

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2014-27538
(P2014-27538A)

(43) 公開日 平成26年2月6日(2014.2.6)

(51) Int.Cl.	F I	テーマコード (参考)
HO4W 48/18 (2009.01)	HO4Q 7/00 411	5K067
HO4W 88/06 (2009.01)	HO4Q 7/00 653	

審査請求 未請求 請求項の数 13 O L (全 37 頁)

(21) 出願番号 特願2012-167251 (P2012-167251)
(22) 出願日 平成24年7月27日 (2012.7.27)

(71) 出願人 00005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町15番1号
(74) 代理人 110000110
特許業務法人快友国際特許事務所
(72) 発明者 西川 直希
愛知県名古屋市瑞穂区苗代町15番1号
ブラザー工業株式会社内
Fターム(参考) 5K067 AA23 AA30 BB21 EE02 EE06
EE10 HH22 HH36

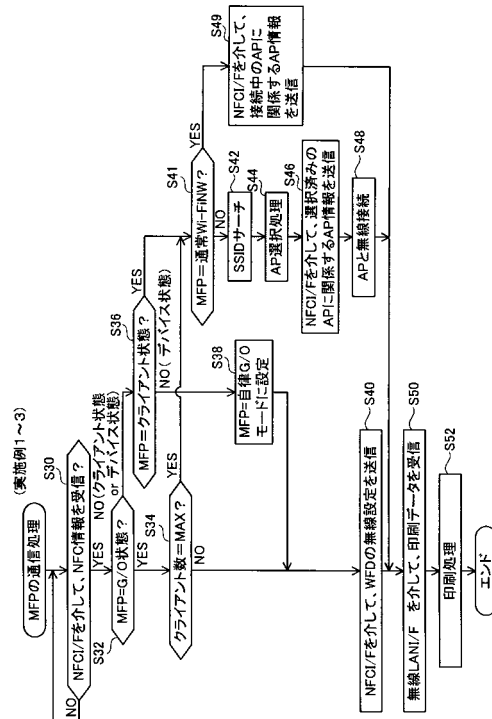
(54) 【発明の名称】 通信装置

(57) 【要約】

【課題】 対象データの無線通信を適切に実行し得る技術を開示する。

【解決手段】 携帯端末が、中継装置を介さない直接無線通信をMFPと実行するための特定の態様で、WFDネットワークに参加することが可能である第1の場合(S34でNOの場合)に、MFPは、携帯端末がWFDネットワークに参加するための無線設定を、携帯端末に送信する(S40)携帯端末が、特定の態様でWFDネットワークに参加することが可能でない第2の場合に、MFPは、携帯端末が通常Wi-Fiネットワークに参加するための無線設定を、携帯端末に送信する(S46、S49)。MFPは、第1の場合に、WFDネットワークを利用して、携帯端末と対象データの直接無線通信を実行し、第2の場合に、通常Wi-Fiネットワークを利用して、アクセスポイントを介して、携帯端末と対象データの無線通信を実行する。

【選択図】 図3



【特許請求の範囲】**【請求項 1】**

親局状態又は子局状態で動作して、第 1 種の無線ネットワークに属することが可能な第 1 の通信装置であって、

前記第 2 の通信装置が、中継装置を介さない直接無線通信を前記第 1 の通信装置と実行するための特定の態様で、前記第 1 種の無線ネットワークに参加することが可能である第 1 の場合に、前記第 2 の通信装置が前記第 1 種の無線ネットワークに参加するための第 1 の無線設定を、前記第 2 の通信装置に送信し、

前記第 2 の通信装置が、前記特定の態様で前記第 1 種の無線ネットワークに参加することが可能でない第 2 の場合に、前記第 2 の通信装置が第 2 種の無線ネットワークに参加するための第 2 の無線設定を、前記第 2 の通信装置に送信する送信部であって、

前記第 2 種の無線ネットワークは、前記第 1 の通信装置及び前記第 2 の通信装置とは別体に構成されている特定の中継装置を含む無線ネットワークである、前記送信部と、

前記第 1 の場合に、前記第 1 種の無線ネットワークを利用して、前記第 2 の通信装置と対象データの直接無線通信を実行し、

前記第 2 の場合に、前記第 2 種の無線ネットワークを利用して、前記特定の中継装置を介して、前記第 2 の通信装置と前記対象データの無線通信を実行する通信実行部と、

を備える、第 1 の通信装置。

【請求項 2】

前記第 1 の通信装置は、さらに、

前記第 2 の通信装置と無線通信を実行するための第 1 種のインターフェースと、

前記第 2 の通信装置と無線通信を実行するための第 2 種のインターフェースであって、前記第 2 種のインターフェースを介した無線通信の通信速度は、前記第 1 種のインターフェースを介した無線通信の通信速度よりも速い、前記第 2 種のインターフェースと、

を備え、

前記送信部は、

前記第 1 の場合に、前記第 1 種のインターフェースを介して、前記第 1 の無線設定を前記第 2 の通信装置に送信し、

前記第 2 の場合に、前記第 1 種のインターフェースを介して、前記第 2 の無線設定を前記第 2 の通信装置に送信し、

前記第 1 種及び第 2 種の無線ネットワークのそれぞれは、前記第 2 種のインターフェースを介した無線通信を実行するための無線ネットワークである、請求項 1 に記載の第 1 の通信装置。

【請求項 3】

前記第 1 の通信装置が前記親局状態で動作して前記第 1 種の無線ネットワークに属する場合に、前記第 1 種の無線ネットワークに属することが可能な子局機器の最大数は、 N (前記 N は 1 以上の整数) であり、

前記子局機器は、前記子局状態で動作して前記第 1 種の無線ネットワークに属する機器であり、

前記第 1 の通信装置は、さらに、

前記第 1 の通信装置が前記親局状態で動作して前記第 1 種の無線ネットワークに現在属している場合に、前記第 1 種の無線ネットワークに現在属している前記子局機器の数が、前記 N 未満であるのか、前記 N であるのか、を判断する第 1 の判断部を備え、

前記送信部は、

前記子局機器の数が前記 N 未満であると判断される前記第 1 の場合に、前記第 1 の無線設定を前記第 2 の通信装置に送信し、

前記子局機器の数が前記 N であると判断される前記第 2 の場合に、前記第 2 の無線設定を前記第 2 の通信装置に送信する、請求項 1 又は 2 に記載の第 1 の通信装置。

【請求項 4】

前記第 1 の通信装置は、さらに、

前記第 1 の通信装置が前記第 1 種の無線ネットワークに現在属していない場合に、前記第 1 の通信装置が前記親局状態で動作するための前記第 1 種の無線ネットワークを新たに形成する形成部を備え、

前記送信部は、前記第 1 種の無線ネットワークが新たに形成される前記第 1 の場合に、前記第 1 の無線設定を前記第 2 の通信装置に送信する、請求項 1 から 3 のいずれか一項に記載の第 1 の通信装置。

【請求項 5】

前記送信部は、

前記第 1 の通信装置が前記子局状態で動作して前記第 1 種の無線ネットワークに現在属している前記第 2 の場合に、前記第 2 の無線設定を前記第 2 の通信装置に送信する、請求項 1 から 4 のいずれか一項に記載の第 1 の通信装置。

10

【請求項 6】

前記第 1 の通信装置は、さらに、

前記第 2 の場合に、前記第 1 の通信装置が前記第 2 種の無線ネットワークに現在属しているのか否かを判断する第 2 の判断部と、

前記第 2 の場合において、前記第 1 の通信装置が前記第 2 種の無線ネットワークに現在属していないと判断される場合に、前記第 1 の通信装置の周辺に存在する中継装置を検索する検索部と、を備え、

前記送信部は、

前記第 2 の場合において、前記第 1 の通信装置が前記第 2 種の無線ネットワークに現在属していると判断される場合に、前記第 2 の通信装置が、前記第 1 の通信装置が現在属している前記第 2 種の無線ネットワークに参加するための前記第 2 の無線設定を、前記第 2 の通信装置に送信し、

20

前記第 2 の場合において、前記第 1 の通信装置が前記第 2 種の無線ネットワークに現在属していないと判断される場合に、前記第 2 の通信装置が、前記検索によって見つかった 1 個以上の中継装置のうちの前記特定の中継装置を含む前記第 2 種の無線ネットワークに参加するための前記第 2 の無線設定を、前記第 2 の通信装置に送信する、請求項 1 から 5 のいずれか一項に記載の第 1 の通信装置。

【請求項 7】

前記第 1 の通信装置は、さらに、

前記検索によって複数個の中継装置が見つかった場合に、前記対象データの処理に関する処理関係情報を用いて、前記複数個の中継装置の中から、前記特定の中継装置を選択する選択部を備える、請求項 6 に記載の第 1 の通信装置。

30

【請求項 8】

前記検索部は、前記複数個の中継装置のそれぞれから通信関係情報を取得し、

前記複数個の中継装置から取得される複数個の通信関係情報のそれぞれは、

当該通信関係情報の取得元の中継装置が現在利用している認証方式を示す認証方式情報と、

当該通信関係情報の取得元の中継装置が現在利用している暗号化方式を示す暗号化方式情報と、

40

当該通信関係情報の取得元の中継装置を利用した無線通信の通信速度を示す通信速度情報と、

のうちの少なくとも 1 個の情報を含み、

前記選択部は、前記処理関係情報と、前記複数個の通信関係情報と、を用いて、前記複数個の中継装置の中から、前記特定の中継装置を選択する、請求項 7 に記載の第 1 の通信装置。

【請求項 9】

前記選択部は、前記対象データに関するデータ関係情報を含む前記処理関係情報と、前記複数個の通信関係情報と、を用いて、前記特定の中継装置を選択する、請求項 8 に記載の第 1 の通信装置。

50

【請求項 10】

前記対象データは、前記第2の通信装置から前記第1の通信装置に送信されるべきデータであり、

前記第1の通信装置は、さらに、

前記第2の通信装置から前記データ関係情報を受信する受信部を備え、

前記選択部は、受信済みの前記データ関係情報を含む前記処理関係情報と、前記複数個の通信関係情報と、を用いて、前記特定の中継装置を選択する、請求項9に記載の第1の通信装置。

【請求項 11】

前記複数個の通信関係情報のそれぞれは、当該通信関係情報の取得元の中継装置が現在利用している認証方式を示す認証方式情報を含み、

10

前記選択部は、

前記データ関係情報が、前記対象データのセキュリティが比較的に高いことを示す場合には、前記複数個の中継装置の中から、第1の認証方式を現在利用している前記特定の中継装置を選択し、

前記データ関係情報が、前記対象データのセキュリティが比較的に低いことを示す場合には、前記複数個の中継装置の中から、前記第1の認証方式とは異なる第2の認証方式を現在利用している前記特定の中継装置を選択する、請求項9又は10に記載の第1の通信装置。

【請求項 12】

20

前記複数個の通信関係情報のそれぞれは、当該通信関係情報の取得元の中継装置が現在利用している暗号化方式を示す暗号化方式情報を含み、

前記選択部は、

前記データ関係情報が、前記対象データのセキュリティが比較的に高いことを示す場合には、前記複数個の中継装置の中から、第1の暗号化方式を現在利用している前記特定の中継装置を選択し、

前記データ関係情報が、前記対象データのセキュリティが比較的に低いことを示す場合には、前記複数個の中継装置の中から、前記第1の暗号化方式とは異なる第2の暗号化方式を現在利用している前記特定の中継装置を選択する、請求項9又は10に記載の第1の通信装置。

30

【請求項 13】

親局状態又は子局状態で動作して、第1種の無線ネットワークに属することが可能な第1の通信装置のためのコンピュータプログラムであって、

前記第1の通信装置に搭載されるコンピュータに、以下の各処理、即ち、

前記第2の通信装置が、中継装置を介さない直接無線通信を前記第1の通信装置と実行するための特定の態様で、前記第1種の無線ネットワークに参加することが可能である第1の場合に、前記第2の通信装置が前記第1種の無線ネットワークに参加するための第1の無線設定を、前記第2の通信装置に送信し、

前記第2の通信装置が、前記特定の態様で前記第1種の無線ネットワークに参加することが可能でない第2の場合に、前記第2の通信装置が第2種の無線ネットワークに参加するための第2の無線設定を、前記第2の通信装置に送信する送信処理であって、

40

前記第2種の無線ネットワークは、前記第1の通信装置及び前記第2の通信装置とは別体に構成されている特定の中継装置を含む無線ネットワークである、前記送信処理と、

前記第1の場合に、前記第1種の無線ネットワークを利用して、前記第2の通信装置と対象データの直接無線通信を実行し、

前記第2の場合に、前記第2種の無線ネットワークを利用して、前記特定の中継装置を介して、前記第2の通信装置と前記対象データの無線通信を実行する通信実行処理と、

を実行させる、コンピュータプログラム。

【発明の詳細な説明】

【技術分野】

50

【 0 0 0 1 】

本明細書によって開示される技術は、第2の通信装置と対象データの無線通信を実行するための第1の通信装置に関する。

【 背景技術 】

【 0 0 0 2 】

特許文献1には、データを送信する側の無線通信装置であるイニシエータと、当該データを受信する側の無線通信装置であるターゲットと、を備えるシステムが開示されている。イニシエータは、ターゲットに送信予定のデータのサイズが閾値以下である場合には、NFCを利用して、当該データをターゲットに送信する。一方において、イニシエータは、ターゲットに送信予定のデータのサイズが閾値よりも大きい場合には、通信方式をNFCからBluetooth（登録商標）にハンドオーバーし、Bluetooth（登録商標）を利用して、データをターゲットに送信する。

10

【 先行技術文献 】

【 特許文献 】

【 0 0 0 3 】

【 特許文献1 】 特開2010-178002号公報

【 発明の概要 】

【 発明が解決しようとする課題 】

【 0 0 0 4 】

本明細書では、第2の通信装置と対象データの無線通信を適切に実行し得る第1の通信装置を開示する。

20

【 課題を解決するための手段 】

【 0 0 0 5 】

本明細書によって開示される技術は、親局状態又は子局状態で動作して、第1種の無線ネットワークに属することが可能な第1の通信装置である。第1の通信装置は、送信部と、通信実行部と、を備える。送信部は、第2の通信装置が、中継装置を介さない直接無線通信を第1の通信装置と実行するための特定の態様で、第1種の無線ネットワークに参加することが可能である第1の場合に、第2の通信装置が第1種の無線ネットワークに参加するための第1の無線設定を、第2の通信装置に送信する。送信部は、第2の通信装置が、特定の態様で第1種の無線ネットワークに参加することが可能でない第2の場合に、第2の通信装置が第2種の無線ネットワークに参加するための第2の無線設定を、第2の通信装置に送信する。第2種の無線ネットワークは、第1の通信装置及び第2の通信装置とは別体に構成されている特定の中継装置を含む無線ネットワークである。通信実行部は、第1の場合に、第1種の無線ネットワークを利用して、第2の通信装置と対象データの直接無線通信を実行し、第2の場合に、第2種の無線ネットワークを利用して、特定の中継装置を介して、第2の通信装置と対象データの無線通信を実行する。

30

【 0 0 0 6 】

上記の構成によると、第1の通信装置は、第2の通信装置が特定の態様で第1種の無線ネットワークに参加することが可能であるのか否かに応じて、第1又は第2の無線設定を第2の通信装置に適切に送信し得る。このために、第1の通信装置は、第1種又は第2種の無線ネットワークに第2の通信装置を適切に参加させ得る。この結果、第1の通信装置は、第1種又は第2種の無線ネットワークを利用して、第2の通信装置と対象データの無線通信を適切に実行し得る。

40

【 0 0 0 7 】

第1の通信装置は、さらに、第2の通信装置と無線通信を実行するための第1種のインターフェースと、第2の通信装置と無線通信を実行するための第2種のインターフェースと、を備えていてもよい。第2種のインターフェースを介した無線通信の通信速度は、第1種のインターフェースを介した無線通信の通信速度よりも速くてもよい。送信部は、第1の場合に、第1種のインターフェースを介して、第1の無線設定を第2の通信装置に送信し、第2の場合に、第1種のインターフェースを介して、第2の無線設定を第2の通信

50

装置に送信してもよい。第1種及び第2種の無線ネットワークのそれぞれは、第2種のインターフェースを介した無線通信を実行するための無線ネットワークであってもよい。この構成によると、第1の通信装置は、第1種のインターフェースを利用して、第1又は第2の無線設定を第2の通信装置に適切に送信し得る。また、第1の通信装置は、第2種のインターフェースを利用して、第2の通信装置と対象データの無線通信を適切に実行し得る。

【0008】

第1の通信装置が親局状態で動作して第1種の無線ネットワークに属する場合に、第1種の無線ネットワークに属することが可能な子局機器の最大数は、 N （前記 N は1以上の整数）であってもよい。子局機器は、子局状態で動作して第1種の無線ネットワークに属する機器であってもよい。第1の通信装置は、さらに、第1の通信装置が親局状態で動作して第1種の無線ネットワークに現在属している場合に、第1種の無線ネットワークに現在属している子局機器の数が、 N 未満であるのか、 N であるのか、を判断する第1の判断部を備えていてもよい。送信部は、子局機器の数が N 未満であると判断される第1の場合に、第1の無線設定を第2の通信装置に送信し、子局機器の数が N であると判断される第2の場合に、第2の無線設定を第2の通信装置に送信してもよい。この構成によると、第1の通信装置は、子局機器の数が、 N 未満であるのか、 N であるのか、に応じて、第1種又は第2種の無線ネットワークに第2の通信装置を適切に参加させ得る。

