

## 明 細 書

発明の名称： 通信装置、通信方法、およびプログラム

### 技術分野

[0001] 本発明は、無線通信を行う通信装置に関する。

### 背景技術

[0002] 無線LAN (Local Area Network) 技術は、無線LAN技術の標準化団体であるIEEE 802. 11により規格が策定されており、無線LAN技術の規格には、IEEE 802. 11/a/b/g/n/ac/axなどがある。ここでIEEEはInstitute of Electrical and Electronics Engineersの略である。

[0003] 特許文献1に記載されている、IEEE 802. 11axではOFDMAにより最大9. 6ギガビット毎秒 (Gbps) という高いピークスループットに加え、混雑状況下での通信速度向上を実現している。尚、OFDMAは、Orthogonal Frequency-Division Multiple Accessの略である。

[0004] 更なるスループット向上のために、IEEE 802. 11axの後継規格として、IEEE 802. 11beの規格策定を行うTask Groupが発足した。

[0005] 従来、IEEE 802. 11のAP (Access Point) は単一の周波数チャネルを介してSTA (Station) と接続を確立し、通信を行っていた。IEEE 802. 11be規格では、1台のAPが2. 4GHz帯、5GHz帯、及び6GHz帯を含む複数の周波数チャネルを介してSTAと複数のリンクを同時に確立し、通信を行うMulti-Link通信が検討されている。

[0006] 一方で、無線LAN技術の相互接続を保証するWi-Fi Allianceによる標準化が重要な役割を果たしており、無線LAN技術において、

より安全性の高い認証プログラムであるWPA3の規格化が現在進められている。尚、WPAはW i - F i P r o t e c t e d A c c e s sの略である。

[0007] また、無線LANにおける通信においては、ユニキャスト通信を暗号化する暗号鍵であるPTKと、ブロードキャスト通信またはマルチキャスト通信を暗号化する鍵であるGTKとを用いて通信の暗号化を行っている。ここで、PTKはPairwise Transient Keyの、GTKはGroup Transient Keyのそれぞれ略である。

[0008] さらに、11be規格で検討が進められているMulti-Link通信では、接続を確立するそれぞれのリンクにおいて、共通のPTKを用いることが検討されている。

## 先行技術文献

### 特許文献

[0009] 特許文献1：特開2018-50133号公報

### 発明の概要

#### 発明が解決しようとする課題

[0010] Multi-Link通信では、それぞれのリンクにおいて共通のPTKを用いるために、それぞれのリンクで同一のセキュリティ方式を用いて各リンクの認証および暗号化を行う必要がある。また、6GHz帯で通信を行う場合には、WPA3を用いて認証、暗号化を行うことが規定されている。しかし例えば6GHz帯の周波数チャンネルと6GHz帯以外の周波数チャンネルを介して通信装置と他の通信装置が複数のリンクを同時に確立して通信する場合において、各リンク間で異なるセキュリティ方式を用いて認証、暗号化を行うおそれがある。

[0011] 上記課題を鑑み、本発明の通信装置は、通信装置と他の通信装置が複数のリンクを確立した状態で他の通信装置と通信を行う際に、特定の周波数チャンネルで動作する場合は、特定のセキュリティ方式を用いて認証を行うことを

目的とする。

### 課題を解決するための手段

- [0012] 上記目的を達成するため、本発明の通信装置は、WPA (Wi-Fi Protected Access) 2方式を用いた認証とWPA 3方式を用いた認証を実行可能な通信装置であって、周波数チャネルを介して前記通信装置と他の通信装置の間のリンクを確立する確立手段と、前記他の通信装置との通信を実行するための認証を制御する制御手段と、を有し、前記制御手段は、前記確立手段によって前記通信装置と前記他の通信装置との間で複数のリンクを確立した状態で前記他の通信装置と通信を行う際に、前記複数のリンクの少なくとも1つで使用される周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記WPA 3方式を用いて認証を実行する。
- [0013] また、本発明の通信装置は、WPA (Wi-Fi Protected Access) 2方式を用いた認証とWPA 3方式を用いた認証を実行可能で、通信のアクセスポイントとして動作する通信装置であって、他の通信装置と通信を行う通信手段と、前記他の通信装置との通信の認証を制御する制御手段と、を有し、前記制御手段は、前記通信装置と前記他の通信装置との間で協調動作を行う通信で使用される周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記WPA 3方式を用いて認証を実行することを特徴とする。
- [0014] また、本発明の通信装置は、第1のセキュリティ方式を用いた認証と第2のセキュリティ方式を用いた認証を実行可能な通信装置であって、周波数チャネルを介して前記通信装置と他の通信装置の間のリンクを確立する確立手段と、前記他の通信装置との通信の認証を制御する制御手段と、前記制御手段は、前記確立手段によって前記通信装置と前記他の通信装置との間で複数のリンクを確立した状態で前記他の通信装置と通信を行う際に、前記複数のリンクの少なくとも1つで使用される周波数チャネルが特定の周波数であることに基づいて前記第1のセキュリティ方式を用いて認証を実行し、前記複

数のリンクで使用される周波数チャンネルがいずれも前記特定の周波数帯に含まれる周波数チャンネルでないことに基づいて前記第1のセキュリティ方式または前記第2のセキュリティ方式を用いて認証を実行することを特徴とする。

[0015] また、本発明の通信装置は、第1のセキュリティ方式を用いた認証と第2のセキュリティ方式を用いた認証を実行可能で、通信のアクセスポイントとして動作する通信装置であって、通信のアクセスポイントとして動作する他の通信装置と通信を行う通信手段と、前記他の通信装置との通信の認証を制御する制御手段と、を有し、前記制御手段は、前記通信装置と前記他の通信装置との間で協調動作を行う通信で使用される周波数チャンネルが特定の周波数帯に含まれる周波数チャンネルであることに基づいて、前記第1のセキュリティ方式を用いて認証を実行し、前記協調動作を行う通信で使用される周波数チャンネルが前記特定の周波数帯に含まれる周波数チャンネルでないことに基づいて前記第1のセキュリティ方式または前記第2のセキュリティ方式を用いて認証を実行することを特徴とする。

### 発明の効果

[0016] 本発明によれば、通信装置と複数の周波数チャンネルを介して他の通信装置と通信を行う際に、特定の周波数チャンネルで動作する場合は、特定の認証方式を用いて認証および暗号化を行うことができる。

### 図面の簡単な説明

[0017] [図1]本発明におけるネットワークの構成を示す図である。

[図2]本発明における通信装置のハードウェア構成を示す図である。

[図3]本発明における通信装置の機能構成を示す図である。

[図4]本発明における通信装置101が決定したセキュリティ方式に従い付与するRSNEを示すエレメントの一例である。

[図5]本発明における通信装置101が決定したセキュリティ方式に従い付与するExtended Capabilityを示すエレメントの一例である。

[図6]本発明における通信装置101が決定したセキュリティ方式に従い付与するRSNXEを示すエレメントの一例である。

[図7]本発明における通信装置101がセキュリティ方式を決定する処理を示すフローチャート図である。

[図8]本発明におけるグラフィカルユーザインタフェース表示の例。

[図9]本発明におけるグラフィカルユーザインタフェース表示の例。

[図10]本発明におけるグラフィカルユーザインタフェース表示の例。

[図11]本発明におけるグラフィカルユーザインタフェース表示の例。

[図12]本発明におけるグラフィカルユーザインタフェース表示の例。

[図13]本発明におけるグラフィカルユーザインタフェース表示の例。

[図14]本発明におけるグラフィカルユーザインタフェース表示の例。

[図15]本発明におけるグラフィカルユーザインタフェース表示の例。

[図16]本発明におけるグラフィカルユーザインタフェース表示の例。

[図17]本発明におけるグラフィカルユーザインタフェース表示の例。

[図18]本発明におけるグラフィカルユーザインタフェース表示の例。

[図19]本発明におけるグラフィカルユーザインタフェース表示の例。

[図20]本発明におけるグラフィカルユーザインタフェース表示の例。

[図21]本発明におけるグラフィカルユーザインタフェース表示の例。

[図22]本発明におけるグラフィカルユーザインタフェース表示の例。

[図23]本発明におけるグラフィカルユーザインタフェース表示の例。

[図24]本発明における通信装置101がセキュリティ方式を決定する処理を示すフローチャート図である。

### 発明を実施するための形態

[0018] 以下、添付の図面を参照して、本発明の実施形態を詳細に説明する。尚、以下の実施形態において示す構成は一例に過ぎず、本発明は図示された構成に限定されるものではない。

[0019] (無線通信システムの構成)

図1は、本実施形態にかかる通信装置102が参加するネットワークの構

成を示す。通信装置102はネットワーク100に参加する役割を有するステーション（STA）である。通信装置101は、無線ネットワーク100を構築する役割を有するアクセスポイント（AP）である。通信装置101は通信装置102と通信可能である。

