信路の設定可否の判定条件に、無線回線設定用情報(Credential)を併用する例を示す。なお、本実施形態に係る第1通信装置10及び第2通信装置11の構成は、実施形態1と同様であるため、説明を省略する。

#### 【0033】

図9は、第2通信装置11において、NFCを介して接続されたP2Pの論理通信セッション(100)の、既存の無線LANの通信パス(110)へのハンドオーバ(120)の可否の判定を行う処理を示すフローチャートである。本実施形態では、この処理において、無線回線設定用情報(Credential)指標に基づいて、ハンドオーバの可否判定を行う。なお、図9に示す処理は、第2通信装置11のメディアハンドオーバ選択部214又は314が行う処理である。また、図10に、第1通信装置10と第2通信装置との間で実行される、近接無線通信インタフェースから高速無線通信インタフェースへのメディアハンドオーバの処理手順を示すシーケンスチャートを示す。

10

#### 【0034】

P2P通信を実施する第2通信装置11は、NFC通信機能部を起動中(S901)に第1通信装置10が近接することで、相手方装置の近接を検知し、NFCの設定を行う(F1001)。そして、その後、第1通信装置10側のNFC通信の動作開始を判定する(S902)。

#### 【0035】

第2通信装置11は、NFCを介して第1通信装置10の通信ミドルウェアと双方向通信が可能な場合は、第1通信装置10の無線IP通信部215に対応した設定済みCredential216を確認する(F1002)。そして、第2通信装置11は、設定済みCredential216の情報から、第1通信装置10のMACアドレスを取得する(S903)。そして、第2通信装置11は、入手した第1通信装置10のMACアドレスを指標として用いて、無線IP通信部211又は311に対応したARP情報テーブル212又は312を確認する(S904)。

20

#### 【0036】

ARP情報テーブル212又は312内に、第1通信装置10の無線IP通信部215又は315のMACアドレスが登録済みであれば(S904でYES)、既存の無線LAN接続の接続先で、第2通信装置とのIP通信が可能と判断できる。このため、第2通信装置11は、無線LAN接続先の変更(1000、S909)を実行せずに1処理単位を終了する。

30

#### 【0037】

一方、第1通信装置10の無線IP通信部215又は315のMACアドレスがARP情報テーブル212又は312に未登録の場合(S904でNO)、第2通信装置11は、第1通信装置10の設定済みCredential216を確認する(S905)。そして、第2通信装置11は、第1通信装置10の設定済みCredential216情報内のSSIDと、第2通信装置11の無線IP通信部211に設定中のSSIDが同一であるかの判定を行う(S906)。なお、SSIDはBasic Service Set IDの略であり、接続先のネットワークの識別情報を表す。

40

#### 【0038】

SSIDが同一と判定された場合(S906でYES)、第1通信装置10と第2通信装置とが1つのAPが形成する1つの無線セル内に存在していると判断できる。このため、第2通信装置11は、次に、第1通信装置10のVLAN(バーチャル(仮想)LAN)の設定状況を確認する(S907)。具体的には、例えば、図6におけるオプション情報エリアである<other>に記載される情報が参照される。そして、第2通信装置11は、第1通信装置10のVLANの設定が、第2通信装置11の設定と同一グループであるかを判定する(S908)。そして、第1通信装置10と第2通信装置11とのVLAN設定が同一グループである場合(S908でYES)は、既存の無線LAN接続の接続先を用いて、第1通信装置10と第2通信装置11との間でIP通信が可能と判断で

50

きる。したがって、この場合、第2通信装置11は、無線LAN接続先の変更(1000、S909)を実行せずに1処理単位を終了する。なお、上述の説明では、1つのVLANのグループに第1通信装置10と第2通信装置11とが含まれるかを判定したが、これに限られない。例えば、VLANの設定以外の何らかの情報に基づいて、ネットワーク内の互いに接続できる通信装置をグループ化する何らかの論理的なセグメントにおいて、第1通信装置10と第2通信装置11とが同一グループに含まれるかを判定するのであってもよい。