10

【0009】

第1の通信装置は、さらに、第1の通信装置が第1種の無線ネットワークに現在属していない場合に、第1の通信装置が親局状態で動作するための第1種の無線ネットワークを新たに形成する形成部を備えていてもよい。送信部は、第1種の無線ネットワークが新たに形成される第1の場合に、第1の無線設定を第2の通信装置に送信してもよい。この構成によると、第1の通信装置は、第1の通信装置が親局状態で動作するための第1種の無線ネットワークを新たに形成して、第1種の無線ネットワークに第2の通信装置を適切に参加させ得る。

20

【0010】

送信部は、第1の通信装置が子局状態で動作して第1種の無線ネットワークに現在属している第2の場合に、第2の無線設定を第2の通信装置に送信してもよい。この構成によると、第1の通信装置は、第1の通信装置が子局状態で動作して第1種の無線ネットワークに現在属している第2の場合に、第2種の無線ネットワークに第2の通信装置を適切に参加させ得る。

30

【0011】

第1の通信装置は、さらに、第2の場合に、第1の通信装置が第2種の無線ネットワークに現在属しているのか否かを判断する第2の判断部と、第2の場合において、第1の通信装置が第2種の無線ネットワークに現在属していないと判断される場合に、第1の通信装置の周辺に存在する中継装置を検索する検索部と、を備えていてもよい。送信部は、第2の場合において、第1の通信装置が第2種の無線ネットワークに現在属していると判断される場合に、第2の通信装置が、第1の通信装置が現在属している第2種の無線ネットワークに参加するための第2の無線設定を、第2の通信装置に送信してもよい。送信部は、第2の場合において、第1の通信装置が第2種の無線ネットワークに現在属していないと判断される場合に、第2の通信装置が、検索によって見つかった1個以上の中継装置のうち特定のの中継装置を含む第2種の無線ネットワークに参加するための第2の無線設定を、第2の通信装置に送信してもよい。この構成によると、第1の通信装置は、第2の場合に、第2種の無線ネットワークに現在属しているのか否かに応じて、適切な処理を実行することができ、この結果、第2種の無線ネットワークに第2の通信装置を適切に参加させ得る。

40

【0012】

第1の通信装置は、さらに、検索によって複数個の中継装置が見つかった場合に、対象データの処理に係る処理関係情報を用いて、複数個の中継装置の中から、特定のの中継

50

装置を選択する選択部を備えていてもよい。この構成によると、第1の通信装置は、処理関係情報を用いて、適切な中継装置を選択し得る。

【0013】

検索部は、複数個の中継装置のそれぞれから通信関係情報を取得してもよい。複数個の中継装置から取得される複数個の通信関係情報のそれぞれは、(A)当該通信関係情報の取得元の中継装置が現在利用している認証方式を示す認証方式情報と、(B)当該通信関係情報の取得元の中継装置が現在利用している暗号化方式を示す暗号化方式情報と、(C)当該通信関係情報の取得元の中継装置を利用した無線通信の通信速度を示す通信速度情報と、のうちの少なくとも1個の情報を含んでいてもよい。選択部は、処理関係情報と、複数個の通信関係情報と、を用いて、複数個の中継装置の中から、特定の中継装置を選択してもよい。この構成によると、第1の通信装置は、処理関係情報と、複数個の通信関係情報と、を用いて、適切な中継装置を選択し得る。

10

【0014】

選択部は、対象データに関するデータ関係情報を含む処理関係情報と、複数個の通信関係情報と、を用いて、特定の中継装置を選択してもよい。この構成によると、第1の通信装置は、データ関係情報を用いて、適切な中継装置を選択し得る。

【0015】

対象データは、第2の通信装置から第1の通信装置に送信されるべきデータであってもよい。第1の通信装置は、さらに、第2の通信装置からデータ関係情報を受信する受信部を備えていてもよい。選択部は、受信済みのデータ関係情報を含む処理関係情報と、複数個の通信関係情報と、を用いて、特定の中継装置を選択してもよい。この構成によると、第1の通信装置は、第2の通信装置から受信されるデータ関係情報を用いて、適切な中継装置を選択し得る。

20

【0016】

複数個の通信関係情報のそれぞれは、当該通信関係情報の取得元の中継装置が現在利用している認証方式を示す認証方式情報を含んでいてもよい。選択部は、データ関係情報が、対象データのセキュリティが比較的高いことを示す場合には、複数個の中継装置の中から、第1の認証方式を現在利用している特定の中継装置を選択し、データ関係情報が、対象データのセキュリティが比較的低いことを示す場合には、複数個の中継装置の中から、第1の認証方式とは異なる第2の認証方式を現在利用している特定の中継装置を選択してもよい。この構成によると、第1の通信装置は、対象データのセキュリティに応じて、適切な中継装置を選択し得る。

30

【0017】

複数個の通信関係情報のそれぞれは、当該通信関係情報の取得元の中継装置が現在利用している暗号化方式を示す暗号化方式情報を含んでいてもよい。選択部は、データ関係情報が、対象データのセキュリティが比較的高いことを示す場合には、複数個の中継装置の中から、第1の暗号化方式を現在利用している特定の中継装置を選択し、データ関係情報が、対象データのセキュリティが比較的低いことを示す場合には、複数個の中継装置の中から、第1の暗号化方式とは異なる第2の暗号化方式を現在利用している特定の中継装置を選択してもよい。この構成によると、第1の通信装置は、対象データのセキュリティに応じて、適切な中継装置を選択し得る。

40

【0018】

選択部は、データ関係情報が、対象データの出力を許可するためのパスワードを含む場合には、対象データのセキュリティが比較的高いと判断し、データ関係情報が、パスワードを含まない場合には、対象データのセキュリティが比較的低いと判断してもよい。この構成によると、第1の通信装置は、対象データのセキュリティの高低を適切に判断し得る。

【0019】

複数個の通信関係情報のそれぞれは、当該通信関係情報の取得元の中継装置を利用した無線通信の通信速度を示す通信速度情報を含んでいてもよい。選択部は、データ関係情報

50

が、対象データのデータサイズが比較的に大きいことを示す場合には、複数個の中継装置の中から、比較的に大きい通信速度を実現する特定の中継装置を選択し、データ関係情報が、対象データのデータサイズが比較的に小さいことを示す場合には、複数個の中継装置の中から、比較的に小さい通信速度を実現する特定の中継装置を選択してもよい。この構成によると、第1の通信装置は、対象データのデータサイズに応じて、適切な中継装置を選択し得る。

【0020】

複数個の通信関係情報のそれぞれは、当該通信関係情報の取得元の中継装置を利用した無線通信の通信速度を示す通信速度情報を含んでいてもよい。選択部は、データ関係情報が、対象データが第1のデータ形式を有することを示す場合には、複数個の中継装置の中から、比較的に大きい通信速度を実現する特定の中継装置を選択し、データ関係情報が、対象データが第1のデータ形式とは異なる第2のデータ形式を有することを示す場合には、複数個の中継装置の中から、比較的に小さい通信速度を実現する特定の中継装置を選択してもよい。この構成によると、第1の通信装置は、対象データのデータ形式に応じて、適切な中継装置を選択し得る。

10

【0021】

選択部は、第1の通信装置が対象データを処理するための能力に関する第1の能力関係情報及び第2の通信装置が対象データを処理するための能力に関する第2の能力関係情報のうちの少なくとも一方の能力関係情報を含む処理関係情報と、複数個の通信関係情報と、を用いて、特定の中継装置を選択してもよい。この構成によると、第1の通信装置は、能力関係情報を用いて、適切な中継装置を選択し得る。

20

【0022】

第1の通信装置は、さらに、第1の通信装置の現在の状態をチェックすることによって、第1の能力関係情報を取得する能力取得部を備えていてもよい。選択部は、取得済みの第1の能力関係情報を含む処理関係情報と、複数個の通信関係情報と、を用いて、特定の中継装置を選択してもよい。この構成によると、第1の通信装置は、第1の通信装置の能力に関する第1の能力関係情報を用いて、適切な中継装置を選択し得る。

【0023】

第1の通信装置は、さらに、第2の通信装置から第2の能力関係情報を受信する受信部を備えていてもよい。選択部は、受信済みの第2の能力関係情報を含む処理関係情報と、複数個の通信関係情報と、を用いて、特定の中継装置を選択してもよい。この構成によると、第1の通信装置は、第2の通信装置の能力に関する第2の能力関係情報を用いて、適切な中継装置を選択し得る。

30

【0024】

複数個の通信関係情報のそれぞれは、当該通信関係情報の取得元の中継装置を利用した無線通信の通信速度を示す通信速度情報を含んでいてもよい。選択部は、少なくとも一方の能力関係情報が、対象データを処理するための能力が比較的に高いことを示す場合には、複数個の中継装置の中から、比較的に大きい通信速度を実現する特定の中継装置を選択し、少なくとも一方の能力関係情報が、対象データを処理するための能力が比較的に低いことを示す場合には、複数個の中継装置の中から、比較的に小さい通信速度を実現する特定の中継装置を選択してもよい。この構成によると、第1の通信装置は、対象データを処理するための能力に応じて、適切な中継装置を選択し得る。

40

【0025】

選択部は、少なくとも一方の能力関係情報が示す値が、所定の閾値以上である場合には、対象データを処理するための能力が比較的に高いと判断し、少なくとも一方の能力関係情報が示す値が、所定の閾値未満である場合には、対象データを処理するための能力が比較的に低いと判断してもよい。この構成によると、第1の通信装置は、対象データを処理するための能力の高低を適切に判断し得る。

【0026】

選択部は、対象データに関するデータ関係情報と、第1の通信装置が対象データを処

50

理するための能力に係る第1の能力関係情報及び第2の通信装置が対象データを処理するための能力に係る第2の能力関係情報のうちの少なくとも一方の能力関係情報と、を含む処理関係情報と、複数の通信関係情報と、を用いて、特定の中継装置を選択してもよい。この構成によると、第1の通信装置は、データ関係情報と能力関係情報とを用いて、適切な中継装置を選択し得る。

【0027】

上記の第1の通信装置を実現するための制御方法、コンピュータプログラム、及び、当該コンピュータプログラムを格納するコンピュータ読取可能記録媒体も、新規で有用である。また、上記の第1の通信装置と上記の第2の通信装置とを備える通信システムも、新規で有用である。

10

【図面の簡単な説明】

【0028】

【図1】通信システムの構成を示す。

【図2】携帯端末のアプリケーション処理のフローチャートを示す。

【図3】MFPの通信処理のフローチャートを示す。

【図4】MFP及び携帯端末が実行する通信及び処理を表わすシーケンス図を示す。

【図5】実施例1の概要を表わすテーブルを示す。

【図6】実施例2の概要を表わすテーブルを示す。

【図7】実施例3の概要を表わすテーブルを示す。

【図8】携帯端末のアプリケーション処理のフローチャートを示す。

20

【図9】MFPの通信処理のフローチャートを示す。

【図10】MFP及び携帯端末が実行する通信及び処理を表わすシーケンス図を示す。

【発明を実施するための形態】

【0029】

(実施例1)

(通信システム2の構成)

図1に示されるように、通信システム2は、複数のアクセスポイント(以下では「AP(Access Pointの略)」と呼ぶ)4a, 4bと、多機能機(以下では「MFP(Multi-Function Peripheralの略)」と呼ぶ)10と、携帯端末50と、を備える。なお、通信システム2に含まれるAPの個数は、2個に限定されず、3個以上であってもよい。

30

【0030】

(MFP10が実行可能な無線通信の種類)

MFP10は、NFC(Near Field Communicationの略)方式に従った無線通信と、WFD(Wi-Fi Directの略)方式に従った無線通信と、通常Wi-Fi方式に従った無線通信と、を実行可能である。以下では、上記の各方式に従った無線通信のことを、それぞれ、「NFC通信」、「WFD通信」、「通常Wi-Fi通信」と呼ぶ。

【0031】

(NFC通信)

NFC方式は、いわゆる近距離無線通信のための無線通信方式であり、例えば、ISO/IEC21481又は18092の国際標準規格に基づく無線通信方式である。MFP10は、携帯端末50とNFC通信を実行可能である。

40

【0032】

(WFD通信)

WFD方式は、Wi-Fi Allianceによって作成された規格書「Wi-Fi Peer-to-Peer(P2P) Technical Specification Version 1.1」に記述されている無線通信方式である。WFD方式は、例えば、IEEE(The Institute of Electrical and Electronics Engineers, Inc.の略)の802.11の規格、及び、それに準ずる規格(例えば、802.11a, 11b, 11g, 11n等)に従って、無線通信を実行するための無線通信方式である。

【0033】

50

MFP10は、WFDネットワークに属することによって、当該WFDネットワークに属する他の機器と対象データのWFD通信を実行することができる。対象データは、OSI参照モデルのネットワーク層の情報を含むデータであり、例えば、印刷データ、スキャンデータ等を含む。

【0034】

以下では、MFP10のように、WFD通信を実行可能な機器のことを「WFD対応機器」と呼ぶ。上記のWFDの規格書では、WFD対応機器の状態として、Group Owner状態（以下では「G/O状態」と呼ぶ）、クライアント状態、及び、デバイス状態の3つの状態が定義されている。WFD対応機器は、上記の3つの状態のうちの1つの状態を選択的に動作可能である。

10

【0035】

デバイス状態の一对のWFD対応機器がWFDネットワークを形成すべき際に、通常、当該一对のWFD対応機器の間で、G/Oネゴシエーションと呼ばれる無線通信が実行される。G/Oネゴシエーションにおいて、当該一对のWFD対応機器のうち的一方がG/O状態になると共に、当該一对のWFD対応機器のうち他方がクライアント状態になることが決定される。G/O状態の機器（以下では「G/O機器」と呼ぶ）と、クライアント状態の機器（以下では「クライアント機器」と呼ぶ）と、によって、WFDネットワークが形成される。WFDネットワークでは、1個のG/O機器と、1個以上のクライアント機器と、が存在し得る。G/O機器は、1個以上のクライアント機器を管理する。具体的に言うと、G/O機器は、1個以上のクライアント機器のそれぞれについて、当該クライアント機器の認証を実行し、当該クライアント機器の認証が成功すると、当該クライアント機器の識別情報（即ちMACアドレス）をG/O機器のメモリ内の管理リストに記述する。なお、本実施例では、MFP10が属するWFDネットワークにおいて、G/O機器（即ち、MFP10、又は、MFP10とは異なるG/O機器）は、認証方式「WPA2」と、暗号化方式「AES」と、を利用して、クライアント機器の認証を実行する。G/O機器は、クライアント機器がWFDネットワークから離脱すると、当該クライアント機器の識別情報を管理リストから消去する。

20

【0036】

G/O機器は、管理リストに登録されているクライアント機器と、対象データの無線通信を実行可能である。しかしながら、G/O機器は、管理リストに登録されていない未登録機器との間で、当該未登録機器がWFDネットワークに属するための特定データの無線通信を実行可能であるが、対象データの無線通信を実行不可能である。特定データは、OSI参照モデルのネットワーク層の情報を含まないデータであり、例えば、Probe Request信号（以下では「PReq信号」と呼ぶ）、Probe Response信号（以下では「Pres信号」と呼ぶ）等の物理層のデータを含む。なお、G/O機器は、複数個のクライアント機器の間の対象データの無線通信を中継可能である。

30

【0037】

WFDネットワークに属していないWFD対応機器（即ち、G/O機器の管理リストに登録されていない未登録機器）が、デバイス状態の機器である。デバイス状態の機器は、WFDネットワークに属するための上記の特定データの無線通信を、G/O機器と実行可能であるが、上記の対象データの無線通信を、G/O機器又はクライアント機器と実行不可能である。

40

【0038】

上述したように、WFDネットワークでは、一对のWFD対応機器は、これらのWFD対応機器とは別体に構成されているAPを介さずに、対象データのWFD通信を実行することができる。即ち、WFD通信は、APを介さない無線通信であると言える。

【0039】

なお、以下では、上記のWFDの規格書で定義されている3つの状態（即ち、G/O状態、クライアント状態、デバイス状態）のうちの1つの状態を選択的に動作可能ではないが、APを介した無線通信（即ち後述の通常Wi-Fi通信）を実行可能な機器のことを

50

、「WFD非対応機器」と呼ぶ。「WFD非対応機器」は、「レガシー機器」とも呼ばれる。G/O状態の機器は、WFD非対応機器の識別情報を、管理リストに記述することができる。この場合、WFD非対応機器は、クライアント機器として、WFDネットワークに参加することができる。本実施例では、携帯端末50は、WFD非対応機器（即ちレガシー機器）である。従って、MFP10がG/O状態である場合には、MFP10は、携帯端末50と対象データのWFD通信を実行可能である。

【0040】

（通常Wi-Fi通信）

通常Wi-Fi方式は、Wi-Fi Allianceによって定められた無線通信方式であって、WFD方式とは異なる無線通信方式である。通常Wi-Fi方式は、WFD方式と同様に、IEEEの802.11の規格、及び、それに準ずる規格（例えば、802.11a, 11b, 11g, 11n等）に従って、無線通信を実行するための無線通信方式である。ただし、上述したように、WFD方式は、APを介さない無線通信を実行するための無線通信方式である。これに対し、通常Wi-Fi方式は、APを介して無線通信を実行するための無線通信方式である。この点において、WFD方式と通常Wi-Fi方式とは異なる。