[0020] 通信装置101、通信装置102の各々は、IEEE802.11be（EHT）規格に準拠した無線通信を実行することができる。尚、IEEEはInstitute of Electrical and Electronics Engineersの略である。通信装置101、通信装置102は、2.4GHz帯、5GHz帯、および6GHz帯の周波数において通信することができる。各通信装置が使用する周波数帯は、これに限定されるものではなく、例えば60GHz帯のように、異なる周波数帯を使用してもよい。また、通信装置101、通信装置102は、20MHz、40MHz、80MHz、160MHz、および320MHzの帯域幅を使用して通信することができる。各通信装置が使用する帯域幅は、これに限定されるものではなく、例えば240MHzや4MHzのように、異なる帯域幅を使用してもよい。

[0021] 通信装置101、通信装置102は、IEEE802.11be規格に準拠したOFDMA通信を実行することで、複数のユーザの信号を多重する、マルチユーザ（MU、Multi User）通信を実現することができる。OFDMAは、Orthogonal Frequency Division Multiple Access（直交周波数分割多元接続）の略である。OFDMA通信では、分割された周波数帯域の一部（RU、Resource Unit）が各STAにそれぞれ重ならないように割り当てられ、各STAの搬送波が直交する。そのため、APは規定された帯域幅の中で複数のSTAと並行して通信することができる。

[0022] 尚、通信装置101、通信装置102は、IEEE802.11be規格に対応するとしたが、これに加えて、IEEE802.11be規格より前の規格であるレガシー規格に対応していてもよい。具体的には、通信装置1

01、通信装置102は、IEEE802.11a/b/g/n/ac/ax規格の少なくともいずれか一つに対応していてもよい。また、IEEE802.11シリーズ規格に加えて、Bluetooth（登録商標）、NFC、UWB、ZigBee、MBOAなどの他の通信規格に対応していてもよい。尚、UWBはUltra Wide Bandの略であり、MBOAはMulti Band OFDM Allianceの略である。また、NFCはNear Field Communicationの略である。UWBには、ワイヤレスUSB、ワイヤレス1394、WiNETなどが含まれる。また、有線LANなどの有線通信の通信規格に対応していてもよい。通信装置101の具体例としては、無線LANルーターやパーソナルコンピュータ（PC）などが挙げられるが、これらに限定されない。また通信装置101は、IEEE802.11b規格に準拠した無線通信を実行することができる無線チップなどの情報処理装置であってもよい。また、通信装置102の具体的な例としては、カメラ、タブレット、スマートフォン、PC、携帯電話、ビデオカメラ、ヘッドセットなどが挙げられるが、これらに限定されない。また、通信装置102は、IEEE802.11b規格に準拠した無線通信を実行することができる無線チップなどの情報処理装置であってもよい。

[0023] 各通信装置は、20MHz、40MHz、80MHz、160MHz、および320MHzの帯域幅を使用して通信することができる。

[0024] また、通信装置101および通信装置102は、複数の周波数チャネルを介してリンクを確立し、通信するMulti-Link通信を実行する。IEEE802.11シリーズ規格では、各周波数チャネルの帯域幅は20MHzとして定義されている。ここで、周波数チャネルとは、IEEE802.11シリーズ規格に定義された周波数チャネルであって、IEEE802.11シリーズ規格では、2.4GHz帯、5GHz帯、6GHz帯、60GHz帯の各周波数帯に複数の周波数チャネルが定義されている。尚、隣接する周波数チャネルとボンディングすることで、1つの周波数チャネルにお

いて40MHz以上の帯域幅を利用してもよい。例えば通信装置101は通信装置102と2.4GHz帯の第1の周波数チャンネルを介したリンク103を確立し、通信することができる。通信装置102はこれと並行して通信装置101と5GHz帯の第2の周波数チャンネルを介したリンク104を確立し、通信することができる。この場合に、通信装置102は、第1の周波数チャンネルを介したリンク103と並行して、第2の周波数チャンネルを介した第2のリンク104を維持するMulti-Link通信を実行する。このように通信装置101は複数の周波数チャンネルを介した複数のリンクを通信装置102と同時に確立することで、通信装置102との通信におけるスループットを向上させることができる。本実施形態ではリンク103を2.4GHz帯の6chで20MHzの接続とし、Link番号を1とする。リンク104を6GHz帯の113chで320MHzの接続とし、Link番号を2とする。

[0025] 例えば、通信装置101と通信装置102とは2.4GHz帯におけるリンク103と6GHz帯における第2のリンク104に加えて、5GHz帯における第3のリンクを確立するようにしてもよい。あるいは同じ周波数帯に含まれる複数の異なるチャンネルを介してリンクを確立するようにしてもよい。例えば2.4GHz帯における6chのリンクを第1のリンクとして、これに加えて2.4GHz帯における1chのリンクを第2のリンクとして確立するようにしてもよい。尚、周波数帯が同じリンクと、異なるリンクとが混在していてもよい。例えば、通信装置101と通信装置102で2.4GHz帯における6chのリンク103に加えて、2.4GHz帯の1chのリンクと、5GHz帯における149chのリンクを確立してもよい。通信装置101は通信装置102と周波数の異なる複数の接続を確立することで、ある帯域が混雑している場合であっても、通信装置102と他方の帯域で通信を確立することができるため、スループットの低下や通信遅延を防ぐことができる。

[0026] 尚、図1の無線ネットワーク100は1台のAPと1台のSTAによって

構成されているが、APおよびSTAの台数や配置はこれに限定されない。  
例えば、図1の無線ネットワークに加えて、STAを1台増やしてもよい。  
このとき確立する各リンクの周波数帯やリンクの数、周波数幅は問わない。

[0027] Multi-link通信を行う場合、通信装置101と通信装置102とは、1つのデータを分割して複数のリンクを介して相手装置に送信する。

[0028] また、通信装置101と通信装置102はMIMO (Multiple-Input And Multiple-Output) 通信を実行できてもよい。この場合、通信装置101および通信装置102は複数のアンテナを有し、一方がそれぞれのアンテナから異なる信号を同じ周波数チャネルを用いて送る。受信側は、複数のアンテナを用いて複数ストリームから到達したすべての信号を同時に受信し、各ストリームの信号を分離し、復号する。このように、MIMO通信を実行することで、通信装置101および通信装置102は、MIMO通信を実行しない場合と比べて、同じ時間でより多くのデータを通信することができる。また、通信装置101および通信装置102は、Multi-link通信を行う場合に、一部のリンクにおいてMIMO通信を実行してもよい。

[0029] 本実施形態において通信装置101、通信装置102は、セキュリティ方式であるWPA (Wi-Fi Protected Access) 規格に加えて、WPA2、WPA3規格に対応しているものとする。WPA、WPA2、WPA3は、対向装置の認証と、対向装置との通信の暗号化を行う規格である。通信装置101、102は、WPA3規格に対応していることから、WPA3規格において暗号鍵を共有する方式であるSAE (Simultaneous Authentication of Equals) を用いることができる。また、6GHzでの通信ではこれまでの通信装置との相互接続性を考慮する必要がないため、Wi-Fi Allianceでは、6GHzでの通信を、WPA3を用いて認証、暗号化を行うことが決まっている。またWPA3では、暗号化方式としてTKIPやWEPではなく、AES-CCMPやAES-GCMPが用いられる。

[0030] 図2に、本実施形態における通信装置101のハードウェア構成例を示す。通信装置101は、記憶部201、制御部202、機能部203、入力部204、出力部205、通信部206およびアンテナ207を有する。尚、アンテナは複数でもよい。

[0031] 記憶部201は、ROMやRAM等の1以上のメモリにより構成され、後述する各種動作を行うためのコンピュータプログラムや、無線通信のための通信パラメータ等の各種情報を記憶する。ROMはRead Only Memoryの、RAMはRandom Access Memoryの夫々略である。尚、記憶部201として、ROM、RAM等のメモリの他に、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモリカード、DVDなどの記憶媒体を用いてもよい。また、記憶部201が複数のメモリ等を備えていてもよい。

[0032] 制御部202は、例えば、例えばCPUやMPU等の1以上のプロセッサにより構成され、記憶部201に記憶されたコンピュータプログラムを実行することにより、通信装置101の全体を制御する。尚、制御部202は、記憶部201に記憶されたコンピュータプログラムとOS（Operating System）との協働により、通信装置101の全体を制御するようにしてもよい。また、制御部202は、他の通信装置との通信において送信するデータや信号（無線フレーム）を生成する。尚、CPUはCentral Processing Unitの、MPUは、Micro Processing Unitの略である。また、制御部202がマルチコア等の複数のプロセッサを備え、複数のプロセッサにより通信装置101全体を制御するようにしてもよい。