#### 【0039】

一方、第1通信装置10の設定済みCredential216情報内のSSIDと、第2通信装置11の無線IP通信部211に設定中のSSIDが同一でない場合(S906でNO)は、新規の無線LANの設定を実行する(S909)。同様に、第1通信装置10と第2通信装置11とのVLAN設定が同一グループでない場合(S908でNO)にも、新規の無線LANの設定を実行する(S909)。具体的には、第2通信装置11は、第1通信装置10の無線回線設定用情報(Credential)216を用いてWPS-NFCにより規定のセットアップ手順を実行する(F1004、F1005、S909)。そして、セットアップの成否の判定を行い(S910)、成功した場合(S910でYES)はそのまま1処理単位を終了する。一方、失敗した場合(S910でNO)は利用者にP2P通信路の設定失敗を喚起するための表示(S911)を行った後、1処理単位を終了する。

#### 【0040】

上記1処理単位にて、失敗表示(S911)がされないような状況では、無線LAN経由で、第1通信装置10、第2通信装置11間のP2P論理接続が可能である。このため、S911で失敗表示された場合を除いて、無線LAN上でP2P通信用の論理接続セッションを設定して(F1007、F1008)、P2P通信用通信路を確保する。

#### 【0041】

上述の処理によっても、実施形態1と同様に、近接する相手方装置とのP2P通信路の設定の際に、既存の無線LAN接続先を利用するケース、すなわち図1又は図7に示すようなケースを増やすことが可能となる。これにより、図1及び図7に示す場合などにおいて、通信装置自身又は相手方装置内で動作中の他のアプリケーション(Webアクセス等)への意図しない通信回線断などの影響を発生させるリスクを低減することができる。

#### 【0042】

##### <<実施形態3>>

上述の実施形態1及び実施形態2においては、NFC通信路の近接を契機に設定されるP2P論理通信路を、無線LAN通信路にメディアハンドオーバーする際に、既存の無線LAN接続パスを優先的に利用する例を示した。本実施形態では、既に確立された無線LAN接続パスを用いて通信を行う際に、通信装置が、無線LAN接続に係るAP13~15との間の無線LAN通信路の切断に備えてバックアップのIBSS用設定をP2P論理通信路を利用して行う場合について説明する。

#### 【0043】

図11は、第1通信装置10及び第2通信装置11のP2P論理通信路を用いた通信中に実行される、バックアップ通信パス用の無線接続設定情報交換処理の概念を示すフローチャートである。

#### 【0044】

通信装置は、P2P通信の開始後、まず、相手方装置とのP2P通信媒体が無線LANの直接通信路(IBSS)であるかの判定を行う(S1101)。ここで、直接通信路とは、APを経由しない通信路のことである。既に直接通信路を利用している場合(S1101でYES)は、通信装置は、処理を、NFCの近接状態になくなったことの検知を契機に行われるP2P通信セッションの切断監視処理(S1107~S1109)へ移行させる。

#### 【0045】

無線LANの間接通信路（AP経由の通信路）を介してP2P通信路を設定している場合（S1101でNO）、通信装置は、相手方装置との間で、NFC-NFCを利用するバックアップの直接無線通信路（IBSS）用の設定情報を交換する（S1102）。その後、通信装置は、接続中のAPとの通信可否状態を確認する（S1103、S1104）。そして、APとの通信が不能となったことを認識した場合（S1104でNO）、バックアップの直接無線通信路（IBSS）用の設定情報の取得の成否を確認する（S1105）。

#### 【0046】

バックアップの直接無線通信路（IBSS）用の設定情報の取得に成功している場合（S1105でYES）は、通信装置は、その設定に従って接続先を切り替え（S1106）、相手方装置との間のP2P論理通信路の接続を継続する。一方、バックアップの直接無線通信路（IBSS）用の設定情報の取得に失敗している場合（S1105でNO）は、通信装置は、P2P通信の継続不能表示を行う（S1110）。そして、その後、通信装置は、処理を、NFCの近接状態になくなったことの検知を契機とする、P2P通信セッションの切断監視処理（S1107～S1109）に移行させる。