10

【0041】

MFP10は、通常Wi-Fiネットワークに属することによって、当該通常Wi-Fiネットワークに属する他の機器と、APを介して、対象データの通常Wi-Fi通信を実行することができる。本実施例では、携帯端末50は、WFD非対応機器（即ちレガシー機器）であるために、通常Wi-Fi通信を実行可能である。従って、MFP10は、複数個のAP4a, 4bのうちのいずれかのAPを介して、対象データの通常Wi-Fi通信を携帯端末50と実行可能である。

20

【0042】

本実施例では、通常Wi-Fi通信のための認証方式として、Open、WPA（Wi-Fi Protected Accessの略）、又は、WPA2のいずれかが利用される。これらの3種類の認証方式では、「Open」が最も低セキュリティの認証方式であり、「WPA」が「Open」より高セキュリティの認証方式であり、「WPA2」が「WPA」より高セキュリティの認証方式である。「Open」では、パスワードを利用した認証が実行されない。これに対し、「WPA」及び「WPA2」では、パスワードを利用した認証が実行される。

30

【0043】

また、本実施例では、通常Wi-Fi通信のための暗号化方式として、WEP（Wired Equivalent Privacy）、TKIP（Temporal Key Integrity Protocolの略）、又は、AES（Advanced Encryption Standardの略）が利用される。これらの3種類の暗号化方式では、「WEP」が最も低セキュリティの暗号化方式であり、「TKIP」が「WEP」より高セキュリティの暗号化方式であり、「AES」が「TKIP」より高セキュリティの暗号化方式である。

【0044】

通常Wi-Fiネットワークは、社内LAN、家庭内LAN等のように、APを設置可能な環境で構築される無線ネットワークであり、一般的に言うと、定常的に形成されるべき無線ネットワークである。これに対し、WFDネットワークは、APを必要としないために、例えば、一对のWFD対応機器の間で一時的な無線通信を実行させるために構築される無線ネットワークであり、一般的に言うと、一時的に形成されるべき無線ネットワークである。このように、本実施例では、通常Wi-Fiネットワークが、定常的に形成されるべき無線ネットワークであり、WFDネットワークが、一時的に形成されるべき無線ネットワークである状況を想定している。

40

【0045】

（MFP10の構成）

MFP10は、印刷機能及びスキャン機能を含む多機能を実行可能である。図1に示さ

50

れるように、MFP10は、操作部12と、表示部14と、印刷実行部16と、スキャン実行部18と、無線LANインターフェース（以下ではインターフェースのことを「I/F」と記載する）20と、NFC I/F22と、制御部30と、を備える。各部12～30は、バス線（符号省略）に接続されている。

【0046】

操作部12は、複数のキーを備える。ユーザは、操作部12を操作することによって、様々な指示をMFP10に入力することができる。表示部14は、様々な情報を表示するためのディスプレイである。印刷実行部16は、インクジェット方式、レーザ方式等の印刷機構である。スキャン実行部18は、CCD、CIS等のスキャン機構である。

【0047】

無線LAN I/F20は、WFD通信及び通常Wi-Fi通信を実行するためのインターフェースである。無線LAN I/F20は、物理的には1個のインターフェース（即ち1個のICチップ）である。但し、無線LAN I/F20には、WFD通信で利用されるMACアドレス（以下では「WFD用MACアドレス」と呼ぶ）と、通常Wi-Fi通信で利用されるMACアドレス（以下では「通常Wi-Fi用MACアドレス」と呼ぶ）と、の両方が割り当てられる。具体的に言うと、無線LAN I/F20には、通常Wi-Fi用MACアドレスが、予め割り当てられている。制御部30は、通常Wi-Fi用MACアドレスを用いて、通常Wi-Fi用MACアドレスとは異なるWFD用MACアドレスを生成して、WFD用MACアドレスを無線LAN I/F20に割り当てる。従って、制御部30は、通常Wi-Fi用MACアドレスを利用した通常Wi-Fi通信と、WFD用MACアドレスを利用したWFD通信と、の両方を同時的に実行し得る。即ち、MFP10は、WFDネットワークと通常Wi-Fiネットワークとの両方に同時的に属することができる。

【0048】

MFP10によって利用されるMACアドレスという観点では、WFD通信及び通常Wi-Fi通信は、例えば、以下のように表現することができる。即ち、WFD通信は、MFP10のWFD用MACアドレスが利用される無線通信であり、通常Wi-Fi通信は、MFP10の通常Wi-Fi用MACアドレスが利用される無線通信である。また、WFDネットワークは、MFP10のWFD用MACアドレスが利用される無線ネットワークであり、通常Wi-Fiネットワークは、MFP10の通常Wi-Fi用MACアドレスが利用される無線ネットワークである。

【0049】

NFC I/F22は、NFC通信を実行するためのインターフェースである。NFC I/F22を構成するチップと、無線LAN I/F20を構成するチップとは、物理的に異なる。

【0050】

無線LAN I/F20を介した無線通信の通信速度（例えば、最大の通信速度が11～600Mbps）は、NFC I/F22を介した無線通信の通信速度（例えば、最大の通信速度が100～424Kbps）よりも速い。また、無線LAN I/F20を介した無線通信における搬送波の周波数（例えば、2.4GHz帯、5.0GHz帯）は、NFC I/F22を介した無線通信における搬送波の周波数（例えば、13.56MHz帯）とは異なる。また、例えば、MFP10と携帯端末50との距離が約10cm以下である場合に、制御部30は、NFC I/F22を介して、携帯端末50とNFC通信を実行可能である。一方において、MFP10と携帯端末50との距離が、10cm以下である場合でも、10cm以上である場合（例えば最大で約100m）でも、制御部30は、無線LAN I/F20を介して、携帯端末50とWFD通信及び通常Wi-Fi通信を実行可能である。即ち、MFP10が無線LAN I/F20を介して通信先の機器（例えば携帯端末50）と無線通信を実行可能な最大の距離は、MFP10がNFC I/F22を介して通信先の機器と無線通信を実行可能な最大の距離よりも大きい。

【0051】

10

20

30

40

50

制御部 30 は、CPU 32 とメモリ 34 とを備える。CPU 32 は、メモリ 34 に格納されているプログラムに従って、様々な処理を実行する。CPU 32 がプログラムに従って処理を実行することによって、各部 41 ~ 49 の機能が実現される。メモリ 34 は、ROM、RAM、ハードディスク等によって構成される。メモリ 34 は、CPU 32 によって実行される上記のプログラムを格納する。

【0052】

メモリ 34 は、さらに、WFD に関する MFP 10 の現在の状態（即ち、G/O 状態、クライアント状態、及び、デバイス状態のいずれかの状態）を示す WFD 状態値を格納する。MFP 10 が WFD ネットワークに属している場合（即ち、WFD 状態値が G/O 状態又はクライアント状態を示す場合）には、メモリ 34 は、さらに、WFD 通信を実行するための WFD 無線設定を格納する。

10

【0053】

WFD 無線設定は、認証方式情報、暗号化方式情報、パスワード、SSID (Service Set Identifier)、及び、BSSID (Basic Service Set Identifier) を含む。WFD 無線設定に含まれる SSID は、WFD ネットワークを識別するためのネットワーク識別子である。WFD 無線設定に含まれる BSSID は、WFD ネットワークの G/O 機器に割り当てられている固有の識別子（例えば G/O 機器の MAC アドレス）である。

【0054】

G/O 機器は、通常、WFD ネットワークを形成する際に、WFD 無線設定を準備して、当該 WFD 無線設定をクライアント機器に供給する。例えば、MFP 10 の制御部 30 は、MFP 10 が G/O 状態で動作して WFD ネットワークを形成する際に、WFD 無線設定を準備する。具体的に言うと、制御部 30 は、予め決められている認証方式情報（即ち「WPA2」）及び暗号化方式情報（即ち「AES」）を準備する。制御部 30 は、予め決められているパスワードを準備するか、あるいは、パスワードを新たに生成することによってパスワードを準備する。制御部 30 は、予め決められている SSID を準備するか、あるいは、SSID を新たに生成することによって SSID を準備する。また、制御部 30 は、予め決められている WFD 用 MAC アドレスを BSSID として準備する。

20

【0055】

従って、MFP 10 が G/O 状態で動作して WFD ネットワークに属している場合には、メモリ 34 は、MFP 10 が当該 WFD ネットワークを形成した際に、MFP 10 によって準備された WFD 無線設定を格納する。一方において、MFP 10 がクライアント状態で動作して WFD ネットワークに属している場合には、メモリ 34 は、MFP 10 とは異なる G/O 機器が当該 WFD ネットワークを形成した際に、当該 G/O 機器によって準備された WFD 無線設定（即ち、当該 G/O 機器から取得された WFD 無線設定）を格納する。

30

【0056】

また、MFP 10 が通常 Wi-Fi ネットワークに属している場合には、メモリ 34 は、さらに、通常 Wi-Fi 通信を実行するための通常 Wi-Fi 無線設定を格納する。通常 Wi-Fi 無線設定は、通常、認証方式情報、暗号化方式情報、SSID、BSSID、及び、パスワードを含む。通常 Wi-Fi 無線設定に含まれる SSID は、通常 Wi-Fi ネットワークを識別するためのネットワーク識別子である。通常 Wi-Fi 無線設定情報に含まれる BSSID は、通常 Wi-Fi ネットワークを形成している AP に割り当てられている固有の識別子（例えば AP の MAC アドレス）である。

40

【0057】

MFP 10 が通常 Wi-Fi ネットワークに参加するための手法としては、MFP 10 のユーザが所定の操作を操作部 12 に加える第 1 の手法と、後述の図 3 の S42 ~ S48 を実行する第 2 の手法と、が存在する。

【0058】

第 1 の手法では、MFP 10 は、上記の所定の操作が操作部 12 に加えられると、SSID サーチを実行する。この結果、MFP 10 は、MFP 10 の周囲に存在する AP 4a

50

、4 bのそれぞれから、当該APで現在利用されている認証方式を示す認証方式情報と、当該APで現在利用されている暗号化方式を示す暗号化方式情報と、当該APで現在利用されているSSID及びBSSIDと、を取得する。次いで、MFP10は、複数のAPから取得された複数のSSIDを、表示部14に表示させる。ユーザは、操作部12を用いて、複数のSSIDの中から1個のSSID（即ち1個のAP）を選択する。

【0059】

上述したように、認証方式「WPA」又は「WPA2」を採用している高セキュリティの通常Wi-Fiネットワークでは、パスワードを利用した認証が実行される。従って、選択済みのAPが、認証方式「WPA」又は「WPA2」を利用している場合には、ユーザは、操作部12を用いて、さらに、パスワードを入力する。MFP10は、選択済みのAPから取得された認証方式情報、暗号化方式情報、SSID、及び、BSSIDを利用すると共に、ユーザによって入力されたパスワードを利用して、選択済みのAPと無線接続を実行する。無線接続は、MFP10が通常Wi-Fiネットワークに参加するための通信処理（例えば、認証のための通信処理（Authentication信号、Association Request信号、Association Response信号の通信等））を含む。これにより、MFP10は、選択済みのAPが形成している通常Wi-Fiネットワークに参加する。

10

【0060】

一方において、認証方式「Open」を採用している低セキュリティの通常Wi-Fiネットワークでは、パスワードを利用した認証が実行されない。従って、選択済みのAPが、認証方式「Open」を利用している場合には、ユーザは、パスワードを入力しない。MFP10は、選択済みのAPから取得された認証方式情報、暗号化方式情報、SSID、及び、BSSIDを利用して、選択済みのAPと無線接続を実行し、選択済みのAPが形成している通常Wi-Fiネットワークに参加する。メモリ34は、選択済みのAPとの無線接続で利用された各情報（認証方式情報等）を、通常Wi-Fi無線設定として格納する。

20

【0061】

メモリ34は、さらに、MFP10が上記の第1の手法によって通常Wi-Fiネットワークに参加する毎に、当該通常Wi-Fiネットワークを識別するためのSSIDと、当該通常Wi-Fiネットワークで利用されているパスワードと、が対応づけられている参加情報を格納する。即ち、メモリ34は、MFP10が過去に参加した1個以上の通常Wi-Fiネットワークに対応する1個以上の参加情報を累積的に格納する。なお、上述したように、認証方式「Open」を採用している通常Wi-Fiネットワークでは、パスワードが利用されない。従って、このような通常Wi-Fiネットワークに対応する参加情報は、SSIDを含むが、パスワードを含まない。

30

【0062】

後で詳しく説明するが、上記の第2の手法でも、MFP10は、SSIDサーチを実行する（図3のS42）。次いで、MFP10は、ユーザの指示を受けずに、1個のSSID（即ち1個のAP）を自動的に選択する（S44）。次いで、MFP10は、選択済みのAPと無線接続を実行する（S48）。これにより、MFP10は、選択済みのAPが形成している通常Wi-Fiネットワークに自動的に参加する。

40

【0063】

（携帯端末50の構成）

携帯端末50は、例えば、携帯電話（例えばスマートフォン）、PDA、ノートPC、タブレットPC、携帯型音楽再生装置、携帯型動画再生装置等の可搬型の端末装置である。携帯端末50は、NFC通信と通常Wi-Fi通信とを実行可能である。

【0064】

携帯端末50は、操作部52と、表示部54と、無線LANI/F60と、NFCI/F62と、制御部70と、を備える。各部52～70は、バス線（符号省略）に接続されている。操作部52は、複数のキーを備える。ユーザは、操作部52を操作することによって、様々な指示を携帯端末50に入力することができる。表示部54は、様々な情報を

50

表示するためのディスプレイである。

【0065】

無線LAN I / F 60は、通常Wi-Fi通信を実行するためのインターフェースである。NFC I / F 62は、NFC通信を実行するためのインターフェースである。これらのインターフェース60, 62の相違は、MFP 10のインターフェース20, 22の相違と同様である。即ち、例えば、無線LAN I / F 60を介した無線通信の通信速度は、NFC I / F 62を介した無線通信の通信速度よりも速い。

【0066】

制御部70は、CPU 72とメモリ74とを備える。CPU 72は、メモリ74に格納されているプログラムに従って、様々な処理を実行する。メモリ74内のプログラムは、MFP 10に様々な機能(例えば印刷機能、スキャン機能等)を実行させるためのアプリケーション76を含む。アプリケーション76は、例えば、MFP 10のベンダによって提供されるサーバから携帯端末50にインストールされてもよいし、MFP 10と共に出荷されるメディアから携帯端末50にインストールされてもよい。CPU 72がアプリケーション76に従って処理を実行することによって、各部81~86の機能が実現される。なお、各部81~86は、後述の第4~第6実施例で機能する。

10

【0067】

(AP 4a, 4bの構成)

AP 4a, 4bのそれぞれは、WFDのG/O機器ではなく、無線アクセスポイント又は無線LANルータと呼ばれる通常のAPであり、通常Wi-Fiネットワークを形成する。AP 4a, 4bは、通常Wi-Fiネットワークに属する複数の機器のうちの第1の機器(例えば携帯端末50)から対象データを受信して、上記の複数の機器のうちの第2の機器(例えばMFP 10)に当該対象データを送信する。即ち、AP 4a, 4bは、通常Wi-Fiネットワークに属する一対の機器の間の対象データの無線通信を中継する中継装置として機能する。

20

【0068】

なお、WFDのG/O機器と通常のAP(即ちAP 4a, 4b)との間の相違点は、以下の通りである。即ち、WFDのG/O機器は、当該機器が属しているWFDネットワークから離脱して、他のWFDネットワークに新たに属する場合に、G/O状態とは異なる状態(即ちクライアント状態)で動作し得る。これに対し、通常のAPは、当該APがどの通常Wi-Fiネットワークを形成しても、一対の機器の間の無線通信を中継する機能を実行する。即ち、通常のAPは、WFDのG/O状態と同様の動作しか実行することができず、WFDのクライアント状態と同様の動作を実行することができない。

30

【0069】

(携帯端末50のアプリケーション処理; 図2)

続いて、図2を参照して、携帯端末50の制御部70がアプリケーション76に従って実行する処理の内容を説明する。携帯端末50のユーザは、携帯端末50に格納されている印刷対象のデータ(以下では「印刷データ」と呼ぶ)によって表わされる画像を、MFP 10に印刷させることを望む場合に、操作部52を操作して、アプリケーション76を起動させる。これにより、制御部70は、アプリケーション76に従って、図2のフローチャートを開始する。

40

【0070】

ユーザは、携帯端末50のメモリ74に格納されている印刷データを選択するための操作と、印刷データに対してパスワードを設定するの否かを選択するための操作と、を含む印刷操作を、操作部52に加える。この場合、制御部70は、S10でYESと判断して、S11に進む。

【0071】

なお、印刷データに対してパスワードが設定される場合には、ユーザが、MFP 10の操作部12を操作して、当該パスワードをMFP 10に入力しないと、MFP 10は、印刷データに従った印刷を開始しない。即ち、携帯端末50に印刷操作を加えたユーザのみ

50

が、MFP10が印刷することによって生成される印刷物を取得することができる。これに対し、印刷データに対してパスワードが設定されない場合には、MFP10は、印刷データを受信すると、ただちに印刷を開始する（即ち、MFP10にパスワードが入力されなくても印刷を開始する）。即ち、携帯端末50に印刷操作を加えたユーザ以外の第三者が、印刷物を取得し得る。従って、印刷データに対してパスワードが設定される場合は、印刷データに対してパスワードが設定されない場合と比較して、印刷データのセキュリティが高い。