[0033] また、制御部202は、機能部203を制御して、無線通信や、撮像、印刷、投影等の所定の処理を実行する。機能部203は、通信装置101が所定の処理を実行するためのハードウェアである。

[0034] 入力部204は、ユーザからの各種操作の受付を行う。出力部205は、

モニタ画面やスピーカーを介して、ユーザに対して各種出力を行う。ここで、出力部205による出力とは、モニタ画面上への表示や、スピーカーによる音声出力、振動出力などであってもよい。尚、タッチパネルのように入力部204と出力部205の両方を1つのモジュールで実現するようにしてもよい。また、入力部204および出力部205は、夫々通信装置101と一体であってもよいし、別体であってもよい。

[0035] 通信部206は、IEEE802.11b規格に準拠した無線通信の制御を行う。また、通信部206は、IEEE802.11b規格に加えて、他のIEEE802.11シリーズ規格に準拠した無線通信の制御や、有線LAN等の有線通信の制御を行ってもよい。通信部206は、アンテナ207を制御して、制御部202によって生成された無線通信のための信号の送受信を行う。

[0036] 尚、通信装置101が、IEEE802.11b規格に加えて、NFC規格やBluetooth規格等に対応している場合、これらの通信規格に準拠した無線通信の制御を行ってもよい。また、通信装置101が複数の通信規格に準拠した無線通信を実行できる場合、夫々の通信規格に対応した通信部とアンテナを個別に有する構成であってもよい。通信装置101は通信部206を介して、画像データや文書データ、映像データ等のデータを通信装置101と通信する。尚、アンテナ207は、通信部206と別体として構成されていてもよいし、通信部206と合わせて一つのモジュールとして構成されていてもよい。

[0037] アンテナ207は、2.4GHz帯、5GHz帯、および6GHz帯における通信が可能なアンテナである。本実施形態では、通信装置101は1つのアンテナを有するとしたが、3つのアンテナでもよい。または周波数帯ごとに異なるアンテナを有していてもよい。また、通信装置101は、アンテナを複数有している場合、各アンテナに対応した通信部206を有していてもよい。

[0038] 尚、通信装置102は通信装置101と同様のハードウェア構成を有する

。

[0039] 図3には、本実施形態における通信装置101の機能構成のブロック図を示す。尚、通信装置102も同様の構成である。ここでは通信装置101は無線LAN制御部301を備えるものとする。尚、無線LAN制御部の数は1つに限らず、2つでもよいし、3つ以上でも構わない。通信装置101は、さらに、フレーム生成部302、送信時間制御部303、ビーコン受信制御部304、UI制御部305および記憶部306、無線アンテナ307を有する。

[0040] 無線LAN制御部301は、他の無線LAN装置との間で無線信号を送受信するためのアンテナ並びに回路、およびそれらを制御するプログラムを含んで構成される。無線LAN制御部301は、IEEE802.11規格シリーズに従って、フレーム生成部302で生成されたフレームを元に無線LANの通信制御を実行する。

[0041] フレーム生成部302は、無線LAN制御部301で送信すべき無線制御フレームを生成する。フレーム生成部302で生成する無線制御の内容は記憶部305に保存されている設定によって制約を課してもよい。またUI制御部305からのユーザ設定によって変更してもよい。生成されたフレームの情報は無線LAN制御部301に送られ、通信相手に送信される。

[0042] 通信方式決定部303は、無線LAN制御部301から受け取った受信フレームおよびUI制御部305での設定情報から相手と通信する時に用いる通信形式を決定する。また決定した通信形式を認証方式決定部306に伝える。通信方式を決定した後、無線LAN制御部301は決定された通信方式に従って相手装置と通信を行う。

[0043] 認証方式決定部304は、通信方式決定部303からの情報およびUI制御部305での設定情報から相手装置を認証する方式を決定する。無線LAN制御部301は決定された認証方式に基づき相手装置を認証する。

[0044] UI制御部305は、APの不図示のユーザによるAPに対する操作を受け付けるためのタッチパネルまたはボタン等のユーザインタフェースに関わ

るハードウェアおよびそれらを制御するプログラムを含んで構成される。尚、UI制御部305は、例えば画像等の表示、または音声出力等の情報をユーザに提示するための機能も有する。

[0045] 記憶部306は、APが動作するプログラムおよびデータを保存するROMとRAM等によって構成されうる記憶装置である。

[0046] 図4は、IEEE802.11で定義されるRSNE (Robust Security Network element) である。RSNEは、IEEE802.11に準拠するマネジメントフレームに格納される。

[0047] Element IDフィールド401ではエレメントがRSNEであることを示す。すなわち値は48となる。

[0048] Pairwise Cipher Suite Countフィールド405には対応する暗号方式の数を示す。具体的な値はPairwise Cipher Suite Listフィールド406に示す。例えば、CCMP-128に対応する場合は00-0F-AC-04となる。Pairwise Cipher Suite Countフィールド405で複数対応することを示した場合、例えば405で2とした場合には506を複数連続させる。例えばCCMP-128、GCMP-128に対応する場合は00-0F-AC-04の後、00-0F-AC-08となる。この順は逆でもよい。また対応する数はいくつでもよい。

[0049] AKM Suite Countフィールド407には対応する認証方式の数を示す。具体的な値はAKM Suite Listフィールド408に示す。本実施形態では、WPA3-SAEのみをRSNEに付与するため、AKM Suite Countフィールド407は1とし、AKM Suite Listフィールド408はSAEを示す00-0F-AC-08とする。尚、この値はWPA3以降で規定される値であればよい。すなわちSAEでハッシュをSHA-384とする認証方式が00-0F-AC-14に追加された場合、上記に加えて示すようにしてもよい。また、SAEでFT (Fast Transition) を実施する00-0F-AC-

09を含めてもよい。ただし、対応するのはWPA3のみなので、PSKを示す00-0F-AC-02や00-0F-AC-06は含めない。

[0050] 図5はIEEE802.11に定義されるExtended Capabilityである。Extended Capabilityは、IEEE802.11に準拠するマネジメントフレームに格納される。

[0051] ここで示すフィールドは先頭からElement IDフィールド501、Lengthフィールド502、Extended Capabilitiesフィールド503である。

[0052] Extended Capabilitiesフィールド503には、SAE Password Identifiers In Useサブフィールド504、SAE Password Identifiers Used Exclusivelyサブフィールド505を含む。これらのフィールドは同じSSIDのネットワークを構築する際に、ユーザごとにパスワードを変更するためのIDを設定可能なPassword IDを用いた場合に有効にする。例えば構築したネットワークの一部をPassword IDありにした場合、SAE Password Identifiers In Useサブフィールド504を有効にする。構築したネットワークすべてをPassword IDありとした場合、当該サブフィールド504、当該サブフィールド505を有効にする。

[0053] これらの値は例えば、既存のネットワークに加えてMulti-Linkで6GHzを使用するネットワークを構築する時に有効にしてもよい。例えば、Multi-Link通信で6GHzを含むネットワークに接続するときはPassword IDを必須にすることで、Password IDに対応するWPA3を用いた接続を強制することができるようになる。Password IDを必須にするには、例えば対応機器は必ず所定の方式でつなげるためのビットを用意し、当該ビットを立てることなどが考えられる。

[0054] また例えば、Multi-Link通信で6GHzを含むネットワークを

構築する場合には必ず SAE Password Identifiers In Use サブフィールド 504 を有効にしてもよい。Password ID を用いることでパスワードの秘匿性が高くなるため、セキュリティが向上することが考えられる。そのため、Multi-Link 通信で 6 GHz を含むときには必ず Password ID を有効にすることで、通信装置 102 はより安全性の高いネットワークに構築することが可能になる。逆に、STA は SAE Password Identifiers In Use が無効になっていながら、Multi-Link 通信で 6 GHz を含むネットワークを構築している AP を信頼できないものとして接続しないように制御することもできる。また AP にとっても、Password ID に対応していない STA が接続要求してきたときには、当該 STA は信用できないものとして接続しないように制御してもよい。

[0055] 図 6 は IEEE 802.11 で定義される RSNXE (RSN Extension element) である。RSNXE は、IEEE 802.11 に準拠するマネジメントフレームに格納される。

[0056] ここで示すフィールドは先頭から Element ID フィールド 601、Length フィールド 602、Extended RSN Capabilities フィールド 603 である。

[0057] SAE hash-to-element サブフィールド 606 は WPA3 で規定する SAE 認証のうち、H2E (Hash to Element) 方式に対応していることを示す。SAE-PK サブフィールド 607 は SAE 認証のうち、SAE-PK (SAE Public Key) 方式に対応していることを示す。