#### 【0047】

P2P通信セッションの切断監視処理（S1107～S1109）においては、まず、NFCの近接通信により相手方装置との間の近接状態が確認される（S1107）。そして、通信装置が、相手方装置とNFCで通信可能か否かを判定し（S1108）、通信不能な場合（S1108でNO）に、P2P通信セッションを切断する（S1109）。なお、P2P通信セッションの切断を行う際に、NFC機能部同士の近接の検知を契機に設定したIBSSを用いたP2P論理通信路で通信中である場合には、設定情報を、そのIBSS用の設定を行う前に設定されていた情報に戻す。

#### 【0048】

このような処理により、近接する相手方装置とのP2P通信路の設定後に、相手方装置の移動等により既存の間接無線通信路（AP経由での通信路）の維持が困難になっても、バックアップの直接無線通信路（IBSS）を介してP2P論理通信路を維持できる。さらに、NFC機能部同士が遠隔状態になったことを検出し、これを契機に論理通信路を解放し、設定情報を、直前の間接無線通信路（AP経由での通信路）への接続用の設定情報へと戻すことで、既存のネットワーク設定へ容易に復帰することができる。

#### 【0049】

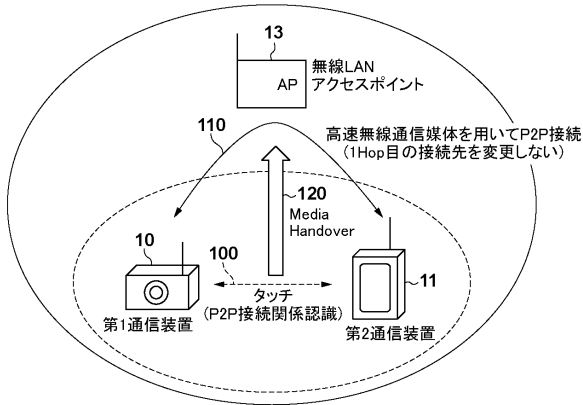
なお、本実施形態では、P2P通信路のセッションの切断（S1109）の判断基準を、NFC機能部同士が遠隔状態になったこと（S1107、S1108）としたが、これに限られない。例えば、この基準に加えて、さらに、P2P通信セッションの利用状況を判断基準に加えてもよい。なお、利用状況とは、例えば、通信セッションにおいてデータパケット通信が行われていない時間が規定時間以上継続しているか否か、又は上位アプリケーションからのセッション確保継続要求があったか否かなどを含む。すなわち、高速無線通信インタフェースによるP2P通信セッションの利用状況を観測し、相手方装置と近接していないことを検知した場合に観測した利用状況がP2P通信セッションを利用していないことを示す場合にのみ、セッションを切断してもよい。このようにすることで、利用者の誤操作等によるNFC通信の瞬断に対しても、利用中のP2P通信路を維持することができ、無駄な再接続処理等を行うことを防ぐことで、通信の効率を向上させることができる。

#### 【0050】

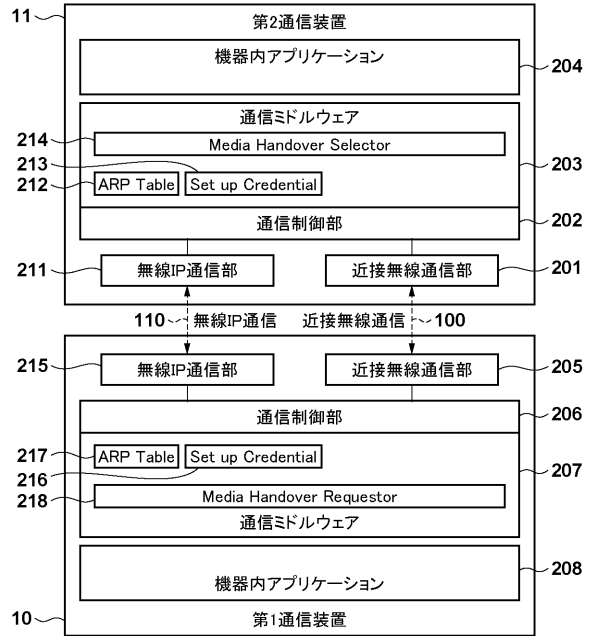
<<その他の実施形態>>

また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはCPUやMPU等）がプログラムを読み出して実行する処理である。