【0072】

S11では、制御部70は、まず、印刷機能の実行をMFP10に指示するための印刷コマンドと、印刷データのセキュリティを示すセキュリティ情報と、を含むNFC情報を生成する。NFC情報は、印刷データを含まない。なお、制御部70は、印刷データに対してパスワードを設定することがユーザによって選択された場合には、セキュアを示すセキュリティ情報を生成する。この場合、セキュリティ情報は、さらに、印刷データに対して設定されるパスワードを含む。一方において、制御部70は、印刷データに対してパスワードを設定しないことがユーザによって選択された場合には、非セキュアを示すセキュリティ情報を生成する。この場合、セキュリティ情報は、パスワードを含まない。

10

【0073】

MFP10が電源ONにされている間に、MFP10のNFCI/F22は、NFC通信を実行可能な機器（即ち携帯端末50）を検出するための検出電波を発信している。携帯端末50のユーザは、上記の印刷操作を加えた後に、携帯端末50をMFP10に近づける。これにより、携帯端末50とMFP10との間の距離が、互いに電波が届く距離（例えば10cm）より小さくなる。この場合、携帯端末50は、MFP10から検出電波を受信して、応答電波をMFP10に送信する。この結果、MFP10と携帯端末50との間に、NFC通信セッションが確立される。S12では、制御部70は、NFC通信セッションを利用して、NFCI/F62を介して、生成済みのNFC情報をMFP10に送信する。

20

【0074】

携帯端末50からMFP10にNFC情報が送信されると、MFP10は、後述の図3のS30でYESと判断して、S32以降の処理を実行する。この結果、MFP10は、NFC通信セッションを利用して、WFD無線設定（図3のS40）又はAP情報（図3のS46）を携帯端末50に送信する。WFD無線設定は、G/O状態のMFP10が形成しているWFDネットワークで現在利用されている各情報（即ち、認証方式情報、暗号化方式情報、SSID、BSSID、及び、パスワード）を含む。AP情報は、APが形成している通常Wi-Fiネットワークで現在利用されている各情報（即ち、認証方式情報、暗号化方式情報、SSID、及び、BSSID）を含む。なお、当該通常Wi-Fiネットワークでパスワードを利用した認証が実行される場合、即ち、当該通常Wi-Fiネットワークで現在利用されている認証方式が「WPA」又は「WPA2」である場合には、AP情報は、さらに、当該通常Wi-Fiネットワークで現在利用されているパスワードを含む。一方において、当該通常Wi-Fiネットワークでパスワードを利用した認証が実行されない場合、即ち、当該通常Wi-Fiネットワークで現在利用されている認証方式が「Open」である場合には、AP情報は、パスワードを含まない。

30

40

【0075】

図2のS14では、携帯端末50の制御部70は、MFP10から、NFCI/F62を介して、WFD無線設定又はAP情報を受信する。なお、制御部70は、S14でWFD無線設定又はAP情報を受信した後に、例えば、携帯端末50から所定の音を出力させて、NFC通信が完了したことを携帯端末50のユーザに通知する。これにより、ユーザは、MFP10から携帯端末50を遠ざけてよいことを認識できる。S14を終えると、S16に進む。

【0076】

S16では、制御部70は、S14で受信された情報に応じた無線接続を実行する。S

50

14で受信された情報がWFD無線設定である場合には、制御部70は、受信済みのWFD無線設定を用いて、無線LANI/F60を介して、G/O状態のMFP10と無線接続を実行する。当該無線接続は、G/O状態のMFP10が形成している特定のWFDネットワークに参加するための通信処理（例えば、認証のための通信処理）を含む。これにより、携帯端末50は、クライアント機器として上記の特定のWFDネットワークに参加することができる。この結果、MFP10及び携帯端末50が同一のWFDネットワークに属することになる。

【0077】

一方において、S14で受信された情報がAP情報である場合には、制御部70は、受信済みのAP情報を用いて、無線LANI/F60を介して、APと無線接続を実行する。当該無線接続は、受信済みのAP情報に含まれるSSIDによって識別される特定の通常Wi-Fiネットワークに参加するための通信処理（例えば、認証のための通信処理）を含む。これにより、携帯端末50は、上記の特定の通常Wi-Fiネットワークに参加することができる。この結果、MFP10及び携帯端末50が同一の通常Wi-Fiネットワークに属することになる。

10

【0078】

なお、S16が実行される際に、携帯端末50が既にWFDネットワーク又は通常Wi-Fiネットワークに属している場合には、S16において、制御部70は、既存のネットワークから離脱して、上記の特定のWFDネットワーク又は特定の通常Wi-Fiネットワークに参加する。なお、制御部70は、上記の既存のネットワークから離脱する場合には、上記の既存のネットワークに再び参加するための無線設定（例えばSSID、パスワード等）をメモリ74に格納しておく。

20

【0079】

S16を終えると、S20において、制御部70は、無線LANI/F60を介して、印刷データをMFP10に送信する。例えば、携帯端末50が上記の特定のWFDネットワークに参加した場合には、S20では、制御部70は、上記の特定のWFDネットワークを利用して、G/O状態であるMFP10に印刷データを送信する。即ち、中継装置（例えばAP4a, 4b）が印刷データを中継しなくても、携帯端末50からMFP10に印刷データが直接的に送信される。また、例えば、携帯端末50が上記の特定の通常Wi-Fiネットワークに参加した場合には、S20では、制御部70は、上記の特定の通常Wi-Fiネットワークを利用して、AP（例えば4a）を介して、MFP10に印刷データを送信する。

30

【0080】

S20が終了すると、図2のアプリケーション処理が終了する。なお、S16において、携帯端末50が既存のネットワークから離脱した場合には、S20が終了すると、制御部70は、S16で参加した新たなネットワークから離脱して、S16でメモリ74に格納された無線設定を用いて、元のネットワークに再び参加する。一方において、S16において、携帯端末50が既存のネットワークから離脱しなかった場合には、S20が終了しても、制御部70は、上記の新たなネットワークに参加している状態を維持する。

40

【0081】

（MFP10の通信処理；図3）

続いて、図3を参照して、MFP10の制御部30が実行する処理の内容を説明する。上述したように、図2のS12において、携帯端末50からMFP10にNFC情報が送信される。MFP10の受信部41は、携帯端末50から、NFCI/F22を介して、NFC情報を受信する。この場合、受信部41は、図3のS30でYESと判断して、S32に進む。

【0082】

S32では、第1の判断部47は、MFP10の現在の状態がG/O状態であるのか否かを判断する（即ち、MFP10がG/O状態で動作してWFDネットワークに属しているのか否かを判断する）。メモリ34内のWFD状態値がG/O状態を示す場合には、第

50

1の判断部47は、S32でYESと判断して、S34に進む。一方において、メモリ34内のWFD状態値がクライアント状態又はデバイス状態を示す場合には、第1の判断部47は、S32でNOと判断して、S36に進む。

【0083】

S34では、第1の判断部47は、G/O状態のMFP10が形成しているWFDネットワークに属しているクライアント機器の数が、予め決められている最大値Nに一致するの否かを判断する。なお、Nは、1でもよいし、2以上の整数であってもよい。クライアント機器の数が最大値Nに一致する場合には、第1の判断部47は、S34でYESと判断して、S41に進む。一方において、クライアント機器の数が最大値未満である場合には、第1の判断部47は、S34でNOと判断して、S40に進む。

10

【0084】

S36では、第1の判断部47は、MFP10の現在の状態がクライアント状態であるの否かを判断する(即ち、MFP10がクライアント状態で動作してWFDネットワークに属しているの否かを判断する)。メモリ34内のWFD状態値がクライアント状態を示す場合には、第1の判断部47は、S36でYESと判断して、S41に進む。一方において、メモリ34内のWFD状態値がデバイス状態を示す場合、即ち、MFP10がWFDネットワークに属していない場合には、第1の判断部47は、S36でNOと判断して、S38に進む。

【0085】

S38では、形成部49は、MFP10を自律G/Oモードに移行させる。上述したように、WFDネットワークが新たに形成されるべき際には、通常、G/Oネゴシエーションが実行されて、G/O機器とクライアント機器とが決定される。これに対し、自律G/Oモードでは、G/Oネゴシエーションが実行されずに、MFP10がG/O状態になることが決定される。S38の段階では、MFP10がG/O機器であるが、クライアント機器が存在しない。即ち、形成部49は、G/O機器(即ちMFP10)のみが属しているWFDネットワークを形成する。自律G/Oモードは、G/O状態で動作することをMFP10に維持させるモードである。例えば、MFP10がG/OネゴシエーションでG/O状態になってWFDネットワークを形成した場合には、当該WFDネットワークからクライアント機器がいなくなると、MFP10は、G/O状態からデバイス状態に移行する(即ち、WFDネットワークが消滅する)。これに対し、例えば、MFP10が自律G/OモードでG/O状態になってWFDネットワークを形成した場合には、クライアント機器がいなくても、MFP10は、G/O状態を維持する(即ち、WFDネットワークを維持する)。

20

30

【0086】

S38では、形成部49は、さらに、WFDネットワークで利用されるべきWFD無線設定(即ち、認証方式情報、暗号化方式情報、SSID、BSSID、及び、パスワード)を準備する。形成部49がWFD無線設定を準備する手法は、上述のとおりである。S38では、形成部49は、さらに、G/O状態を示すWFD状態値と、準備済みのWFD無線設定と、をメモリ34に格納させる。S38を終えると、S40に進む。

【0087】

S40では、送信部42は、NFCI/F22を介して、メモリ34内のWFD無線設定を携帯端末50に送信する。上述したように、S40の処理は、S34でNOの場合、又は、S36でNOの場合(即ちS38を経た場合)に実行される。S34でNOの場合には、G/O状態のMFP10が形成しているWFDネットワークに属しているクライアント機器の数が、最大値未満である。従って、携帯端末50をクライアント機器としてWFDネットワークに参加させることができる。また、S36でNOの場合には、S38において、G/O状態のMFP10のみが属しているWFDネットワークが形成される。従って、携帯端末50をクライアント機器としてWFDネットワークに参加させることができる。S40では、携帯端末50をクライアント機器としてWFDネットワークに参加させるために、MFP10から携帯端末50にWFD無線設定が送信される。S40を終え

40

50

ると、S 5 0に進む。

【0088】

一方において、S 3 4でYESの場合、又は、S 3 6でYESの場合には、S 4 1が実行される。S 4 1では、第2の判断部48は、MFP10が通常Wi-Fiネットワークに現在参加しているのか否かを判断する。第2の判断部48は、メモリ34内に通常Wi-Fi無線設定が格納されている場合には、S 4 1でYESと判断してS 4 9に進み、メモリ34内に通常Wi-Fi無線設定が格納されていない場合には、S 4 1でNOと判断してS 4 2に進む。

【0089】

S 4 9では、送信部42は、MFP10が現在属している通常Wi-Fiネットワークに含まれるAP(即ち、MFP10との無線接続が確立されているAP)に関するAP情報を準備する。具体的に言うと、送信部42は、メモリ34内の通常Wi-Fi無線設定を含むAP情報を準備する。そして、送信部42は、NFCI/F22を介して、準備済みのAP情報を携帯端末50に送信する。これにより、携帯端末50は、AP情報を用いて、通常Wi-Fiネットワークに参加する(図2のS16)。この結果、MFP10及び携帯端末50が同一の通常Wi-Fiネットワークに属することになる。S 4 9が終了すると、S 5 0に進む。

【0090】

一方において、S 4 1でNOの場合には、S 4 2~48の各処理が実行される。S 3 4でYESの場合には、G/O状態のMFP10が形成しているWFDネットワークに属しているクライアント機器の数が、最大値Nに一致する。従って、携帯端末50をクライアント機器としてWFDネットワークに参加させることができない。また、S 3 6でYESの場合には、クライアント状態のMFP10が、G/O状態である他の機器が形成しているWFDネットワークに属している。この場合、MFP10は、当該WFDネットワークに他の機器(即ち携帯端末50)に参加させるための権限を有していない。従って、携帯端末50をクライアント機器としてWFDネットワークに参加させることができない。さらに、S 4 1でNOの場合には、MFP10が通常Wi-Fiネットワークに現在参加していない。このために、MFP10は、MFP10が現在参加している通常Wi-Fiネットワークに携帯端末50に参加させることもできない。このために、S 4 2~S 4 8では、制御部30は、MFP10及び携帯端末50を同一の通常Wi-Fiネットワークに参加させるための処理を実行する。

【0091】

上述したように、本実施例では、携帯端末50をWFDネットワークに参加させることができるのであれば(S 3 4でNO、S 3 6でNO)、携帯端末50をWFDネットワークに参加させるための処理を実行する(S 4 0)。これにより、一時的に形成されるべきWFDネットワークに携帯端末50に参加させることができる。この場合、通常Wi-Fi無線設定が携帯端末50に送信されないために、定常的に形成されるべき通常Wi-Fiネットワークのセキュリティが低下するのを抑制することができる。このような実情に鑑みて、本実施例では、携帯端末50をWFDネットワークに参加させることを優先し(S 3 2~S 4 0)、それが不可能であれば、携帯端末50を通常Wi-Fiネットワークに参加させる(S 4 1~S 4 9)。

【0092】

S 4 2では、通信取得部44は、SSIDサーチを実行して、MFP10の周囲に存在するAPを検索する。このようにAPを検索するために、「通信取得部」を「検索部」と呼んでもよい。通信取得部44は、無線LANI/F20を介して、Preq信号を送信する。MFP10の周囲に存在するAP4a, 4bのそれぞれは、MFP10からPreq信号を受信すると、Pres信号をMFP10に送信する。通信取得部44は、AP4a, 4bのそれぞれから、無線LANI/F20を介して、Pres信号を受信する。即ち、本実施例では、通信取得部44は、SSIDサーチによって、2個のAP4a, 4bを見つけることができる。

10

20

30

40

50

【0093】

なお、仮に、MFP10の周囲にG/O機器が存在している場合には、当該G/O機器も、MFP10からPReq信号を受信すると、Pres信号をMFP10に送信する。従って、通信取得部44は、AP4a, 4bのみならず、G/O機器からも、Pres信号を受信し得る。ただし、本実施例では、MFP10の周囲にG/O機器が存在しない場合を例として、以下の説明を続ける。

【0094】

Pres信号は、APが現在利用しているSSIDと、APが現在利用している認証方式を示す認証方式情報と、APが現在利用している暗号化方式を示す暗号化方式情報と、APが実現する無線通信の通信速度を示す通信速度情報と、を含む。従って、通信取得部44は、Pres信号を受信することによって、当該Pres信号の送信元のAPを利用した無線通信に関する情報を取得する。

10

【0095】

S44では、選択部43は、複数個のAP4a, 4bの中から、1個のAPを選択する。上述したように、メモリ34は、MFP10が過去に参加した1個以上の通常Wi-Fiネットワークに対応する1個以上の参加情報を格納している。選択部43は、S42で取得された複数個のPres信号に含まれる複数個のSSIDの中から、メモリ34内の1個以上の参加情報に含まれる1個以上のSSIDに一致する1個以上のSSIDを抽出する。次いで、選択部43は、抽出済みの1個以上のSSIDの中から1個のSSIDを選択することによって、1個のAPを選択する。なお、1個のAPを選択するための具体的な手法については、後で詳しく説明する。

20

【0096】

S46では、送信部42は、まず、選択済みのAPに関するAP情報を準備する。具体的に言うと、送信部42は、S42のSSIDサーチにおいて、選択済みのAPから取得された認証方式情報、暗号化方式情報、SSID、及び、BSSIDを準備する。また、送信部42は、選択済みのAPから取得されたSSIDを含む参加情報をメモリ34から読み出して、当該参加情報にパスワードが含まれている場合には、当該パスワードを準備する。そして、送信部42は、NFCI/F22を介して、準備済みの各情報を含むAP情報を携帯端末50に送信する。

【0097】

S48では、通信実行部46は、S46で準備された各情報を用いて、無線LANI/F20を介して、選択済みのAPと無線接続を実行する。当該無線接続は、S46で準備されたSSIDによって識別される特定の通常Wi-Fiネットワークに参加するための通信処理を含む。これにより、MFP10は、上記の特定の通常Wi-Fiネットワークに参加することができる。上述したように、携帯端末50も、上記の特定の通常Wi-Fiネットワークに参加する(図2のS16)。この結果、MFP10及び携帯端末50が同一の通常Wi-Fiネットワークに属することになる。S48を終えると、S50に進む。

30

【0098】

S50では、通信実行部46は、携帯端末50から、無線LANI/F20を介して、印刷データを受信する。例えば、S40を経て実行されるS50では、通信実行部46は、クライアント状態の携帯端末50から、中継装置を介さずに、印刷データを直接的に受信する。また、例えば、S48又はS49を経て実行されるS50では、通信実行部46は、携帯端末50から、APを介して、印刷データを受信する。

40

【0099】

次いで、S52では、制御部30は、印刷データを処理して(例えば、印刷実行部16が処理可能なデータに加工して)、処理済みデータを印刷実行部16に供給する。これにより、印刷実行部16は、処理済みデータに従って、印刷媒体に印刷を実行する。なお、S30で受信されたNFC情報に含まれるセキュリティ情報がセキュアを示す場合には、ユーザが当該セキュリティ情報に含まれるパスワードをMFP10に入力するまで、印刷

50

実行部 16 は、印刷を開始しない（即ち印刷の実行を保留する）。一方において、S 30 で受信された NFC 情報に含まれるセキュリティ情報が非セキュアを示す場合には、印刷実行部 16 は、制御部 30 から処理済みデータを取得すると、ただちに印刷を開始する。S 52 が終了すると、図 3 の通信処理が終了する。なお、S 48 において、MFP 10 が新たな通常 Wi-Fi ネットワークに参加した場合には、S 52 が終了しても、制御部 30 は、上記の新たな通常 Wi-Fi ネットワークに参加している状態を維持する。