[0058] SAE hash-to-element とは SAE の認証方式の 1 つであり、オフラインでやり取りすべきパラメータを事前に計算することができる。これにより、計算時間を基に算出値を推測するサイドチャネル攻撃を防ぐことができ、セキュリティを高めることができる。

[0059] そのため、例えば Multi-Link 通信で 6 GHz を含むネットワー

クを構築する場合には必ずSAE hash-to-elementサブフィールド606もしくはSAE-PKサブフィールド607を有効にすることとしてもよい。よって、Multi-Link通信で6GHzを含むときには必ずSAE hash-to-elementを有効にすることで、通信装置102はより安全性の高いネットワークに構築することが可能になる。逆に、通信装置102はSAE hash-to-elementが無効になりつつMulti-Link通信で6GHzを含むネットワークを構築しているAPを信頼できないものとして接続しないと判断することができるようになる。逆にAPにとっても、SAE hash-to-elementに対応していないSTAが接続してきたときには、そのSTAは信用できないものとして接続しないと判断できる。

[0060] また、SAE-PKとはSAEの認証方式の1つであり、STAが正規のAPと接続を試みているかを確認することができる方式である。STAが接続を確立しようとしているAPが偽のAPである場合は、STAが値を検証することで偽のAPと判定することができるようになる。これにより、公衆無線LANでのセキュリティ向上に貢献できる。よって、Multi-Linkで6GHzを含むときには必ずSAE-PKを有効にすることで、通信装置102はより安全性の高いネットワークに構築することが可能になる。逆に、通信装置102はSAE-PKが無効でありながら、Multi-Link通信でネットワークを構築しているAPを信頼できないものとして接続しないように制御できるようになる。またさらAPにとっても、SAE-PKに対応していないSTAが接続要求してきたときには、当該STAは信用できないものとして接続しないように制御できる。

[0061] 尚、上述したPassword ID、SAE hash-to-element、SAE-PKについてはAP、STAの接続判定条件として、いずれかに対応している場合にのみ接続し、いずれにも対応していない場合には接続しないものとしてもよい。

[0062] (処理の流れ)

(実施形態1)

図7を用いて、通信装置101の記憶部201に記憶されているプログラムを制御部202が実行することによって、Multi-Link通信を実行する際の周波数帯として6GHzが選択された場合にWPA3で認証、暗号化を行うように制御する処理を示す。通信装置101は少なくともMulti-Linkで通信可能な無線LAN制御部を有していることとする。

[0063] 図7のフローチャートは通信装置101がネットワークを構築するとき、もしくはユーザによってネットワーク設定の変更が指示されるときに開始する。

[0064] まず、通信装置101は無線設定画面をユーザに表示する(S701)。このとき表示する画面については図8から図19を用いて後述する。次に、画面上の設定する項目において通信を実行する周波数帯として6GHzが選択されているか否かを判定する(S702)。図8では、「基本(6GHz)」が選択されていることから、S702において、6GHzが選択されていると判定することができる。図9以降のS702の判定方法は後述する。S702において6GHzの設定画面が選択されていると判定された場合、GUIでの設定ではセキュリティ方式としてWPA3およびOWEのみを選択できるようにする(S710)。すなわち、RSNEに含まれるAKM Suite Listフィールド408に、WPA3-SAEのみ、あるいはWPA-EAPを含めてBeaconやProbe Response、Association Responseを送信する。

[0065] このときのGUIの例を図8に示す。図8では6GHzでのネットワーク構築を設定する画面を示している。6GHz帯での通信は、WPA3を用いて認証を行うことが必須であるため、図8に示されるセキュリティ方式にはWPA3を表示する。また、6GHz帯では、WPA/WPA2、OPENでの認証を行わないことが規定されている。そのため、無線の認証・暗号化方式としてOPEN(AES)、WPA3-SAE、WPA3-EAPのみが選択できるように表示する。このときの表示方法はこれに限定されない。

また例えば、OPEN (AES) の代わりに OWE、OPEN (暗号化あり)、OPEN (OWE)、OWE (パスワード無しの通信暗号化)、OWE (OPEN) などでも表現してもよい。OWE (Opportunistic Wireless Encryption) とはセキュリティ方式の1つであり、パスワードを用いない環境であっても通信を暗号化することが可能となる。そのため、通信内容の暗号化を行わない従来のOPENよりもセキュリティは向上できる。

[0066] WPA3-SAEも別の表現方法を用いてもよい。例えば、WPA3-Personal、WPA3、SAE、WPA3 (AES) などでも表現してもよい。WPA3-EAPも別の表現方法を用いてもよい。例えば、WPA3-Enterprise、WPA3、WPA3-Enterprise (192bit) などでも表現してもよい。WPA3-EnterpriseとWPA3-Enterprise (192bit) は別に選択肢を与えてもよい。

[0067] 図8に示す認証方式の選択肢として、図8に示す認証方式の一部を表示してもよい。例えばWPA3-SAEのみ選択肢として与えてもよい。この場合、6GHzの設定画面では表示部に、図8のようにWPA3に対応する選択肢を与えないで、予め決定された暗号化方式に基づいて暗号化を行ってもよい。図8に示す認証方式の選択肢はさらに増やしてもよい。例えばWPA3-SAE (H2E) やWPA3-SAE-PK、WPA3-SAE (Password ID)、WPA4などが選択肢に入ってもよい。ただし、WEP、WPA-TKIP、WPA-AES、WPA2-TKIP、WPA2-AESおよびそれと同等の方式を表現するものは選択肢に与えないか、選択できないようにして表示する。

[0068] S702において、6GHzの設定画面でないと判定された場合、Multi-Link通信を行うための設定画面か否かを判定する (S703)。図8を用いて説明すると、S703の判定は例えば、上部タブの「基本 (マルチ)」が選択されているか否かを判定する。ここで、S703においてM

Multi-Link通信を行うための設定画面ではないと判定された場合、GUIに表示される無線の認証・暗号化方式として、WPA3およびOWE以外にも、WPA2以前の方式を含めて選択可能な状態で表示する（S713）。また、図4のRSNEに含まれるAKM Suite Listフィールド408に、WPA2-AESを含めてビーコンやProbe Response、Association Responseを送信する。

[0069] このとき、すなわちS703においてMulti-Link通信を行うための設定画面ではないと判定された場合のGUIの例を図9に示す。図9では構築するネットワーク設定画面として「基本（2.4GHz）」が選択されており、2.4GHzでのネットワーク構築を設定する画面であることがわかる。この場合は、2.4GHzでのネットワーク構築を設定する画面、単一のネットワークを構築する画面である場合は、S703においてMulti-Link通信を行うための設定画面ではないと判定される。S703においてMulti-Link通信を行うための設定画面ではないと判定される場合は、図9に示すように、無線の認証・暗号化方式としてOPEN（AES）、WPA3-SAE、WPA3-EAP以外にOPEN、WPA2以前の方式が選択できるように表示する。すなわち、S703においてMulti-Link通信を行うための設定画面ではないと判定される場合は、S713においてWPA2以前の認証方式も含めて選択可能な状態で表示する。

[0070] 図9に示す認証方式の表示として、APの有する機能によって選択肢を変化させてもよい。例えばAPがEAPに対応していない場合、図9に示される選択肢からWPA2-EAP（AES）、WPA3-EAP（AES）、WPA2/WPA3-EAP（AES）を除いてもよい。

[0071] また例えば、APがPersonalに対応していない場合は、OPENとEAPのみを表示させてもよい。もしくはOPEN以外を選択肢に表示してもよい。（TKIP/AES）や（AES）の表記はなくてもよい。また、WPA2-PSK/WPA3-SAEの表記は異なるものでもよい。例え

ばWPA2/WPA3やWPA2/PA3-*Personal*であってもよい。WPA3-SAEも同様にWPA3、WPA3-*Personal*やWPA3-SAE (*Personal*) であってもよい。

[0072] OPEN (AES) は異なるものであってもよい。例えばOPEN (OWE) , OWE、WPA/WPA2-PSKはMIXと表示していてもよい。またWPA/WPA2/WPA3の表記があってもよい。これをWPA-MIXと表示してもよい。

[0073] また、図10のように「基本 (マルチ)」が選択されることで、Multi-Link通信を行うための設定画面であると判定してもよい。すなわち、図10のようにMulti-Link通信を行うことを意味する「基本 (マルチ)」が選択されることで、S703においてMulti-Link通信を行うための設定画面であると判定される。このとき、少なくとも一方のリンクにおいて6GHz帯で動作する周波数チャンネルが含まれる可能性があるか否かを判定する (S704)。S704における判定は、例えば図10のようにLinkごとに設定するチャンネルの周波数帯において6GHzの周波数帯が指定されることや、6GHzの周波数帯の具体的なチャンネルを指定されることで判定する。例えば図10ではLink1として「2.4GHz 自動」が選択されており、Link2として「5GHz 自動」が選択されている。この時にはMulti-Linkでも6GHzで動作しないことがわかる。すなわち、図10から2.4GHz帯と5GHz帯のMulti-Link通信を行うことが選択されているが、6GHz帯でMulti-Link通信を行わないことがわかる。この場合は、S704において6GHzで動作する周波数チャンネルが含まれる可能性がないと判定する。一方で図11の場合、Link1として「2.4GHz 自動」が選択されており、Link2として「6GHz 自動」が選択されている。この場合にはS704において、Multi-Linkで動作するチャンネルとして6GHzが含まれると判定される。また、図12のようにチャンネルを「自動」としてどの帯域でも動作可能な設定の場合においても、6GHzで動作する可能性