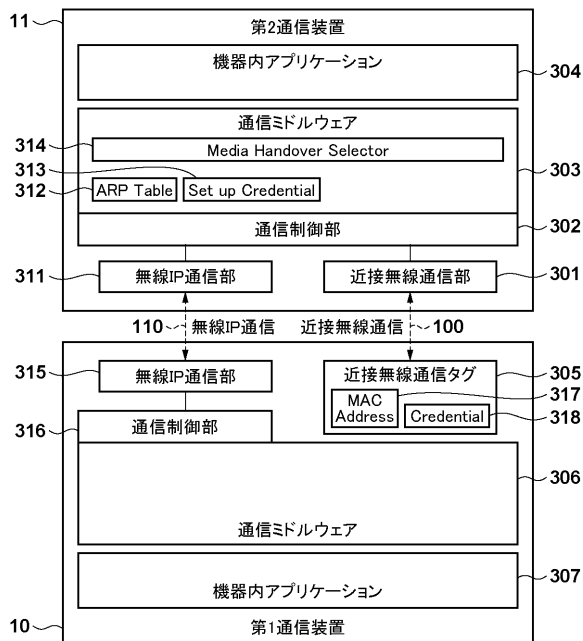
【図 1】



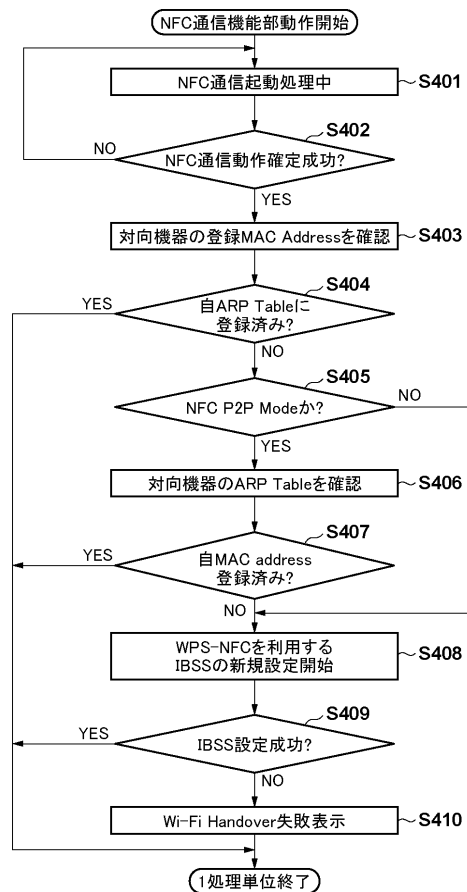
【図 2】



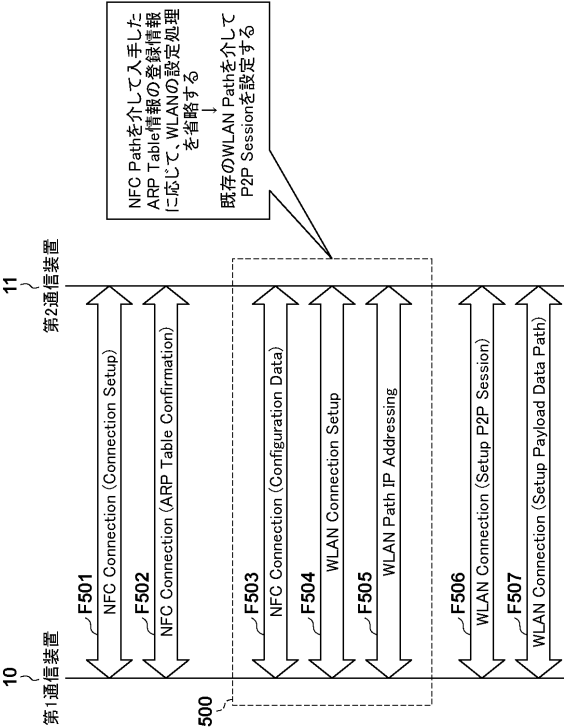
【図 3】



【図 4】



【図5】

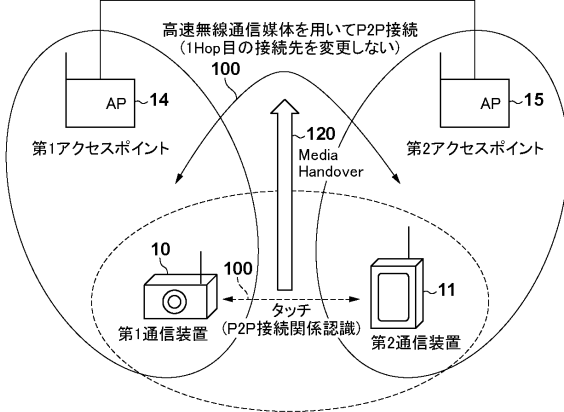


【図6】

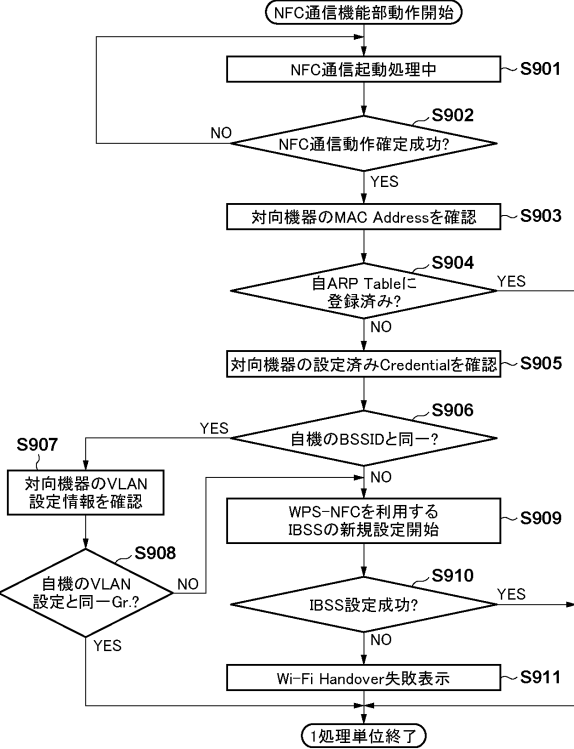
Credential情報の構成要素(Wi-Fi Alliance規格での規定例)

Attribute	R/O	Notes, Allowed Values
Network Index	R	Deprecated – use fixed value 1 for backwards compatibility.
SSID	R	SSID of network.
Authentication Type	R	The authentication type used in this network.
Encryption Type	R	The encryption type used in this network.
Network Key Index	O	Deprecated. Only included by WSC 1.0 devices. Ignored by WSC 2.0 or newer devices.
Network Key	R	
MAC Address	R	Member device's MAC address.
EAP Type	O	
EAP Identity	O	
Key Provided Automatically	O	
802.1X Enabled	O	
Network Key Shareable (inside WFA Vendor Extension)	O	If present, this attribute indicates whether the Network Key can be shared or not with other devices.
<other...>	O	Multiple attributes are permitted.