【0100】

印刷データは、NFC 通信によって通信される情報（上記の NFC 情報、WFD 無線設定、AP 情報等）と比べて、大きいデータサイズを有する。上述したように、NFC 通信の通信速度は、WFD 通信又は通常 Wi-Fi 通信の通信速度よりも遅い。従って、仮に、MFP 10 及び携帯端末 50 の間で、NFC 通信を利用して、印刷データの無線通信が実行される構成を採用すると、印刷データの無線通信のために長時間を要する。このような実情に鑑みて、本実施例では、MFP 10 は、図 3 の S 40、S 46、又は、S 49 を実行して、WFD 無線設定又は AP 情報を携帯端末 50 に送信する。これにより、MFP 10 及び携帯端末 50 は、無線 LAN I/F 20 を介して、印刷データの WFD 通信又は通常 Wi-Fi 通信を実行することができ、この結果、印刷データの無線通信を迅速に実行することができる。

【0101】

上述したように、携帯端末 50 が、中継装置を介さない直接無線通信を MFP 10 と実行するための特定の態様（即ち、MFP 10 が G/O 状態であり、かつ、携帯端末 50 がクライアント状態である態様）で、WFD ネットワークに参加することが可能である場合（即ち、図 3 の S 34 で NO の場合、又は、S 38 が実行される場合）に、MFP 10 は、携帯端末 50 が WFD ネットワークに参加するための無線設定を、携帯端末 50 に送信する（S 40）。一方において、携帯端末 50 が、上記の特定の態様で WFD ネットワークに参加することが可能でない場合（即ち、図 3 の S 34 で YES の場合、又は、S 36 で YES の場合）に、携帯端末 50 が通常 Wi-Fi ネットワークに参加するための無線設定を、携帯端末 50 に送信する（S 46、S 49）。従って、MFP 10 は、携帯端末 50 が上記の特定の態様で WFD ネットワークに参加することが可能であるのか否かに応じて、適切な無線設定を携帯端末 50 に送信することができる。このために、MFP 10 は、WFD ネットワーク又は通常 Wi-Fi ネットワークに携帯端末 50 を適切に参加させることができる。この結果、MFP 10 は、WFD ネットワーク又は通常 Wi-Fi ネットワークを利用して、携帯端末 50 と対象データの無線通信を適切に実行することができる（S 50）。

【0102】

（実施例 1 - 1）

続いて、図 3 の S 44 の AP 選択処理の内容について説明する。S 44 では、選択部 43 は、まず、抽出済みの 1 個以上の SSID のそれぞれについて、当該 SSID の取得元の AP が現在利用している暗号化方式（即ち、当該 SSID を含む Pres 信号に含まれる暗号化方式情報）を確認する。そして、NFC 情報に含まれるセキュリティ情報がセキュアを示す場合、即ち、セキュリティ情報にパスワードが含まれる場合には、選択部 43 は、印刷データのセキュリティが高いと判断する。この場合、選択部 43 は、「AES」が確認された 1 個の SSID を選択することによって、1 個の AP を選択する。一方において、NFC 情報に含まれるセキュリティ情報が非セキュアを示す場合、即ち、セキュリティ情報にパスワードが含まれない場合には、選択部 43 は、印刷データのセキュリティが低いと判断する。この場合、選択部 43 は、「AES」以外の暗号化方式（例えば「TKIP」、「WEP」）が確認された 1 個の SSID を選択することによって、1 個の AP を選択する。

【0103】

なお、NFC 情報に含まれるセキュリティ情報がセキュアを示す場合において、「AES」が確認された SSID が存在しない場合には、選択部 43 は、「AES」以外の暗号

化方式が確認された S S I D を選択してもよい。また、N F C 情報に含まれるセキュリティ情報が非セキュアを示す場合において、「A E S」以外の暗号化方式が確認された S S I D が存在しない場合には、選択部 4 3 は、「A E S」が確認された S S I D を選択してもよい。即ち、選択部 4 3 は、抽出済みの 1 個以上の S S I D の中に、条件を満たす S S I D が存在しない場合には、所定の手法（例えばランダムに選択する手法）を用いて、S S I D を選択してもよい。この点は、以下の各実施例でも同様である。

【0104】

（実施例 1 - 1 の具体例；図 4）

続いて、図 4 を参照して、実施例 1 - 1 の具体例を説明する。図 4 において、M F P 1 0 及び携帯端末 5 0 の間の一本線の矢印は、N F C I / F 2 2 , 6 2 を介した無線通信を示し、M F P 1 0 及び携帯端末 5 0 の間の二本線の矢印は、無線 L A N I / F 2 0 , 6 0 を介した無線通信を示す。A P 4 a は、S S I D 「a a a」、暗号化方式「A E S」、及び、認証方式「W P A 2」を現在利用しており、通信速度「1 0 0 M b p s」を実現する。A P 4 b は、S S I D 「b b b」、暗号化方式「T K I P」、及び、認証方式「W P A」を現在利用しており、通信速度「1 0 M b p s」を実現する。なお、A P 4 a 及び A p 4 b が現在利用している B S S I D は、図示省略している。

10

【0105】

また、図 4 では、M F P 1 0 が G / O 状態として W F D ネットワークを形成しているが、クライアント数が最大値 N であり、携帯端末 5 0 を W F D ネットワークに参加させることができない。また、M F P 1 0 は、通常 W i - F i ネットワークに現在参加していない。M F P 1 0 は、A P 4 a が形成している通常 W i - F i ネットワーク、及び、A P 4 b が形成している通常 W i - F i ネットワークの両方に過去に参加したことがある。従って、M F P 1 0 のメモリ 3 4 は、A P 4 a に対応する参加情報と、A P 4 b に対応する参加情報と、を格納している。

20

【0106】

M F P 1 0 は、携帯端末 5 0 から、N F C I / F 2 2 を介して、N F C 情報を受信すると（図 3 の S 3 0 で Y E S）、S 3 2 で Y E S、S 3 4 で Y E S、S 4 1 で N O と判断して、S S I D 検索を実行する（S 4 2）。これにより、M F P 1 0 は、A P 4 a , 4 b のそれぞれから、P R e s 信号を受信する。

30

【0107】

図 4 のケース A では、N F C 情報に含まれるセキュリティ情報がセキュアを示す。従って、M F P 1 0 は、複数個の A P 4 a , 4 b の中から、暗号化方式「A E S」を現在利用している A P 4 a を選択する（S 4 4）。次いで、M F P 1 0 は、N F C I / F 2 2 を介して、A P 4 a を示す S S I D 「a a a」を含む A P 情報を携帯端末 5 0 に送信する（S 4 6）。次いで、M F P 1 0 は、A P 4 a と無線接続を実行して、A P 4 a が形成している通常 W i - F i ネットワークに参加する（S 4 8）。

30

【0108】

同様に、携帯端末 5 0 も、A P 4 a と無線接続を実行して、A P 4 a が形成している通常 W i - F i ネットワークに参加する（図 2 の S 1 6）。次いで、携帯端末 5 0 は、無線 L A N I / F 6 0 を介して、印刷データを A P 4 a に送信する（S 2 0）。A P 4 a は、印刷データを M F P 1 0 に送信する。この結果、M F P 1 0 は、無線 L A N I / F 2 0 を介して、印刷データを受信して（図 3 の S 5 0）、印刷処理を実行する（S 5 2）。

40

【0109】

一方において、図 4 のケース B では、N F C 情報に含まれるセキュリティ情報が非セキュアを示す。従って、M F P 1 0 は、複数個の A P 4 a , 4 b の中から、暗号化方式「T K I P」を現在利用している A P 4 b を選択する（S 4 4）。次いで、M F P 1 0 は、N F C I / F 2 2 を介して、A P 4 b を示す S S I D 「b b b」を含む A P 情報を携帯端末 5 0 に送信する（S 4 6）。次いで、M F P 1 0 は、A P 4 b と無線接続を実行して、A P 4 b が形成している通常 W i - F i ネットワークに参加する（S 4 8）。これにより、M F P 1 0 は、無線 L A N I / F 2 0 を介して、印刷データを受信して（S 5 0）、印刷

50

処理を実行する (S 5 2)。

【 0 1 1 0 】

上述したように、本実施例では、携帯端末 5 0 のユーザによって印刷データに対してパスワードが設定される場合、即ち、印刷データのセキュリティが高い場合には、選択部 4 3 は、高セキュリティの暗号化方式「AES」を利用している 1 個の AP を選択する。これにより、高セキュリティの印刷データの通信が、高セキュリティの暗号化方式「AES」に従って実行される。即ち、MFP 1 0 は、携帯端末 5 0 のユーザの意図 (即ち高セキュリティ) に応じて、適切な AP を選択することができる。

【 0 1 1 1 】

一方において、携帯端末 5 0 のユーザによって印刷データに対してパスワードが設定されない場合、即ち、印刷データのセキュリティが低い場合には、選択部 4 3 は、低セキュリティの暗号化方式 (例えば「TKIP」、「WEP」) を利用している 1 個の AP を選択する。これにより、低セキュリティの印刷データの通信が、低セキュリティの暗号化方式に従って実行される。携帯端末 5 0 のユーザの意図が低セキュリティであるために、低セキュリティの暗号化方式が利用されても問題ない。仮に、印刷データのセキュリティの高低に関わらず、高セキュリティの暗号化方式「AES」を利用している AP を必ず選択する構成が採用されると、当該 AP が形成している通常 Wi - Fi ネットワークに参加する機器の数が多くなってしまい、当該 AP の負荷が大きくなる。即ち、低セキュリティの印刷データの通信が実行されるべき状況において、高セキュリティの暗号化方式「AES」を利用している AP を選択する構成が採用されると、当該 AP と高セキュリティのデータ通信を実行すべきクライアント機器の通信に支障を来すおそれがある。本実施例では、携帯端末 5 0 のユーザの意図が低セキュリティである場合に、低セキュリティの暗号化方式を利用している AP を選択する構成を採用することによって、複数個の AP 4 a , 4 b のうちの一部の AP のみが大きな負荷を有する事象が発生するのを適切に抑制することができる。

【 0 1 1 2 】

(対応関係)

MFP 1 0、携帯端末 5 0 が、それぞれ、「第 1 の通信装置」、「第 2 の通信装置」の一例である。NFC I / F 2 2、無線 LAN I / F 2 0 が、それぞれ、「第 1 種のインターフェース」、「第 2 種のインターフェース」の一例である。G / O 状態、クライアント状態が、それぞれ、「親局状態」、「子局状態」の一例である。WFD ネットワーク、通常 Wi - Fi ネットワークが、それぞれ、「第 1 種の無線ネットワーク」、「第 2 種の無線ネットワーク」の一例である。図 3 の S 3 4 で NO の場合、又は、S 3 8 が実行される場合が、「第 1 の場合」の一例である。図 3 の S 3 4 で YES の場合、又は、S 3 6 で YES の場合が、「第 2 の場合」の一例である。図 3 の S 4 0 で送信される無線設定、S 4 6 又は S 4 9 で送信される AP 情報に含まれる無線設定が、それぞれ、「第 1 の無線設定」、「第 2 の無線設定」の一例である。複数個の AP 4 a , 4 b が、「複数個の中継装置」の一例である。印刷データが、「対象データ」の一例である。Pres 信号が、「通信関係情報」の一例である。印刷データに対するパスワードを設定するのか否かに応じたセキュリティ情報が、「データ関係情報」及び「処理関係情報」の一例である。また、図 4 の例では、「AES」、「TKIP」が、それぞれ、「第 1 の暗号化方式」、「第 2 の暗号化方式」の一例である。

【 0 1 1 3 】

(実施例 1 - 2)

図 5 を参照して、他の各実施例 1 - 2 ~ 1 - 9 について説明する。各実施例 1 - 2 ~ 1 - 9 は、図 3 の S 4 4 の内容が、実施例 1 - 1 とは異なる。

【 0 1 1 4 】

実施例 1 - 2 では、図 3 の S 4 4 において、選択部 4 3 は、まず、抽出済みの 1 個以上の SSID のそれぞれについて、当該 SSID の取得元の AP が現在利用している認証方式 (即ち、当該 SSID を含む Pres 信号に含まれる認証方式情報) を確認する。そし

て、NFC情報に含まれるセキュリティ情報がセキュアを示す場合には、選択部43は、「WPA2」が確認された1個のSSIDを選択することによって、1個のAP(図4の例では、「WPA2」を現在利用しているAP4a)を選択する。一方において、NFC情報に含まれるセキュリティ情報が非セキュアを示す場合には、選択部43は、「WPA2」以外の認証方式(例えば「WPA」、「Open」)が確認された1個のSSIDを選択することによって、1個のAP(図4の例では、「WPA」を現在利用しているAP4b)を選択する。

【0115】

本実施例では、高セキュリティの印刷データの通信が、高セキュリティの認証方式「WPA2」に従って実行される。即ち、MFP10は、携帯端末50のユーザの意図(即ち高セキュリティ)に応じて、適切なAPを選択することができる。また、MFP10は、携帯端末50のユーザの意図が低セキュリティである場合に、低セキュリティの認証方式を利用しているAPを選択する。これにより、一部のAPのみが大きな負荷を有する事象が発生するのを適切に抑制することができる。なお、本実施例では、「WPA2」、「WPA」が、それぞれ、「第1の認証方式」、「第2の認証方式」の一例である。

10

【0116】

(実施例1-3)

実施例1-1では、携帯端末50のユーザは、印刷データに対してパスワードを設定するのか否かを選択するための操作を、操作部52に加える。そして、携帯端末50は、当該選択に応じて、セキュリティ情報を生成する。これに代えて、実施例1-3では、携帯端末50のユーザは、印刷データを暗号化するのか否かを選択するための操作を、操作部52に加える。

20

【0117】

第1の例では、MFP10及び携帯端末50が、共通鍵を有している状況を想定する。印刷データを暗号化することがユーザによって選択される場合には、携帯端末50の制御部70は、共通鍵を利用して印刷データを暗号化し、MFP10の制御部30は、共通鍵を利用して印刷データを復号化する。一方において、印刷データを暗号化しないことがユーザによって選択される場合には、携帯端末50の制御部70は、印刷データを暗号化しない。

30

【0118】

また、第2の例では、印刷データのデータ形式がPDF(Portable Document Formatの略)である状況を想定する。印刷データを暗号化することがユーザによって選択される場合には、携帯端末50の制御部70は、予め決められている電子署名を利用して印刷データを暗号化し、署名PDFのデータ形式を有する印刷データを準備する。そして、MFP10の制御部30は、携帯端末50から印刷データが受信されると、予め決められている電子署名を利用して、署名PDFのデータ形式を有する印刷データを復号化する。一方において、印刷データを暗号化しないことがユーザによって選択される場合には、携帯端末50の制御部70は、印刷データを暗号化しない(即ち、通常のPDFのデータ形式を有する印刷データを準備する)。

40

【0119】

上記の第1の例及び第2の例のどちらでも、印刷データを暗号化することが選択される場合は、印刷データを暗号化しないことが選択される場合と比較して、印刷データのセキュリティが高い。図2のS11では、携帯端末50の制御部70は、印刷データを暗号化することが選択された場合には、セキュアを示すセキュリティ情報を生成し、印刷データを暗号化しないことが選択された場合には、非セキュアを示すセキュリティ情報を生成する。この点が、実施例1-1とは異なる。その他の点は、実施例1-1と同様である。

【0120】

本実施例でも、実施例1-1と同様の効果を得ることができる。なお、本実施例では、印刷データを暗号化するのか否かに応じたセキュリティ情報が、「データ関係情報」及び「処理関係情報」の一例である。

50

【 0 1 2 1 】

(実施例 1 - 4)

実施例 1 - 4 は、実施例 1 - 3 と同様に、セキュリティ情報は、印刷データを暗号化するの否かに応じて決定される。また、実施例 1 - 2 と同様に、選択部 4 3 は、セキュリティ情報がセキュアを示す場合には、「WPA2」を利用している 1 個の AP を選択し、「WPA2」以外の認証方式を利用している 1 個の AP を選択する。本実施例でも、実施例 1 - 2 と同様の効果を得ることができる。

【 0 1 2 2 】

(実施例 1 - 5)

実施例 1 - 5 では、図 2 の S 1 1 において、携帯端末 5 0 の制御部 7 0 は、セキュリティ情報の代わりに、印刷データのデータサイズを示すサイズ情報を含む NFC 情報を生成する。また、図 3 の S 4 4 において、選択部 4 3 は、まず、抽出済みの 1 個以上の SSID のそれぞれについて、当該 SSID の取得元の AP が実現する通信速度（即ち、当該 SSID を含む Pres 信号に含まれる通信速度情報）を確認する。そして、NFC 情報に含まれるサイズ情報が予め決められている閾値以上である場合には、選択部 4 3 は、100Mbps 以上の通信速度が確認された 1 個の SSID（即ち 1 個の AP）を選択する。一方において、NFC 情報に含まれるサイズ情報が上記の閾値未満である場合には、選択部 4 3 は、100Mbps 未満の通信速度が確認された 1 個の SSID（即ち 1 個の AP）を選択する。