があるものとして判定してもよい。

[0074] 6GHzで動作する可能性がないと判定された場合（S704でNo）、WPA2以前の方式も含めて選択できるように表示する（S713）。このときの表示方法は例えば図10のようなものとなる。認証・暗号化方式の選択肢については前述の図9の説明と同様となるため省略する。図10はMulti-Link通信の設定画面であるが、6GHz周波数帯を用いた通信を選択されていないため、WPA2以前の認証方式に加えて、WPA3が認証方式の選択肢として表示される。

[0075] 6GHzを含む可能性があるかと判定された場合、すでに接続しているSTAが存在するか否かを確認する（S705）。尚、S705の判定はS701の直前に実施してもよいし、実施しなくてもよい。接続を確立するSTAが存在しない場合（S705でNo）、OPEN（AES）およびWPA3のみ表示されるように制御する（S710）。認証・暗号化方式の選択肢については前述の図8の説明と同様となるため省略する。

[0076] 設定更新時点で接続を確立するSTAがいる場合（S705でYes）、接続を確立するSTAがWPA2以前の認証・暗号化方式で接続を確立しているか否かを判定する（S706）。S706において、WPA3以降で接続を確立していると判定された場合、WPA3のみが選択されるように表示する（S710）。S706において、WPA2以前の方式で接続を確立していると判定された場合、設定変更後に6GHzを選択することでWPA3でのみネットワーク構築するため、WPA2以前の方式を用いて既に接続を確立しているSTAが再接続できなくなる可能性がある。そこで、図13に示すような警告を表示する（S707）。ここで、当該警告において、警告を了承する旨の「OK」が押下された場合（S708でYes）、接続を確立しているSTAを切断し、WPA3のみ選択されるように表示する（S710）。尚、接続を確立しているSTAとの切断は後述する「設定」ボタンが押下されたタイミング（S711）で実施してもよい。図13に示される警告において、「OK」が押下されず、「キャンセル」が押下された場合や

画面をそのまま閉じられた場合（S708でNo）、6GHzを含まないネットワークを構築する設定に変更する（S709）。S709は例えば、図11で選択された6GHzを図10で示されるように5GHzに変更するなどが考えられる。尚、S707～S709では既存のネットワーク、すなわち既にSTAと接続を確立しているネットワークとは別にネットワークを構築することを選択してもよい。この場合、認証・暗号化方式の選択肢は必ずWPA3が選択されるように表示する。既存のネットワークは別の画面で管理する。

[0077] この場合の例を図14、図15を示す。S703の段階では図14に示す設定画面であり、この状態でユーザが6GHzで動作することを選択した場合（S704でYes）、既存のネットワークでSTAが接続を確立しているか否かを判定する（S705）。すでに接続を確立しているSTAが存在した場合、警告を表示して（S707）、図15に遷移する。ここで、S707で表示する警告文は、例えば「新しくネットワークを構築してもよろしいですか？」などの確認である。すなわちS707において、既存のネットワークとは異なるネットワークを構築することをユーザに対して確認する。当該警告をユーザが了承し、「OK」を押下すると、図14に示す「ネットワーク1」の設定はそのままの状態ですべて「ネットワーク2」を新たに構築し、6GHz帯も追加して図15に示すような設定画面を表示する。図14ではネットワーク1において6GHzにチェックが入っていなかったが、図15ではネットワークが「ネットワーク2」となり、6GHz帯にチェックが入っていることがわかる。すなわち、既存のネットワークとは異なるネットワークを構築することをユーザが了承することで、既存のネットワーク（2.4GHz／5GHz）に加え、ネットワーク2に相当する6GHzのネットワークが構築される。また、図15では6GHzで動作するので、表示される認証・暗号化方式はOPEN（AES）、WPA3－SAEに限定される。すなわち、RSNEに含まれるAKM Suite Listフィールド408に、WPA3－SAEのみ、あるいはWPA－EAPを含めてBea

conやProbe Response、Association Responseを送信する。あるいは通信装置102に本発明を適用する場合、Probe RequestあるいはAssociation RequestのRSNEに付与する。

[0078] 通信装置101はWPA3-SAEでのネットワーク構築ができれば、対向装置からの接続要求を待つ。あるいは通信装置102に本発明を適用する場合は対向装置を探し、条件に合う対向機に対して接続要求を出すことになる。ここで接続要求とは、Probe RequestやAssociation Requestを指す。

[0079] 通信装置101は対向装置からの接続要求を受信した場合（S712）、対向装置がMulti-Linkで接続を要求してきていること、およびWPA3での接続を要求していることを判定する（S716）。具体的には、S712で受信したProbe RequestやAssociation RequestのAKM Suite Listフィールド408に、WPA3に対応可能であることを示す情報が格納されているか否かを確認する。S716において、対向装置がMulti-Linkにも関わらずWPA3での接続を要求していないと判定された場合は、接続を拒否する（S717）。ここで、S717において別のネットワークを推奨してもよい。あるいは、Multi-Link通信での接続を要求しているが、2.4GHzと5GHzしか含まない接続であれば、WPA2での接続要求に対して認証を進める処理に移ってもよい。ただし、この場合はあとから6GHzを増やすことが要求されたとしても必ず拒否する。

[0080] 尚、上述したようにMulti-Link通信で6GHzを含む接続においてPassowrd ID、SAE hash-to-element、SAE-PKを必須とする場合は、WPA3の判定に加えてこれらを接続承認の条件としてもよい。通信装置102に本発明を適用する場合は、APを探索する際に、上記を満たすネットワークを構築するAPにのみ接続要求を送信することになる。

- [0081] 通信装置101はSTAからの接続要求が条件を満たす場合、通信装置は、STAの認証を進める(S718)。S718において、認証が成功すると、(S719でYes)、対向装置と接続し、通信を開始する(S720)。認証が成功しなければ(S719でNo)、接続を拒否する(S717)。S717において接続を拒否する方法としては、Association ResponseでStatus CodeをFailureにすることなどが考えられる。
- [0082] S713の後、設定ボタンが押下されることで設定された認証・暗号化方式でのネットワークが構築される(S714)。ここではWPA2-PSK/WPA3-SAEが選択されたものとする。
- [0083] S713において、図4で示すRSNEのAKM Suite List フィールド408には、SAEに対応していることを示す値00-0F-AC-08の他、PSKに対応していることを示す値の00-0F-AC-02や00-0F-AC-06を含める。00-0F-AC-02はPSKでハッシュ関数としてSHA-128を使用することを示し、00-0F-AC-06はハッシュ関数としてSHA-256を使用することを示している。これらはどちらか一方のみ含めていてもよい。
- [0084] ネットワークを構築した後は対向装置が接続を要求してくるのを待機する(S715)。対向機装置が接続を要求してきたら認証を進め(S718)、認証が通れば(S719でYes)、接続し通信を開始する(S720)。認証が通らなければ(S719でNo)、接続を拒否する(S717)。
- [0085] 本実施形態によると、Multi-Link通信で6GHzを含む場合には、両リンクにおいてWPA3で認証するように表示を制御することで、6GHzでの通信ではWPA3に限定した通信を持続することが可能となる。また、6GHz帯を含まない場合についてはWPA2でも通信可能とすることで、既存のWPA3に対応していない機器でもネットワークに参加し通信することができるようになる。尚、上記で示した以外にもGUIで表示する方法は考えられる。以下に、複数のネットワークを構築できるAPの設定画