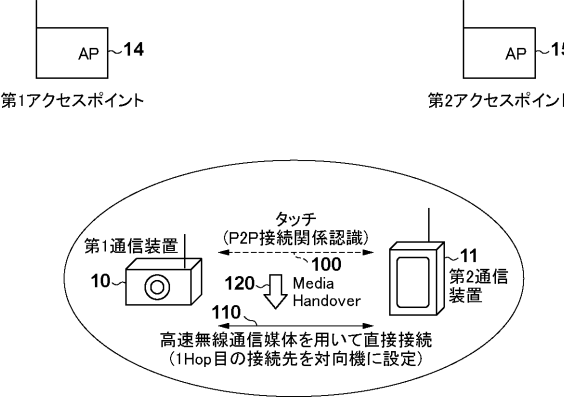
【図7】



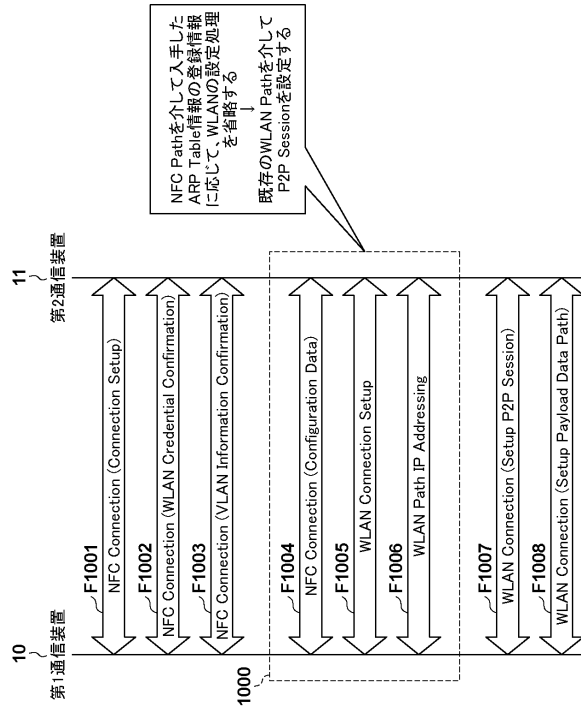
【図9】



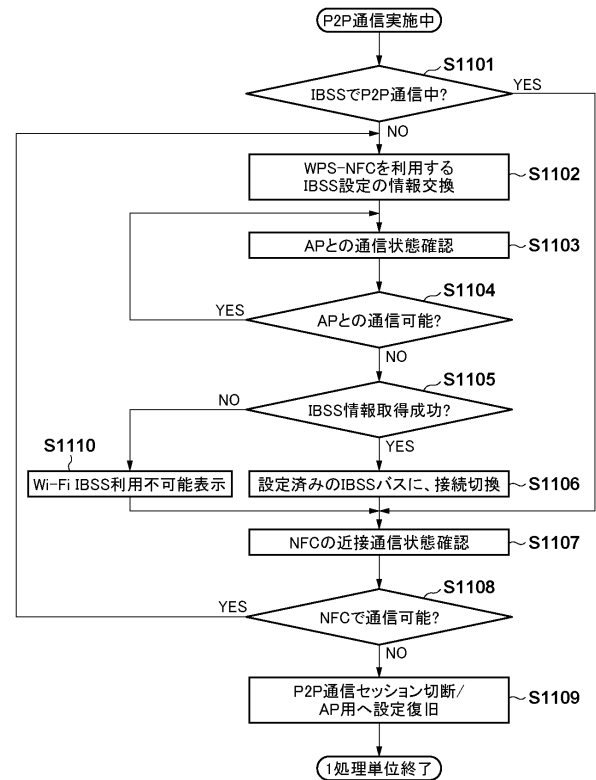
【図8】



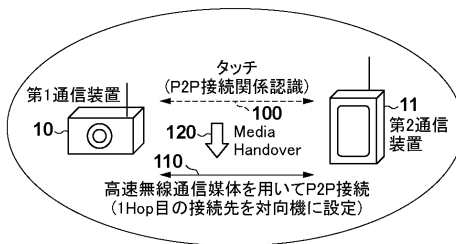
【図10】



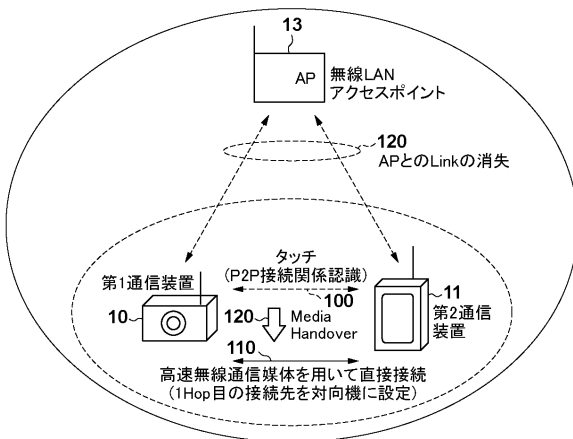
【図11】



【図12】



【図13】





---

フロントページの続き

(72)発明者 濱 田 正志  
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 篠田 享佑

(56)参考文献 特開2013-214804(JP,A)  
特開2011-182449(JP,A)  
特開2010-288208(JP,A)

(58)調査した分野(Int.Cl., DB名)

H04B	7/24 - 7/26
H04W	4/00 - 99/00
3GPP	TSG RAN WG1 - 4
	SA WG1 - 4
	CT WG1、4