【 0 1 2 3 】

本実施例では、印刷データのデータサイズが大きい状況では、高速の通信速度を実現する 1 個の AP が選択される。これにより、データサイズが大きい印刷データの通信に必要な時間を短縮することができる。一方において、印刷データのデータサイズが小さい状況では、低速の通信速度を実現する 1 個の AP が選択される。印刷データのデータサイズが小さいために、低速の通信速度が利用されても、印刷データの通信に必要な時間が長くなりならず済む。仮に、印刷データのデータサイズの大小に関わらず、高速の通信速度を実現する AP を必ず選択する構成が採用されると、当該 AP の負荷が大きくなる。即ち、データサイズが小さい印刷データの通信が実行されるべき状況において、高速の通信速度を実現する AP を選択する構成が採用されると、当該 AP とデータサイズが大きいデータの通信を実行すべきクライアント機器の通信に支障を来すおそれがある。本実施例によると、一部の AP のみが大きな負荷を有する事象が発生するのを適切に抑制することができる。

【 0 1 2 4 】

(実施例 1 - 6)

実施例 1 - 6 では、図 2 の S 1 1 において、携帯端末 5 0 の制御部 7 0 は、セキュリティ情報の代わりに、印刷データのデータ形式を示す形式情報を含む NFC 情報を生成する。また、図 3 の S 4 4 において、NFC 情報に含まれる形式情報が「非圧縮 Bitmap」を示す場合には、選択部 4 3 は、100Mbps 以上が確認された 1 個の SSID（即ち 1 個の AP）を選択する。一方において、NFC 情報に含まれる形式情報が「非圧縮 Bitmap」以外のデータ形式（例えば「PDF」、「JPEG」等）を示す場合には、選択部 4 3 は、100Mbps 未満の通信速度が確認された 1 個の SSID（即ち 1 個の AP）を選択する。

【 0 1 2 5 】

MFP 1 0 が印刷データを処理するための処理速度は、印刷データのデータ形式に依存する。例えば、「非圧縮 Bitmap」のデータ形式を有する印刷データのための処理速度は、「PDF」のデータ形式を有する印刷データのための処理速度よりも速い。本実施例では、印刷データのデータ形式が「非圧縮 Bitmap」である状況では、高速の通信速度を実現する 1 個の AP が選択される。これにより、MFP 1 0 は、印刷データを高速で受信しながら、印刷データを高速で処理することができ、この結果、印刷物をユーザに迅速に提供することができる。

【 0 1 2 6 】

また、本実施例では、印刷データのデータ形式が「非圧縮 Bitmap」以外である状況では、低速の通信速度を実現する1個のAPが選択される。仮に、印刷データのデータ形式が「非圧縮 Bitmap」以外である状況において、高速の通信速度を実現するAPが選択される構成を採用すると、MFP10において、印刷データの受信速度が、印刷データの処理速度よりも速くなり、この結果、印刷データを受信しても、印刷データを迅速に処理することができない可能性がある。このような実情に鑑みて、本実施例では、MFP10は、印刷データのデータ形式が「非圧縮 Bitmap」以外である状況では、低速の通信速度を実現する1個のAPを選択する。これにより、一部のAPのみが大きな負荷を有する事象が発生するのを適切に抑制することができる。なお、本実施例では、例えば、「非圧縮 Bitmap」、「PDF」が、それぞれ、「第1のデータ形式」、「第2のデータ形式」の一例である。 10

【0127】

(実施例1-7)

実施例1-7では、図2のS11において、携帯端末50の制御部70は、セキュリティ情報の代わりに、携帯端末50のCPU占有率を示す占有率情報を含むNFC情報を生成する。携帯端末50のCPU占有率は、ある単位時間において、CPU72が図2のアプリケーション処理を実行している時間の割合を意味する。CPU72が図2のアプリケーション処理のみを実行している場合には、携帯端末50のCPU占有率は、比較的に大きい値(即ち100%)を有する。また、CPU72が図2のアプリケーション処理と、それ以外の処理と、を並列的に実行している場合には、携帯端末50のCPU占有率は、比較的に小さい値を有する。即ち、携帯端末50のCPU占有率が大きい程、携帯端末50が図2のアプリケーション処理を高速で実行可能であり、その結果、図2のS20において、携帯端末50が印刷データをネットワークに高速で送信可能である。 20

【0128】

また、図3のS44において、NFC情報に含まれる占有率情報が示すCPU占有率が閾値以上である場合には、選択部43は、100Mbps以上の通信速度が確認された1個のSSID(即ち1個のAP)を選択する。一方において、NFC情報に含まれる占有率情報が示すCPU占有率が上記の閾値未満である場合には、選択部43は、100Mbps未満の通信速度が確認された1個のSSID(即ち1個のAP)を選択する。

【0129】

本実施例では、携帯端末50のCPU占有率が大きいために、携帯端末50が印刷データをネットワークに高速で送信可能である状況では、高速の通信速度を実現する1個のAPが選択される。これにより、MFP10は、印刷データを高速で受信することができ、この結果、印刷物をユーザに迅速に提供することができる。また、本実施例では、携帯端末50のCPU占有率が小さいために、携帯端末50が印刷データをネットワークに高速で送信不可能である状況では、低速の通信速度を実現する1個のAPが選択される。仮に、携帯端末50のCPU占有率が小さい状況において、高速の通信速度を実現するAPが選択される構成を採用すると、携帯端末50において、印刷データをネットワークに送信する速度が、当該APが実現する通信速度よりも遅くなる可能性がある。そして、携帯端末50のCPU占有率が小さい状況において、高速の通信速度を実現するAPを選択する構成が採用されると、当該APと、当該APと通信すべきクライアント機器と、の間の通信に支障を来すおそれがある。このような実情に鑑みて、本実施例では、MFP10は、携帯端末50のCPU占有率が小さい状況では、低速の通信速度を実現する1個のAPを選択する。これにより、一部のAPのみが大きな負荷を有する事象が発生するのを適切に抑制することができる。なお、本実施例では、占有率情報が、「第2の能力関係情報」の一例である。 40

【0130】

(実施例1-8)

実施例1-8では、図2のS11において、携帯端末50の制御部70は、セキュリティ情報の代わりに、携帯端末50のメモリ残量を示す残量情報を含むNFC情報を生成す 50

る。携帯端末 50 のメモリ残量は、メモリ 74 のうち、図 2 のアプリケーション処理で利用可能な領域のサイズを意味する。携帯端末 50 のメモリ残量が大きい程、携帯端末 50 が図 2 のアプリケーション処理を高速で実行可能であり、その結果、図 2 の S 20 において、携帯端末 50 が印刷データをネットワークに高速で送信可能である。

【0131】

また、図 3 の S 44 において、NFC 情報に含まれる残量情報が示すメモリ残量が閾値以上である場合には、選択部 43 は、100Mbps 以上の通信速度が確認された 1 個の SSID (即ち 1 個の AP) を選択する。一方において、NFC 情報に含まれる残量情報が示すメモリ残量が上記の閾値未満である場合には、選択部 43 は、100Mbps 未満の通信速度が確認された 1 個の SSID (即ち 1 個の AP) を選択する。

10

【0132】

本実施例でも、実施例 1 - 7 と同様の効果が得られる。なお、本実施例では、残量情報が、「第 2 の能力関係情報」の一例である。

【0133】

(実施例 1 - 9)

実施例 1 - 9 では、図 2 の S 11 において、携帯端末 50 の制御部 70 は、セキュリティ情報の代わりに、携帯端末 50 の印刷データ処理速度を示す処理速度情報を含む NFC 情報を生成する。携帯端末 50 の印刷データ処理速度は、携帯端末 50 が印刷データをネットワークに送信する速度を意味し、携帯端末 50 の CPU 占有率及びメモリ残量に依存する。携帯端末 50 のメモリ 74 は、携帯端末 50 の CPU 占有率及びメモリ残量から、携帯端末 50 の印刷データ処理速度を特定するためのテーブルを格納している。従って、図 2 の S 11 において、携帯端末 50 の制御部 70 は、携帯端末 50 の現在の CPU 占有率及びメモリ残量をチェックして、チェック結果と上記のテーブルとを用いて、携帯端末 50 の現在の印刷データ処理速度を特定する。携帯端末 50 の印刷データ処理速度が大きい程、図 2 の S 20 において、携帯端末 50 が印刷データをネットワークに高速で送信可能である。

20

【0134】

また、図 3 の S 44 において、NFC 情報に含まれる処理速度情報が示す印刷データ処理速度が閾値以上である場合には、選択部 43 は、100Mbps 以上の通信速度が確認された 1 個の SSID (即ち 1 個の AP) を選択する。一方において、NFC 情報に含まれる処理速度情報が示す印刷データ処理速度が上記の閾値未満である場合には、選択部 43 は、100Mbps 未満の通信速度が確認された 1 個の SSID (即ち 1 個の AP) を選択する。

30

【0135】

本実施例でも、実施例 1 - 7 と同様の効果が得られる。なお、本実施例では、処理速度情報が、「第 2 の能力関係情報」の一例である。

【0136】

(実施例 2)

続いて、図 6 を参照して、実施例 2 の内容を説明する。上記の実施例 1 では、図 3 の S 44 において、MFP 10 の選択部 43 は、携帯端末 50 から得られる情報 (即ち、携帯端末 50 側の情報) に基づいて、1 個の AP を選択する。これに代えて、本実施例では、選択部 43 は、MFP 10 自身に関する情報 (即ち、MFP 10 側の情報) に基づいて、1 個の AP を選択する。

40

【0137】

(実施例 2 - 1)

図 3 の S 44 において、能力取得部 45 は、まず、MFP 10 の現在の CPU 占有率をチェックすることによって、占有率情報を取得する。上記の実施例 1 - 7 と同様に、MFP 10 の CPU 占有率は、ある単位時間において、CPU 32 が図 3 の通信処理を実行している時間の割合を意味する。MFP 10 の CPU 占有率が大きい程、MFP 10 が図 3 の通信処理を高速で実行可能であり、その結果、図 3 の S 52 において、MFP 10 が印

50

刷データを高速で処理可能である。

【0138】

取得済みの占有率情報が示すCPU占有率が閾値以上である場合には、選択部43は、100Mbps以上の通信速度が確認された1個のSSID（即ち1個のAP）を選択する。一方において、取得済みの占有率情報が示すCPU占有率が上記の閾値未満である場合には、選択部43は、100Mbps未満の通信速度が確認された1個のSSID（即ち1個のAP）を選択する。

【0139】

本実施例では、MFP10のCPU占有率が大きいため、MFP10が印刷データを高速で処理可能である状況では、高速の通信速度を実現する1個のAPが選択される。これにより、MFP10は、印刷データを高速で受信しながら、印刷データを高速で処理することができ、この結果、印刷物をユーザに迅速に提供することができる。また、本実施例では、MFP10のCPU占有率が小さいために、MFP10が印刷データを高速で処理不可能である状況では、低速の通信速度を実現する1個のAPが選択される。仮に、MFP10のCPU占有率が小さい状況において、高速の通信速度を実現するAPが選択される構成を採用すると、MFP10において、印刷データの受信速度が、印刷データの処理速度よりも速くなり、この結果、印刷データを受信しても、印刷データを迅速に処理することができない可能性がある。このような実情に鑑みて、本実施例では、MFP10は、MFP10のCPU占有率が小さい状況では、低速の通信速度を実現する1個のAPを選択する。これにより、一部のAPのみが大きな負荷を有する事象が発生するのを適切に抑制することができる。なお、本実施例では、占有率情報が、「第1の能力関係情報」の一例である。

10

20

【0140】

（実施例2-2）

図3のS44において、能力取得部45は、まず、MFP10の現在のメモリ残量をチェックすることによって、残量情報を取得する。上記の実施例1-8と同様に、MFP10のメモリ残量は、メモリ34のうち、図3の通信処理で利用可能な領域のサイズを意味する。MFP10のメモリ残量が大きい程、MFP10が図3の通信処理を高速で実行可能であり、その結果、図3のS52において、MFP10が印刷データを高速で処理可能である。

30

【0141】

取得済みの残量情報が示すメモリ残量が閾値以上である場合には、選択部43は、100Mbps以上の通信速度が確認された1個のSSID（即ち1個のAP）を選択する。一方において、取得済みの残量情報が示すメモリ残量が上記の閾値未満である場合には、選択部43は、100Mbps未満の通信速度が確認された1個のSSID（即ち1個のAP）を選択する。

【0142】

本実施例でも、実施例2-1と同様の効果が得られる。なお、本実施例では、残量情報が、「第1の能力関係情報」の一例である。

【0143】

（実施例2-3）

図3のS44において、能力取得部45は、まず、MFP10の現在のCPU占有率及びメモリ残量をチェックすることによって、MFP10の印刷データ処理速度情報を取得する。MFP10の印刷データ処理速度は、MFP10の印刷データを処理する速度を意味し、MFP10のCPU占有率及びメモリ残量に依存する。MFP10の印刷データ処理速度が大きい程、図3のS52において、MFP10が印刷データを高速で処理可能である。MFP10のメモリ34は、MFP10のCPU占有率及びメモリ残量から、MFP10の印刷データ処理速度を特定するためのテーブルを格納している。従って、能力取得部45は、MFP10の現在のCPU占有率及びメモリ残量をチェックして、チェック結果と上記のテーブルとを用いて、MFP10の現在の印刷データ処理速度を特定する。

40

50

【 0 1 4 4 】

また、取得済みの処理速度情報が示す印刷データ処理速度が閾値以上である場合には、選択部 4 3 は、1 0 0 M b p s 以上の通信速度が確認された 1 個の S S I D (即ち 1 個の A P) を選択する。一方において、取得済みの処理速度情報が示す印刷データ処理速度が上記の閾値未満である場合には、選択部 4 3 は、1 0 0 M b p s 未満の通信速度が確認された 1 個の S S I D (即ち 1 個の A P) を選択する。

【 0 1 4 5 】

本実施例でも、実施例 2 - 1 と同様の効果が得られる。なお、本実施例では、処理速度情報が、「第 1 の能力関係情報」の一例である。

【 0 1 4 6 】

(実施例 3)

続いて、図 7 を参照して、実施例 3 の内容を説明する。本実施例では、図 3 の S 4 4 において、M F P 1 0 の選択部 4 3 は、携帯端末 5 0 側の情報と、M F P 1 0 側の情報との両方に基づいて、1 個の A P を選択する。

【 0 1 4 7 】

(実施例 3 - 1)

実施例 1 - 1 と同様に、N F C 情報は、印刷データに対してパスワードを設定するの否かに応じたセキュリティ情報を含む。また、実施例 2 - 1 と同様に、図 3 の S 4 4 において、能力取得部 4 5 は、M F P 1 0 の現在の C P U 占有率をチェックして、占有率情報を取得する。また、図 7 のテーブルに示されるように、選択部 4 3 は、N F C 情報に含まれるセキュア情報の内容 (即ちセキュア又は非セキュア) と、取得済みの占有率情報が示す C P U 占有率と、の両方を用いて、1 個の A P を選択する。本実施例では、実施例 1 - 1 及び実施例 2 - 1 と同様の効果が得られる。

【 0 1 4 8 】

(実施例 3 - 2)

携帯端末 5 0 側の情報と M F P 1 0 側の情報との組み合わせは、実施例 3 - 1 に示す組み合わせに限られず、図 5 の実施例 1 - 1 ~ 1 - 9 と図 6 の実施例 2 - 1 ~ 2 - 3 とのいずれの組み合わせであってもよい。例えば、携帯端末 5 0 側の情報が、印刷データのデータサイズを示すサイズ情報であり、M F P 1 0 側の情報が、M F P 1 0 のメモリ残量を示す残量情報であってもよい。この場合、例えば、選択部 4 3 は、(1) サイズ情報が第 1 の閾値以上のデータサイズを示し、かつ、残量情報が第 2 の閾値以上のメモリ残量を示す場合には、高速の通信速度を実現する 1 個の A P を選択し、(2) サイズ情報が第 1 の閾値以上のデータサイズを示し、かつ、残量情報が第 2 の閾値未満のメモリ残量を示す場合には、低速の通信速度を実現する 1 個の A P を選択し、(3) サイズ情報が第 1 の閾値未満のデータサイズを示す場合には、残量情報が示すメモリ残量に関わらず、低速の通信速度を実現する 1 個の A P を選択してもよい。

【 0 1 4 9 】

また、例えば、携帯端末 5 0 側の情報が、携帯端末 5 0 のメモリ残量を示す残量情報であり、M F P 1 0 側の情報が、M F P 1 0 のメモリ残量を示す残量情報であってもよい。この場合、例えば、選択部 4 3 は、(1) 携帯端末 5 0 の残量情報と M F P 1 0 の残量情報との両方が、閾値以上のメモリ残量を示す場合には、高速の通信速度を実現する 1 個の A P を選択し、(2) 携帯端末 5 0 の残量情報と M F P 1 0 の残量情報とのうちの少なくとも一方が、閾値未満のメモリ残量を示す場合には、低速の通信速度を実現する 1 個の A P を選択してもよい。また、例えば、選択部 4 3 は、(1) 携帯端末 5 0 の残量情報と M F P 1 0 の残量情報との両方が、閾値以上のメモリ残量を示す場合には、高速の通信速度 (例えば 1 0 0 M b p s 以上) を実現する 1 個の A P を選択し、(2) 携帯端末 5 0 の残量情報と M F P 1 0 の残量情報とのうちの一方のみが、閾値未満のメモリ残量を示す場合には、中速の通信速度 (例えば 1 0 M b p s 以上 1 0 0 M b p s 未満) を実現する 1 個の A P を選択し、(3) 携帯端末 5 0 の残量情報と M F P 1 0 の残量情報とのうちの両方が、閾値未満のメモリ残量を示す場合には、低速の通信速度 (例えば 1 0 M b p s 未満) を