面を例示する。

- [0086] 図16に、複数のネットワークを構築できるAPのGUIの一例を示す。画面の左側にネットワークの種類を表示する。例えば無線LAN詳細設定(2.4GHz)ではSingle Linkでネットワーク構築を行うための、WPA2以前のセキュリティ方式やOpenを含んだ選択肢を表示する。一方で、図16にあるように無線LAN詳細設定(2.4+6)を選択した場合、2.4+6GHzでのMulti-Linkでネットワークを構築することを示す。この場合には、6GHz周波数帯を用いてMulti-Link通信を行うことが選択されているため、OWE、WPA3のみを選択できるように表示部に表示し、WPA2以前のセキュリティ方式やOpenは表示しない。
- [0087] 図17、18に、動作モード選択時に周波数帯を決定する場合のAPのGUIの一例を示す。図16では、無線チャンネルにおいて周波数帯を決定していたが、図17、18では動作モードにおいて周波数帯を決定する点異なる。
- [0088] 図17のように無線動作モードとして2.4GHz+5GHzを選択した場合、S704において6GHzでの動作は行わないと判定することができる。すなわち、Multi-Link通信を行うことが選択されているが、6GHzを用いずにMulti-Link通信を行うことが示されるため、セキュリティ方式としてはWPA2、Openを含んだ選択肢を表示する。
- [0089] 図18のように無線動作モードとして5GHz+6GHzを選択した場合、S704において6GHzで動作を行うと判定される。すなわち、6GHzを用いてMulti-Link通信を行うことが示されるため、OWE、WPA3のみを選択できるように表示部に表示し、WPA2以前のセキュリティ方式やOpenは表示しない。尚、Multi-Linkで選択される周波数チャンネルは例えば6GHzから2つ選択してもよい。もしくは2.4GHzから1つと5GHzから2つでもよい。
- [0090] 図19、20に、Multi-Link通信で動作する周波数帯を設定す

る画面とSecurityを設定する画面が別画面にて表示されるAPのUIの一例を示す。

[0091] 図19では、Multi-Linkの設定画面で、6GHzにチェックが入れているため、S704において、Multi-Linkにおいて6GHzで動作を行うと判定する。この場合にセキュリティ方式を設定する画面に遷移した際の一例を図20に示す。Multi-Linkにおいて6GHzで動作を行うと判定されたため、Security設定画面ではOWE、WPA3のみを選択できるように表示部に表示し、WPA2以前のセキュリティ方式やOpenは表示しない。尚、図19で6GHzにチェックが入っておらず、Multi-Linkにおいて6GHzで動作を行わないと判定された場合に、セキュリティ方式にはWPA3に加えて、WPA2、Openを含んだ選択肢を表示する。

[0092] 図21に、セキュリティ方式を選択する際にポップアウトする場合のUIの一例を示す。周波数帯の選択方法は図9～19と同様である。図21のようにセキュリティ方式を選択する際に、ポップアウトして選択肢を表示してもよい。6GHzを含むMulti-Link通信が選択された場合にはOWE、WPA3のみが選択されるように表示する。一方で、Multi-Link通信で6GHzを含まない選択となる場合に、セキュリティ方式にはWPA3に加えて、WPA2、Openを含んだ選択肢を表示する。

[0093] 図22に、グレースアウトすることで、特定のセキュリティ方式を選択できないように制御する場合のUIの一例を示す。例えば、6GHzを含むMulti-Link通信が選択された場合にはWPA3のみ選択できるようにし、WPA2以前のセキュリティ方式はグレースアウトさせることで選択できないようにする。

[0094] 図23に、無線機能を選択時に使用する無線チャネルを判定する場合のUIの一例を示す。例えば図23において、2.4GHz+5GHzを選択した場合、S704において、6GHz帯で動作しないと判定し、セキュリティ方式にはWPA3に加えて、WPA2、Openを含んだ選択肢を表示す

る。一方で例えば2.4GHz+6GHzを選択した場合、S704において、6GHzを含むMulti-Link通信を行うと判定し、OWE、WPA3のみが選択されるように表示する。

[0095] このようにネットワーク構築の際のUI上でもユーザの選択肢によって選択できるセキュリティ方式を限定することで、セキュリティ向上が実現できる。また、WPA2以前の認証・暗号化が禁止されている6GHzにおいてWPA2以前の方式で認証・暗号化した通信を実施することがなくなる。

[0096] 尚、UI上はMulti-Linkを選択していてもセキュリティ方式で与える選択肢を変更せず、実際にネットワークを構築する時に通信装置が自動でセキュリティ方式を切り替えていてもよい。例えば同時に複数のネットワークを構築する場合、UI上でWPA2/3が選択されたとする。Multi-Linkで6GHzを使用しないネットワークではWPA2/3で動作し、Multi-Linkで6GHzを使用するネットワークではWPA3のみで動作していてもよい。この場合、Multi-Linkで6GHzが選択された時点でWPA2のみの選択肢を外してもよいし、WPA2のみの選択肢はどのネットワークでも選択できないようにしていてもよい。この場合もMulti-Linkを使用する場合には高いセキュリティ方式での接続を保証することとなる。

[0097] (実施形態2)

本実施形態では、Multi-AP通信で6GHzが選択された場合にWPA3で認証、暗号化を行うように制御する場合について説明する。

[0098] 図24を用いて、通信装置101の記憶部201に記憶されているプログラムを制御部202が実行することによって、Multi-AP通信で6GHzが選択された際の処理の流れを示す。

[0099] Multi-AP通信とは、複数のAPが協調動作を行い、STAとデータ通信を行うことで、通信レートの向上やビームフォーミングを用いた電波干渉低減などの通信性能向上を可能にする技術である。Multi-AP通信に参加するAPは、他のAPを管理する1台のSharing APと、

Sharing APの管理下で動作するShared APに分類される。

[0100] 尚、前述した実施形態で説明済みの内容については本実施形態での説明を省略する。

[0101] 図24には本実施形態において通信装置101が通信装置102と接続するときの通信形式によってセキュリティ方式を選択するための処理をフローチャートで示している。

[0102] 通信装置101は少なくともMulti-APで通信可能な無線LAN制御部を有していることとする。

[0103] 図24のフローチャートは通信装置101がネットワークを構築するとき、もしくはユーザによってネットワーク設定の変更が指示されるときに開始する。

[0104] 処理の多くは実施形態1と重複するため説明を省略する。

[0105] 通信装置101は無線表示した後、Multi-APが選択されたか否かを判定する(S2403)。S2403において、Multi-AP通信が選択されたと判定された場合、S704の処理に進む。S2403においてMulti-AP通信が選択されたと判定されなかった場合、図7におけるS713に移る。

[0106] Multi-AP通信でネットワークを構築する際に、6GHzを使用してSTAと、あるいはAP間で通信するAPが含まれるか否かを判定する(S705)。6GHzを使用してSTAと、あるいはAP間で通信するAPが含まれる場合、S706に進む。S705において、含まれないと判定された場合は、S713に移り、S713においてWPA3に加えて、WPA2を含めて選択されるように表示する。

[0107] Multi-APで6GHzを含む構築したネットワークに対して接続を要求してきたSTAがWPA3で接続要求を送信しているか否かを判定し(S716)、S716においてWPA3での接続要求であった場合には認証を進める(S718)。S716においてにおいてWPA3での接続要求で

はないと判定された場合は接続を拒否する（S 7 1 7）。尚、W P A 3 の代わりに S A E - P K や S A E   h a s h - t o - e l e m e n t であってもよい。もしくは P a s s o w r d   I D を用いた接続要求に基づいて判断してもよい。

[0108]    また S 7 1 6 で接続要求する通信相手は A P でもよい。M u l t i - A P 通信でネットワークを構築する際に、W P A 3 が選択されるように表示を制御してもよい。W P A 3 のみに表示を制御する U I 表示方法は実施形態 1 と同様であるため説明を省略する。

[0109]    このように M u l t i - A P 通信において 6 G H z に対応したネットワークを構築する時にセキュリティ方式として W P A 3 が選択されるように制御することで W P A 2 以前の方式で通信を行わない、セキュリティを向上することができる。また、6 G H z 帯の通信において W P A 2 以前の方式を使用することがなくなる。

[0110]    （その他の実施形態）

各実施形態において設定チャンネルを「自動」と選択したときに 6 G H z を含む可能性があるものと判定し、W P A 3 および O P E N ( A E S ) のみ表示するように制御したが、これに限定されない。例えば、認証・暗号化方式として W P A 3 - S A E を選択した場合には 6 G H z を含めて M u l t i - L i n k の L i n k を構成する。W P A 2 - P S K / W P A 3 - S A E を選択した場合には 2 . 4 G H z 、 5 G H z でのみ M u l t i - L i n k の L i n k を構築する。という制御を実施してもよい。これにより、ユーザが帯域によるセキュリティ強度の規制について意識することなくネットワーク設定が可能となる。

[0111]    各実施形態では L i n k を 2 つとして G U I を示したが、3 つ以上あってもよい。例えば無線チャンネル ( L i n k 1 ) 、無線チャンネル ( L i n k 2 ) 、無線チャンネル ( L i n k 3 ) が G U I 画面上に表示されていてもよい。

[0112]    また、各実施形態において設定画面が W P A 2 となっていた際に、6 G H z を用いて通信を行うことを選択した時点で 2 . 4 G H z 、 5 G H z であっ