10

20

30

40

50

実現する 1 個の A P を選択してもよい。

【 0 1 5 0 】

(実施例 4)

続いて、図 8 及び図 9 を参照して、実施例 4 の内容を説明する。上記の実施例 1 ~ 3 では、M F P 1 0 が、携帯端末 5 0 側の情報及び / 又は M F P 1 0 側の情報に基づいて、1 個の A P を選択する。これに代えて、本実施例では、携帯端末 5 0 が、携帯端末 5 0 側の情報に基づいて、1 個の A P を選択する。携帯端末 5 0 のメモリ 7 4 は、携帯端末 5 0 が過去に参加した 1 個以上の通常 W i - F i ネットワークに対応する 1 個以上の参加情報を累積的に格納する。

【 0 1 5 1 】

10

(携帯端末 5 0 のアプリケーション処理 ; 図 8)

図 8 の S 1 1 0 は、図 2 の S 1 0 と同様である。S 1 1 1 , S 1 1 2 は、N F C 情報にセキュリティ情報が含まれない点において、図 2 の S 1 1 , S 1 2 と相違する。S 1 1 4 では、制御部 7 0 は、M F P 1 0 から、N F C I / F 6 2 を介して、W F D 無線設定を受信したのか否かを判断する。制御部 7 0 は、M F P 1 0 から W F D 無線設定を受信した場合には、S 1 1 6 に進み、M F P 1 0 から W F D 無線設定を受信しなかった場合には、S 1 1 7 に進む。S 1 1 6 は、図 2 の S 1 4 で W F D 無線設定が受信される場合に実行される S 1 6 と同様である。

【 0 1 5 2 】

S 1 1 7 では、制御部 7 0 は、M F P 1 0 から、N F C I / F 6 2 を介して、A P 情報を受信したのか否かを判断する。制御部 7 0 は、M F P 1 0 から A P 情報を受信した場合には、S 1 1 8 ~ S 1 2 2 をスキップして、S 1 2 4 に進む。なお、詳しくは後述するが、M F P 1 0 は、M F P 1 0 が G / O 状態で動作する W F D ネットワーク、又は、M F P 1 0 が現在参加している通常 W i - F i ネットワークに、携帯端末 5 0 を参加させることができない場合 (図 9 の S 1 4 1 で N O の場合) に、所定のレスポンスを携帯端末 5 0 に送信する。所定のレスポンスは、W F D 無線設定又は通常 W i - F i 無線設定を含まず、キャンセル情報を含むレスポンスである。なお、所定のレスポンスは、キャンセル情報も含まない空のレスポンスであってもよい。携帯端末 5 0 の受信部 8 1 は、M F P 1 0 から、N F C I / F 6 2 を介して、所定のレスポンスを受信する。この場合、制御部 7 0 は、S 1 1 7 で N O と判断して、S 1 1 8 に進む。

20

30

【 0 1 5 3 】

S 1 1 8 では、通信取得部 8 4 は、図 3 の S 4 2 と同様の手法を用いて、S S I D サーチを実行する。この結果、通信取得部 8 4 は、複数個の A P 4 a , 4 b から複数個の P R e s 信号を取得する。S 1 2 0 では、選択部 8 3 は、複数個の A P 4 a , 4 b の中から 1 個の A P を選択する。選択部 8 3 は、まず、複数個の P R e s 信号に含まれる複数個の S S I D の中から、メモリ 7 4 内の 1 個以上の参加情報に含まれる 1 個以上の S S I D に一致する 1 個以上の S S I D を抽出する。次いで、選択部 4 3 は、抽出済みの 1 個以上の S S I D の中から 1 個の S S I D を選択することによって、1 個の A P を選択する。なお、1 個の A P を選択するための具体的な手法については、後で詳しく説明する。

【 0 1 5 4 】

40

S 1 2 2 では、送信部 8 2 は、図 3 の S 4 6 と同様の手法を用いて、A P 情報を準備する。次いで、送信部 8 2 は、N F C I / F 6 2 を介して、A P 情報を M F P 1 0 に送信する。なお、制御部 7 0 は、S 1 2 2 で A P 情報を送信した後に、例えば、携帯端末 5 0 から所定の音を出力させて、N F C 通信が完了したことを携帯端末 5 0 のユーザに通知する。これにより、ユーザは、M F P 1 0 から携帯端末 5 0 を遠ざけてよいことを認識できる。S 1 2 2 を経て実行される S 1 2 4 では、通信実行部 8 6 は、選択済みの A P と無線接続を実行する。S 1 1 7 で Y E S の場合に実行される S 1 2 4 では、通信実行部 8 6 は、M F P 1 0 から受信された A P 情報を用いて、A P と無線接続を実行する。S 1 2 6 では、通信実行部 8 6 は、図 2 の S 2 0 と同様の手法を用いて、無線 L A N I / F 6 0 を介して、印刷データを M F P 1 0 に送信する。

50

【 0 1 5 5 】

(M F P 1 0 の通信処理 ; 図 9)

図 9 の S 1 3 0 ~ S 1 4 1 , S 1 4 9 は、図 3 の S 3 0 ~ S 4 1 , S 4 9 と同様である。S 1 4 2 では、M F P 1 0 の制御部 3 0 は、N F C I / F 2 2 を介して、所定のレスポンスを携帯端末 5 0 に送信する。S 1 4 4 では、制御部 3 0 は、携帯端末 5 0 から、N F C I / F 2 2 を介して、A P 情報を受信する。S 1 4 6 , S 1 5 0 , S 1 5 2 は、図 3 の S 4 8 , S 5 0 , S 5 2 と同様である。

【 0 1 5 6 】

(実施例 4 - 1)

続いて、図 8 の S 1 2 0 の A P 選択処理の内容について説明する。本実施例の A P 選択のための手法は、実施例 1 - 1 と同様である。即ち、印刷データに対してパスワードを設定することがユーザによって選択された場合 (即ち、セキュリティ情報がセキュアを示す場合) には、選択部 8 3 は、「 A E S 」が確認された 1 個の S S I D (即ち 1 個の A P) を選択する。一方において、印刷データに対してパスワードを設定しないことがユーザによって選択された場合 (即ち、セキュリティ情報が非セキュアを示す場合) には、選択部 8 3 は、「 A E S 」以外の暗号化方式 (例えば「 T K I P 」、「 W E P 」) が確認された 1 個の S S I D (即ち 1 個の A P) を選択する。

10

【 0 1 5 7 】

(実施例 4 - 1 の具体例 ; 図 1 0)

図 1 0 のシーケンス図において、前提とされる状況は、図 4 と同様である。なお、携帯端末 5 0 のメモリ 7 4 は、A P 4 a に対応する参加情報と、A P 4 b に対応する参加情報と、を格納している。

20

【 0 1 5 8 】

携帯端末 5 0 は、M F P 1 0 から、N F C I / F 6 2 を介して、所定のレスポンスを受信すると (図 8 の S 1 1 7 で N O)、S S I D 検索を実行する (S 1 1 8)。これにより、携帯端末 5 0 は、A P 4 a , 4 b のそれぞれから、P R e s 信号を受信する。

【 0 1 5 9 】

図 1 0 のケース A では、印刷データに対してパスワードが設定されている (即ちセキュリティ情報がセキュアを示す)。従って、携帯端末 5 0 は、複数個の A P 4 a , 4 b の中から、暗号化方式「 A E S 」を利用している A P 4 a を選択する (S 1 2 0)。次いで、携帯端末 5 0 は、N F C I / F 6 2 を介して、A P 4 a を示す S S I D 「 a a a 」を含む A P 情報を M F P 1 0 に送信する (S 1 2 2)。次いで、携帯端末 5 0 は、A P 4 a と無線接続を実行して、A P 4 a が形成している通常 W i - F i ネットワークに参加する (S 1 2 4)。次いで、携帯端末 5 0 は、無線 L A N I / F 6 0 を介して、印刷データを A P 4 a に送信する。A P 4 a は、印刷データを M F P 1 0 に送信する。

30

【 0 1 6 0 】

一方において、図 1 0 のケース B では、印刷データに対してパスワードが設定されていない (即ちセキュリティ情報が非セキュアを示す)。従って、携帯端末 5 0 は、複数個の A P 4 a , 4 b の中から、「 T K I P 」を利用している A P 4 b を選択する (S 1 2 0)。次いで、携帯端末 5 0 は、N F C I / F 2 2 を介して、A P 4 b を示す S S I D 「 b b b 」を含む A P 情報を M F P 1 0 に送信する (S 1 2 2)。次いで、携帯端末 5 0 は、A P 4 b と無線接続を実行して、A P 4 b が形成している通常 W i - F i ネットワークに参加する (S 1 2 4)。次いで、携帯端末 5 0 は、無線 L A N I / F 6 0 を介して、印刷データを A P 4 b に送信する。A P 4 b は、印刷データを M F P 1 0 に送信する。

40

【 0 1 6 1 】

本実施例でも、実施例 1 - 1 と同様の効果が得られる。図 9 の S 1 3 4 で N O の場合、又は、S 1 3 8 が実行される場合が、「第 1 の場合」の一例である。図 9 の S 1 3 4 で Y E S の場合、又は、S 1 3 6 で Y E S の場合が、「第 2 の場合」の一例である。図 3 の S 1 4 0 で送信される無線設定、S 1 4 9 で送信される A P 情報に含まれる無線設定が、それぞれ、「第 1 の無線設定」、「第 2 の無線設定」の一例である。

50

【0162】

(実施例4-2)

図8のS120において、携帯端末50の選択部83は、図5の実施例1-2~1-9のいずれかの携帯端末50側の情報を用いて、実施例1-2~1-9と同様に、AP選択処理を実行してもよい。なお、実施例1-7~1-9と同様のAP選択処理が実行される場合には、携帯端末50の能力取得部85は、携帯端末50の現在の状態をチェックして、携帯端末50の占有率情報、残量情報、又は、処理速度情報を取得する。本実施例でも、実施例1-2~1-9と同様の効果が得られる。

【0163】

(実施例5)

本実施例では、図9のS142において、MFP10の制御部30は、NFCI/F22を介して、MFP10の占有率情報、残量情報、又は、処理速度情報を含む所定のレスポンスを携帯端末50に送信する。これにより、携帯端末50の受信部81は、MFP10から、NFCI/F62を介して、MFP10の占有率情報、残量情報、又は、処理速度情報を含む所定のレスポンスを受信する。携帯端末50は、所定のレスポンスに含まれるMFP10側の情報に基づいて、1個のAPを選択する。即ち、図8のS120において、携帯端末50の選択部83は、図6の実施例2-1~2-3のいずれかのMFP10側の情報を用いて、実施例2-1~2-3と同様に、AP選択処理を実行する。本実施例でも、実施例2-1~2-3と同様の効果が得られる。

【0164】

(実施例6)

本実施例では、携帯端末50が、携帯端末50側の情報と、MFP10側の情報と、の両方に基づいて、1個のAPを選択する。即ち、図8のS120において、携帯端末50の選択部83は、携帯端末50側の情報と、所定のレスポンスに含まれるMFP10側の情報と、の両方に基づいて、1個のAPを選択する。携帯端末50の選択部83は、図7の実施例3-1又は3-2と同様に、AP選択処理を実行する。本実施例でも、実施例3-1又は3-2と同様の効果が得られる。

【0165】

以上、本発明の具体例を詳細に説明したが、これらは例示にすぎず、特許請求の範囲を限定するものではない。特許請求の範囲に記載の技術には以上に例示した具体例を様々に変形、変更したものが含まれる。上記の実施例の変形例を以下に列挙する。

【0166】

(変形例1) 上記の各実施例では、MFP10の周囲にG/O機器が存在しないために、図3のS42のSSIDサーチにおいて、通信取得部44は、G/O機器からPres信号を受信しない。これに代えて、MFP10の周囲にG/O機器が存在していてもよい。この場合、通信取得部44は、G/O機器からPres信号を受信してもよい。さらに、通信取得部44は、G/O機器と複数個のAP4a, 4bとの中から、1個の中継装置を選択してもよい。本実施例では、G/O機器と複数個のAP4a, 4bとが、「複数個の中継装置」の一例である。

【0167】

(変形例2) 上記の実施例1-5, 1-7~1-9、実施例2-1~2-3等において、選択部43, 83は、1個の閾値のみを用いて、1個のAPを選択する。これに代えて、選択部43, 83は、複数個の閾値を用いて、1個のAPを選択してもよい。例えば、実施例1-5において、選択部43は、(1)データサイズが第1の閾値以上である場合には、100Mbps以上の通信速度を実現する1個のAPを選択し、(2)データサイズが第1の閾値未満かつ第2の閾値以上である場合には、10Mbps以上100Mbps未満の通信速度を実現する1個のAPを選択し、(3)データサイズが第2の閾値未満である場合には、10Mbps未満の通信速度を実現する1個のAPを選択してもよい。

【0168】

(変形例3) 例えば、実施例1-6等において、選択部43, 83は、(1)データ形式

10

20

30

40

50

が「非圧縮Bitmap」である場合には、100Mbps以上の通信速度を実現する1個のAPを選択し、(2)データ形式が「JPEG」である場合には、10Mbps以上100Mbps未満の通信速度を実現する1個のAPを選択し、(3)データ形式が「PDF」である場合には、10Mbps未満の通信速度を実現する1個のAPを選択してもよい。

【0169】

(変形例4)選択部43, 83がAP選択処理で利用する情報は、図4～図6の携帯端末50側の情報及びMFP10側の情報に限られない。例えば、以下の各変形例を挙げることができる。

【0170】

(変形例4-1)例えば、携帯端末50の選択部83は、MFP10が印刷データを復号化する能力を有しているのか否かを示すセキュリティ対応情報に基づいて、1個のAPを選択してもよい。即ち、選択部83は、MFP10が印刷データを復号化する能力を有している場合には、図5の実施例1-3, 1-4の「セキュア」と同様に、1個のAPを選択し、MFP10が印刷データを復号化する能力を有していない場合には、図5の実施例1-3, 1-4の「非セキュア」と同様に、1個のAPを選択してもよい。本変形例では、セキュリティ対応情報が、「第2の能力関係情報」の一例である。

【0171】

(変形例4-2)例えば、選択部43, 83は、ユーザが携帯端末50の操作部52を操作することによって指定される印刷解像度を示す印刷解像度情報に基づいて、1個のAPを選択してもよい。より具体的には、選択部43, 83は、ユーザによって指定される印刷解像度が閾値以上である場合には、図5の実施例1-5の「サイズ 閾値」と同様に、100Mbpsの通信速度を実現するAPを選択してもよい。一方において、ユーザによって指定される印刷解像度が閾値未満である場合には、図5の実施例1-5の「サイズ<閾値」と同様に、100Mbps未満の通信速度を実現するAPを選択してもよい。本変形例では、印刷解像度情報が、「データ関係情報」の一例である。なお、ユーザは、MFP10の操作部12を操作することによって、印刷解像度を指定してもよい。この場合、印刷解像度情報は、MFP10側の情報である。

【0172】

(変形例4-3)変形例4-2において、印刷解像度の代わりに、スキャン解像度が利用されてもよい。例えば、携帯端末50からMFP10に印刷データが送信されるのではなく、MFP10から携帯端末50にスキャンデータ(即ち、スキャン実行部18が原稿のスキャンを実行することによって生成されるデータ)が送信される状況を想定する。この場合、選択部43, 83は、ユーザが携帯端末50の操作部52を操作することによって指定されるスキャン解像度を示すスキャン解像度情報に基づいて、1個のAPを選択してもよい。本変形例では、スキャン解像度情報が、「データ関係情報」の一例である。また、スキャンデータが、「対象データ」の一例である。なお、ユーザは、MFP10の操作部12を操作することによって、スキャン解像度を指定してもよい。この場合、スキャン解像度情報は、MFP10側の情報である。

【0173】

(変形例5)上記の各実施例では、選択部43, 83は、携帯端末50側の情報及び/又はMFP10側の情報と、複数個のPres信号と、を用いて、1個のAPを選択する。これに代えて、選択部43, 83は、複数個のPres信号を用いずに、携帯端末50側の情報及び/又はMFP10側の情報を用いて、1個のAPを選択してもよい。例えば、MFP10のメモリ34は、セキュアを示す情報と、ユーザによって予め登録された第1のSSIDと、が対応付けられていると共に、非セキュアを示す情報と、ユーザによって予め登録された第2のSSIDと、が対応付けられているテーブルを格納していてもよい。この場合、選択部43は、セキュリティ情報がセキュアを示す場合には、テーブルを参照して、第1のSSIDを選択し、セキュリティ情報が非セキュアを示す場合には、テーブルを参照して、第2のSSIDを選択してもよい。この構成によると、複数個のPre

10

20

30

40

50

s 信号を用いずに、1 個の A P を選択することができる。即ち、選択部 4 3 , 8 3 は、処理関係情報を用いて、特定の中継装置を選択すればよい。

【 0 1 7 4 】

(変形例 6) A P 情報は、選択済みの A P の S S I D を含んでいなくてもよく、選択済みの A P を特定可能な他の情報 (例えば、選択済みの A P の B S S I D 、選択済みの A P の I P アドレス等) を含んでいてもよい。

【 0 1 7 5 】

(変形例 7) 図 5 の実施例 1 - 1 では、暗号化方式情報に応じて A P 選択処理が実行されるために、P R e s 信号は、認証方式情報及び通信速度情報を含んでいなくてもよい。また、実施例 1 - 2 では、認証方式情報に応じて A P 選択処理が実行されるために、P R e s 信号は、暗号化方式情報及び通信速度情報を含んでいなくてもよい。また、実施例 1 - 5 では、通信速度情報に応じて A P 選択処理が実行されるために、P R e s 信号は、認証方式情報及び暗号化方式情報を含んでいなくてもよい。一般的に言うと、「通信関係情報」は、認証方式情報と暗号化方式情報と通信速度情報とのうちの少なくとも 1 個の情報を含んでいけばよい。

10

【 0 1 7 6 】

(変形例 8) 上記の実施例 1 - 1 等では、選択部 4 3 , 8 3 は、セキュリティ情報が印刷データの印刷を許可するためのパスワードを含むのか否かに応じて、印刷データのセキュリティの高低を判断する。即ち、上記の実施例 1 - 1 等では、印刷データの印刷が、「対象データの出力」の一例である。ただし、例えば、「対象データ」が表示用データである場合には、選択部 4 3 , 8 3 は、セキュリティ情報が表示用データの表示を許可するためのパスワードを含むのか否かに応じて、表示用データのセキュリティの高低を判断してもよい。

20

【 0 1 7 7 】

(変形例 9) 「第 1 種のインターフェース」は、N F C 通信を実行するためのインターフェースに限られず、赤外線通信を実行するためのインターフェースであってもよいし、B l u e t o o t h (登録商標) を実行するためのインターフェースであってもよいし、T r a n s f e r J e t を実行するためのインターフェースであってもよい。一般的に言うと、第 2 種のインターフェースを介した無線通信の通信速度が、第 1 種のインターフェースを介した無線通信の通信速度よりも速ければよい。

30

【 0 1 7 8 】

(変形例 1 0) 「第 1 種のインターフェース」及び「第 2 種のインターフェース」は、上記の各実施例のように、別体に構成されている 2 個のインターフェース (例えば 2 個の I C チップ) であってもよいし、一体に構成されている 1 個のインターフェース (例えば 1 個の I C チップ) であってもよい。

【 0 1 7 9 】

(変形例 1 1) 「親局状態」は、W F D の G / O 状態に限られず、無線ネットワークに属する各機器を管理する状態 (例えば、無線ネットワークに属する各機器の間の無線通信を中継可能な状態) であれば、どのような状態であってもよい。また、「子局状態」は、W F D のクライアント状態に限られず、無線ネットワークの親局状態の機器から管理される状態であれば、どのような状態であってもよい。

40

【 0 1 8 0 】

(変形例 1 2) 図 3 の S 4 0 、 S 4 6 、及び、S 4 9 において、送信部 4 2 は、N F C I / F 2 2 とは異なるインターフェースを介して、無線設定を携帯端末 5 0 に送信してもよい。

【 0 1 8 1 】

(変形例 1 3) 図 3 において、S 3 6 、 S 3 8 、 S 4 1 、 S 4 9 が実行されなくてもよい。即ち、S 3 2 で N O の場合に、S 4 2 に進んでもよい。また、S 3 4 で Y E S の場合に、S 4 2 に進んでもよい。また、図 3 において、S 3 4 、 S 4 1 、 S 4 9 が実行されなくてもよい。即ち、S 3 2 で Y E S の場合に、S 4 0 に進んでもよい。また、S 3 6 で Y E

50

S の場合に、S 4 2 に進んでもよい。一般的に言うと、第 1 の通信装置は、送信部と通信実行部とを少なくとも備えていればよい。

【0182】

(変形例 14) 「第 1 の通信装置」及び「第 2 の通信装置」は、MFP 10 及び携帯端末 50 に限られず、他の通信装置(例えば、プリンタ、スキャナ、FAX 装置、コピー機、電話機、デスクトップ PC、ノート PC、タブレット PC、サーバ、携帯電話、PDA 端末等)であってもよい。また、「対象データ」は、印刷データ、スキャンデータに限られず、他のデータ(例えば、音声データ、FAX データ等)であってもよい。

【0183】

(変形例 15) 上記の実施例では、MFP 10 の CPU 32 がメモリ 34 内のプログラム(即ちソフトウェア)を実行することによって、各部 41 ~ 46 の機能が実現される。これに代えて、各部 41 ~ 49 のうちの少なくとも 1 つは、論理回路等のハードウェアによって実現されてもよい。また、同様に、各部 81 ~ 86 のうちの少なくとも 1 つは、論理回路等のハードウェアによって実現されてもよい。

10

【0184】

また、本明細書または図面に説明した技術要素は、単独であるいは各種の組合せによって技術的有用性を発揮するものであり、出願時請求項記載の組合せに限定されるものではない。また、本明細書または図面に例示した技術は複数目的を同時に達成するものであり、そのうちの一つの目的を達成すること自体で技術的有用性を持つものである。

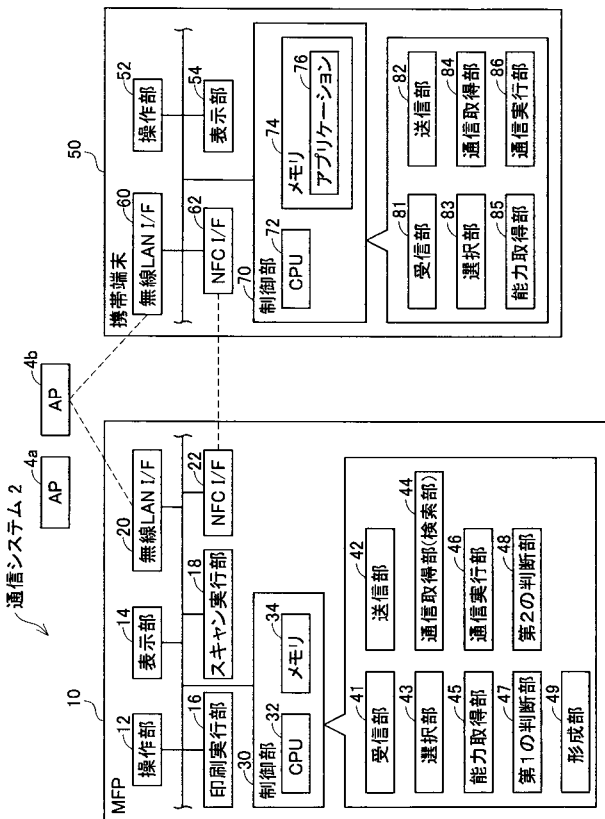
【符号の説明】

20

【0185】

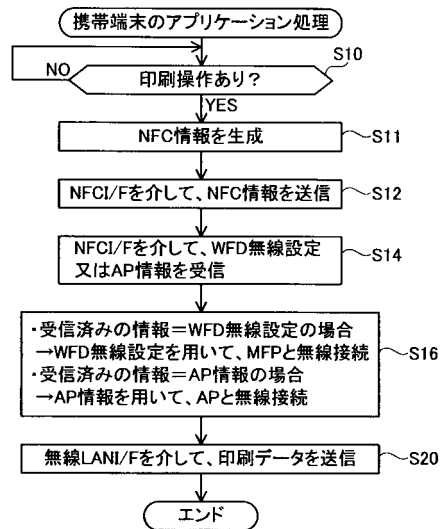
2 : 通信システム、4 a , 4 b : AP、10 : MFP、50 : 携帯端末

【図 1】

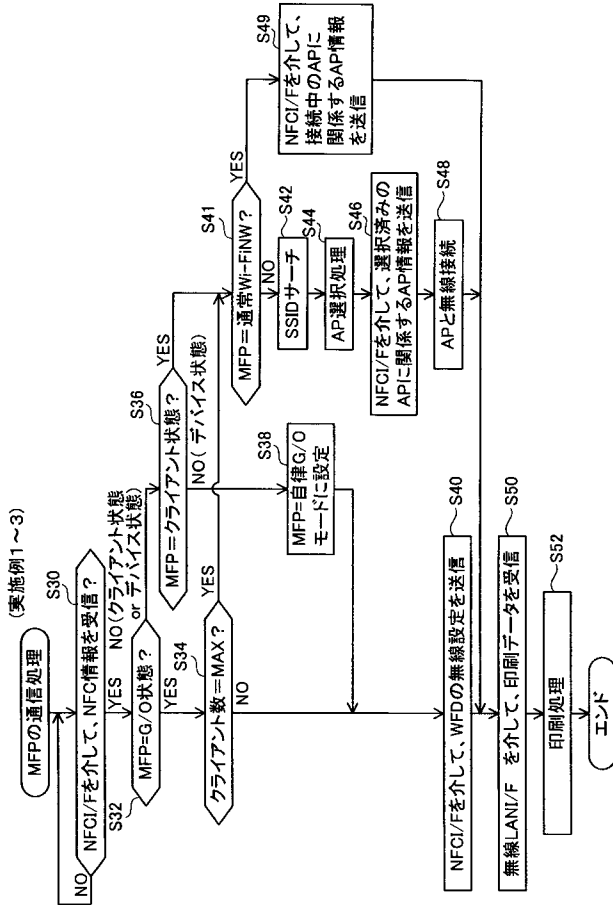


【図 2】

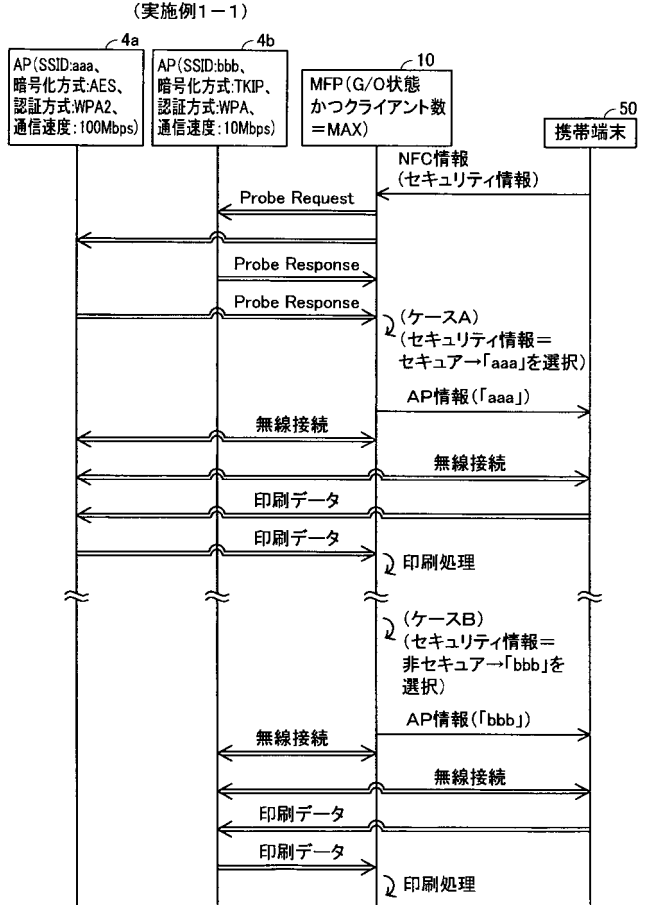
(実施例 1~3)



【 図 3 】



【 図 4 】



【 図 5 】

実施例	携帯端末側の情報	AP選択処理
1-1	パスワードの有無を示すセキュリティ情報	セキュア→AESを利用するAP 非セキュア→AES以外を利用するAP
1-2	パスワードの有無を示すセキュリティ情報	セキュア→WPA2を利用するAP 非セキュア→WPA2以外を利用するAP
1-3	暗号化の有無を示すセキュリティ情報	セキュア→AESを利用するAP 非セキュア→AES以外を利用するAP
1-4	暗号化の有無を示すセキュリティ情報	セキュア→WPA2を利用するAP 非セキュア→WPA2以外を利用するAP
1-5	印刷データのサイズ情報	サイズ≥閾値 →通信速度100Mbps以上を実現するAP サイズ<閾値 →通信速度100Mbps未満を実現するAP
1-6	印刷データの形式情報	形式=非圧縮Bitmap →通信速度100Mbps以上を実現するAP 形式=非圧縮Bitmap以外 →通信速度100Mbps未満を実現するAP
1-7	携帯端末のCPU占有率情報	CPU占有率≥閾値 →通信速度100Mbps以上を実現するAP CPU占有率<閾値 →通信速度100Mbps未満を実現するAP
1-8	携帯端末のメモリ残量情報	メモリ残量≥閾値 →通信速度100Mbps以上を実現するAP メモリ残量<閾値 →通信速度100Mbps未満を実現するAP
1-9	携帯端末の印刷データ処理速度情報	処理速度≥閾値 →通信速度100Mbps以上を実現するAP 処理速度<閾値 →通信速度100Mbps未満を実現するAP

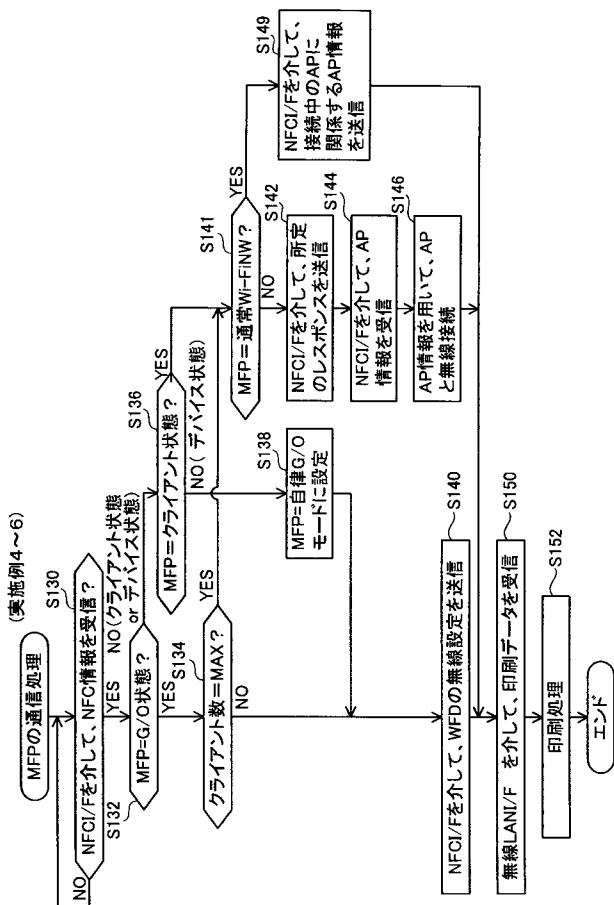
【 図 6 】

実施例	MFP側の情報	AP選択処理
2-1	MFPのCPU占有率情報	CPU占有率≥閾値 →通信速度100Mbps以上を実現するAP CPU占有率<閾値 →通信速度100Mbps未満を実現するAP
2-2	MFPのメモリ残量情報	メモリ残量≥閾値 →通信速度100Mbps以上を実現するAP メモリ残量<閾値 →通信速度100Mbps未満を実現するAP
2-3	MFPの印刷データ処理速度情報	処理速度≥閾値 →通信速度100Mbps以上を実現するAP 処理速度<閾値 →通信速度100Mbps未満を実現するAP

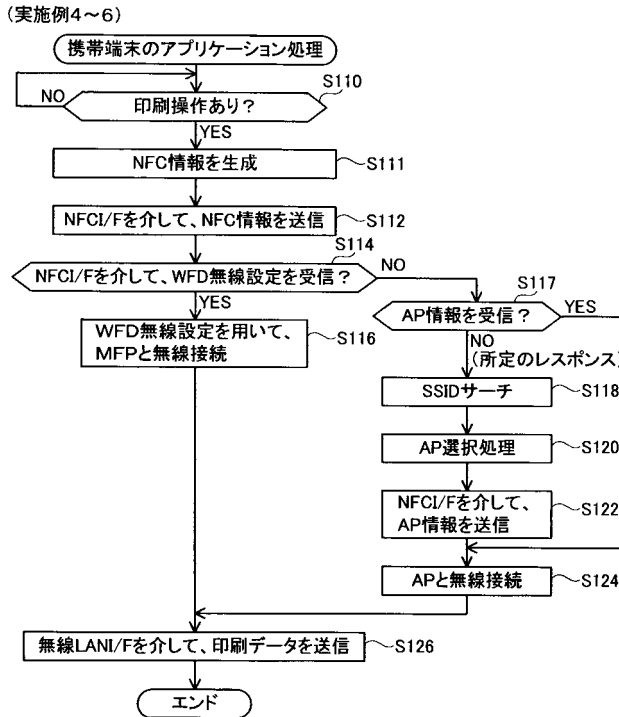
【 図 7 】

実施例	携帯端末側の情報	MFP側の情報	AP選択処理
3-1	パスワードの有無を示すセキュリティ情報	MFPのCPU占有率情報	セキュア、かつ、CPU占有率≧閾値 →暗号化方式AESを利用し、かつ、通信速度100Mbps以上を実現するAP 非セキュア、かつ、CPU占有率<閾値 →暗号化方式AESを利用し、かつ、通信速度100Mbps未満を実現するAP 非セキュア、かつ、CPU占有率≧閾値 →AES以外の暗号化方式を利用し、かつ、通信速度100Mbps以上を実現するAP 非セキュア、かつ、CPU占有率<閾値 →AES以外の暗号化方式を利用し、かつ、通信速度100Mbps未満を実現するAP
3-2	図5の実施例1-1~1-9と、図6の実施例2-1~2-3と、の様々な組み合わせ		

【 図 9 】



【 図 8 】



【 図 10 】