てもWPA3に自動的に切りかえる処理を行ってもよい。これにより、既存のネットワークがWPA2以前の認証・暗号化方式で動作していても、WPA3が選択されるように制御できる。このとき、パスフレーズはWPA2で使用していたものを再度使ってもよい。また、WPA3に変更した旨をユーザに通知してもよい。また、自動で切り替えようとしたときにWPA3に対応していないSTAが接続している場合、設定変更できないことをユーザに通知してもよい。

- [0113] 各実施形態において通信方式やセキュリティ方式の設定方法は画面によるものであったが、これに限らない。例えば、音声入力によって設定してもよい。もしくは文字列によるコマンド入力での設定でもよい。コマンド入力の場合、例えばMulti-LinkであるにもかかわらずWPA2のみを設定しようとしたときにErrorを表示し、設定できないことを示すものとしてもよい。
- [0114] 各実施形態において、ユーザが選択できない選択肢を選んだ際にエラー表示をするとしたが、それに合わせてピープ音を出力してもよい。
- [0115] 本実施形態では、WPA3を例に説明したが、今後WPA3の後継規格としてWPA4等が策定された場合にも適応可能である。
- [0116] 本実施形態に記載の通信装置101、102は印刷手段を有するプリンタであってもよい。プリンタとして動作する場合は、例えば相手装置と通信することで取得したデータを印刷することが可能である。
- [0117] また、本実施形態に記載の通信装置101、102は撮像手段を有するカメラであってもよい。カメラとして動作する場合は、例えば相手装置と通信することで撮像したデータを送信することが可能である。
- [0118] 尚、上述の機能を実現するソフトウェアのプログラムコードを記録した記録媒体をシステムあるいは装置に供給し、システムあるいは装置のコンピュータ（CPU、MPU）が記録媒体に格納されたプログラムコードを読み出し実行するようにしてもよい。この場合、記憶媒体から読み出されたプログラムコード自体が上述の実施形態の機能を実現することとなり、そのプログ

ラムコードを記憶した記憶媒体は上述の装置を構成することになる。

[0119] プログラムコードを供給するための記憶媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、磁気テープ、不揮発性のメモ리카ード、ROM、DVDなどを用いることができる。

[0120] また、コンピュータが読み出したプログラムコードを実行することにより、上述の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているOSが実際の処理の一部または全部を行い、上述の機能を実現してもよい。OSとは、Operating Systemの略である。

[0121] さらに、記憶媒体から読み出されたプログラムコードを、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込む。そして、そのプログラムコードの指示に基づき、機能拡張ボードや機能拡張ユニットに備わるCPUが実際の処理の一部または全部を行い、上述の機能を実現してもよい。

[0122] 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、ASIC）によっても実現可能である。

[0123] 本実施形態の開示は、以下の構成を含む。

[0124] （構成1）

WPA (Wi-Fi Protected Access) 2方式を用いた認証とWPA 3方式を用いた認証を実行可能な通信装置であって、周波数チャネルを介して前記通信装置と他の通信装置の間のリンクを確立する確立手段と、前記他の通信装置との通信の認証を制御する制御手段と、を有し、前記制御手段は、前記確立手段によって前記通信装置と前記他の通信装置との間で複数のリンクを確立した状態で前記他の通信装置と通信を行う際に、

前記複数のリンクの少なくとも1つで使用される周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記WPA3方式を用いて認証を実行することを特徴とする通信装置。

[0125] (構成2)

前記通信装置は前記通信装置と前記他の通信装置との間で複数のリンクを確立した状態で前記他の通信装置と通信を行う指示を受け付ける受付手段をさらに有し、前記受付手段によって、前記特定の周波数帯に含まれる周波数チャネルを用いて前記通信を行うことが指示されたことに基づいて、前記WPA3方式を用いて認証を実行するように表示部を制御することを特徴とする構成1に記載の通信装置。

[0126] (構成3)

前記確立手段によって、前記通信装置と前記他の通信装置との間で前記複数のリンクを確立した状態で前記他の通信装置と行う通信は、IEEE 802.11規格シリーズに準拠したMulti-Link通信であることを特徴とする構成1または2に記載の通信装置。

[0127] (構成4)

WPA(Wi-Fi Protected Access)2方式を用いた認証とWPA3方式を用いた認証を実行可能で、通信のアクセスポイントとして動作する通信装置であって、他の通信装置と通信を行う通信手段と、前記他の通信装置との通信の認証を制御する制御手段と、を有し、前記制御手段は、前記通信装置と前記他の通信装置との間で協調動作を行う通信で使用される周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記WPA3方式を用いて認証を行うように制御することを特徴とする通信装置。

[0128] (構成5)

前記通信装置は、前記通信装置と前記他の通信装置との間で協調動作を行う通信を実行する指示を受け付ける受付手段をさらに有し、前記受付手段によって、前記特定の周波数帯に含まれる周波数チャネルを用いて前記通信を

行うことが指示されたことに基づいて、前記W P A 3方式を用いて認証を実行するように表示部を制御することを特徴とする構成4に記載の通信装置。

[0129] (構成6)

前記通信装置は、前記W P A 3方式で認証を実行することを示す情報を格納したフレームを前記他の通信装置から受信しない場合に、前記他の通信装置と接続を確立しないように制御することを特徴とする構成1から5の何れか1つの構成に記載の通信装置。

[0130] (構成7)

第1のセキュリティ方式を用いた認証と第2のセキュリティ方式を用いた認証を実行可能な通信装置であって、周波数チャネルを介して前記通信装置と他の通信装置の間のリンクを確立する確立手段と、前記他の通信装置との通信の認証を制御する制御手段と、を有し、前記確立手段によって、前記通信装置と前記他の通信装置との間で複数のリンクを確立した状態で、前記他の通信装置と通信を行う際に、前記複数のリンクの少なくとも1つで使用される周波数チャネルが特定の周波数帯の周波数チャネルであることに基づいて、前記第1のセキュリティ方式を用いて認証を実行し、前記複数のリンクで使用される周波数チャネルがいずれも前記特定の周波数帯に含まれる周波数チャネルでないことに基づいて前記第1のセキュリティ方式または前記第2のセキュリティ方式を用いて認証を実行するように制御することを特徴とする通信装置。

[0131] (構成8)

前記通信装置は前記通信装置と前記他の通信装置との間で複数のリンクを確立した状態で前記他の通信装置と通信を行う指示を受け付ける受付手段をさらに有し、前記受付手段によって、前記特定の周波数帯に含まれる周波数チャネルを用いて前記通信を行うことが指示されたことに基づいて、前記第1のセキュリティ方式を用いて認証を実行するように表示部を制御することを特徴とする構成7に記載の通信装置。

[0132] (構成9)

前記確立手段によって、前記通信装置と前記他の通信装置との間で前記複数のリンクを確立した状態で前記他の通信装置と行う通信は、IEEE 802.11規格シリーズに準拠したMulti-Link通信であることを特徴とする構成7または8に記載の通信装置。

[0133] (構成10)

第1のセキュリティ方式を用いた認証と第2のセキュリティ方式を用いた認証を実行可能で、通信のアクセスポイントとして動作する通信装置であって、他の通信装置と通信を行う通信手段と、前記他の通信装置との通信の認証を制御する制御手段と、前記制御手段は、前記通信装置と前記他の通信装置との間で協調動作を行う通信で使用される周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記第1のセキュリティ方式を用いて認証を実行し、前記協調動作を行う通信で使用される周波数チャネルが前記特定の周波数帯に含まれる周波数チャネルでないことに基づいて前記第1のセキュリティ方式または前記第2のセキュリティ方式を用いて認証を実行するように制御することを特徴とする通信装置。

[0134] (構成11)

前記通信装置は、前記通信装置と前記他の通信装置とが協調動作を行う通信を実行する指示を受け付ける受付手段をさらに有し、前記受付手段によって、前記特定の周波数帯に含まれる周波数チャネルを用いて前記通信を行うことが指示されたことに基づいて、前記第1のセキュリティ方式を用いて認証を実行するように表示部を制御することを特徴とする構成10に記載の通信装置。

[0135] (構成12)

前記通信装置は、前記第1のセキュリティ方式で認証を実行することを示す情報を格納したフレームを前記他の通信装置から受信しない場合に、前記他の通信装置と接続を確立しないように制御することを特徴とする構成7から11の何れかの構成に記載の通信装置。

[0136] (構成13)

前記特定の周波数とは6GHz帯であることを特徴とする構成1から12の何れか1つの構成に記載の通信装置。

[0137] (構成14)

前記第1のセキュリティ方式は、WPA3 (Wi-Fi Protected Access) であることを特徴とする構成7から13の何れか1つの構成に記載の通信装置。

[0138] (構成15)

前記第2のセキュリティ方式はWPAまたはWPA2であることを特徴とする構成7から14の何れか1つの構成に記載の通信装置。

[0139] (構成16)

コンピュータを、構成1から15の何れかの1つの構成に記載された通信装置の各手段として機能させるためのプログラム。

[0140] 本発明は上記実施の形態に制限されるものではなく、本発明の精神及び範囲から離脱することなく、様々な変更及び変形が可能である。従って、本発明の範囲を公にするために以下の請求項を添付する。

[0141] 本願は、2021年6月9日提出の日本国特許出願特願2021-096515と2022年4月27日提出の日本国特許出願特2022-073892を基礎として優先権を主張するものであり、その記載内容の全てをここに援用する。

### 請求の範囲

- [請求項1]        W P A ( W i - F i   P r o t e c t e d   A c c e s s ) 2 方式を用いた認証とW P A 3 方式を用いた認証を実行可能な通信装置であって、
- 周波数チャネルを介して前記通信装置と他の通信装置の間のリンクを確立する確立手段と、
- 前記他の通信装置との通信の認証を制御する制御手段と、
- を有し、
- 前記制御手段は、前記確立手段によって前記通信装置と前記他の通信装置との間で複数のリンクを確立した状態で前記他の通信装置と通信を行う際に、前記複数のリンクの少なくとも1つで使用される周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記W P A 3 方式を用いて認証を実行することを特徴とする通信装置。
- [請求項2]        前記通信装置は前記通信装置と前記他の通信装置との間で複数のリンクを確立した状態で前記他の通信装置と通信を行う指示を受け付ける受付手段をさらに有し、
- 前記受付手段によって、前記特定の周波数帯に含まれる周波数チャネルを用いて前記通信を行うことが指示されたことに基づいて、前記W P A 3 方式を用いて認証を実行するように表示部を制御す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]        前記確立手段によって、前記通信装置と前記他の通信装置との間で前記複数のリンクを確立した状態で前記他の通信装置と行う通信は、
- I E E E 8 0 2 . 1 1 規格シリーズに準拠したM u t i - L i n k 通信であることを特徴とする請求項1 または2 に記載の通信装置。
- [請求項4]        前記通信装置は、前記W P A 3 方式で認証を実行することを示す情報を格納したフレームを前記他の通信装置から受信しない場合に、前記他の通信装置と接続を確立しないように制御することを特徴とする

請求項 1 に記載の通信装置。

[請求項5]        W P A ( W i - F i   P r o t e c t e d   A c c e s s ) 2 方式を用いた認証と W P A 3 方式を用いた認証を実行可能で、通信のアクセスポイントとして動作する通信装置であって、

他の通信装置と通信を行う通信手段と、

前記他の通信装置との通信の認証を制御する制御手段と、

を有し、

前記制御手段は、前記通信装置と前記他の通信装置との間で協調動作を行う通信で使用される周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記 W P A 3 方式を用いて認証を実行するように制御することを特徴とする通信装置。

[請求項6]        前記通信装置は、前記通信装置と前記他の通信装置との間で協調動作を行う通信を実行する指示を受け付ける受付手段をさらに有し、

前記受付手段によって、前記特定の周波数帯に含まれる周波数チャネルを用いて前記通信を行うことが指示されたことに基づいて、前記 W P A 3 方式を用いて認証を実行するように表示部を制御することを特徴とする請求項 4 に記載の通信装置。

[請求項7]        前記通信装置は、前記 W P A 3 方式で認証を実行することを示す情報を格納したフレームを前記他の通信装置から受信しない場合に、前記他の通信装置と接続を確立しないように制御することを特徴とする請求項 5 に記載の通信装置。

[請求項8]        第 1 のセキュリティ方式を用いた認証と第 2 のセキュリティ方式を用いた認証を実行可能な通信装置であって、

周波数チャネルを介して前記通信装置と他の通信装置の間のリンクを確立する確立手段と、

前記他の通信装置との通信の認証を制御する制御手段と、

を有し、

前記制御手段は、前記確立手段によって、前記通信装置と前記他の

通信装置との間で複数のリンクを確立した状態で、前記他の通信装置と通信を行う際に、前記複数のリンクの少なくとも１つで使用される周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記第１のセキュリティ方式を用いて認証を実行し、前記複数のリンクで使用される周波数チャネルがいずれも前記特定の周波数帯に含まれる周波数チャネルでないことに基づいて前記第１のセキュリティ方式または前記第２のセキュリティ方式を用いて認証を実行するように制御することを特徴とする通信装置。

[請求項9] 前記通信装置は前記通信装置と前記他の通信装置との間で複数のリンクを確立した状態で前記他の通信装置と通信を行う指示を受け付ける受付手段をさらに有し、

前記受付手段によって、前記特定の周波数帯に含まれる周波数チャネルを用いて前記通信を行うことが指示されたことに基づいて、前記第１のセキュリティ方式を用いて認証を実行するように表示部を制御することを特徴とする請求項８に記載の通信装置。

[請求項10] 前記確立手段によって、前記通信装置と前記他の通信装置との間で前記複数のリンクを確立した状態で前記他の通信装置と行う通信は、IEEE 802.11規格シリーズに準拠したMulti-Link通信であることを特徴とする請求項８または９に記載の通信装置。

[請求項11] 前記通信装置は、前記第１のセキュリティ方式で認証を実行することを示す情報を格納したフレームを前記他の通信装置から受信しない場合に、前記他の通信装置と接続を確立しないように制御することを特徴とする請求項８に記載の通信装置。

[請求項12] 第１のセキュリティ方式を用いた認証と第２のセキュリティ方式を用いた認証を実行可能で、通信のアクセスポイントとして動作する通信装置であって、

他の通信装置と通信を行う通信手段と、

前記他の通信装置との通信の認証を制御する制御手段と、

前記制御手段は、前記通信装置と前記他の通信装置との間で協調動作を行う通信で使用される周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記第1のセキュリティ方式を用いて認証を実行し、前記協調動作を行う通信で使用される周波数チャネルが前記特定の周波数帯に含まれる周波数チャネルでないことに基づいて前記第1のセキュリティ方式または前記第2のセキュリティ方式を用いて認証を実行するように制御することを特徴とする通信装置。

- [請求項13] 前記通信装置は、前記通信装置と前記他の通信装置とが協調動作を行う通信を実行する指示を受け付ける受付手段をさらに有し、  
前記受付手段によって、前記特定の周波数帯に含まれる周波数チャネルを用いて前記通信を行うことが指示されたことに基づいて、前記第1のセキュリティ方式を用いて認証を実行するように表示部を制御することを特徴とする請求項12に記載の通信装置。
- [請求項14] 前記通信装置は、前記第1のセキュリティ方式で認証を実行することを示す情報を格納したフレームを前記他の通信装置から受信しない場合に、前記他の通信装置と接続を確立しないように制御することを特徴とする請求項12に記載の通信装置。
- [請求項15] 前記特定の周波数帯とは6GHz帯であることを特徴とする請求項1、5、8、12に記載の通信装置。
- [請求項16] 前記第1のセキュリティ方式は、WPA3 (Wi-Fi Protected Access) であることを特徴とする請求項8または12に記載の通信装置。
- [請求項17] 前記第2のセキュリティ方式はWPAまたはWPA2であることを特徴とする請求項8または12に記載の通信装置。
- [請求項18] WPA (Wi-Fi Protected Access) 2方式を用いた認証とWPA3方式を用いた認証を実行可能な通信装置の通信方法であって、

周波数チャネルを介して前記通信装置と他の通信装置の間のリンクを確立する確立工程と、

前記他の通信装置との通信の認証を制御する制御工程と、  
を有し、

前記制御工程は、前記確立手段によって前記通信装置と前記他の通信装置との間で複数のリンクを確立した状態で前記他の通信装置と通信を行う際に、前記複数のリンクの少なくとも1つで使用される周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記WPA3方式を用いて認証を実行することを特徴とする通信装置の通信方法。

[請求項19]

WPA(Wi-Fi Protected Access)2方式を用いた認証とWPA3方式を用いた認証を実行可能で、通信のアクセスポイントとして動作する通信装置の通信方法であって、

他の通信装置と通信を行う通信工程と、

前記他の通信装置との通信の認証を制御する制御工程と、  
を有し、

前記制御工程は、前記通信装置と前記他の通信装置との間で協調動作を行う通信で使用される周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記WPA3方式を用いて認証を実行することを特徴とする通信装置の通信方法。

[請求項20]

第1のセキュリティ方式を用いた認証と第2のセキュリティ方式を用いた認証を実行可能な通信装置の通信方法であって、

周波数チャネルを介して前記通信装置と他の通信装置の間のリンクを確立する確立工程と、

前記他の通信装置との通信の認証を制御する制御工程と、  
を有し、

前記制御工程は、前記確立工程によって前記通信装置と前記他の通信装置との間で複数のリンクを確立した状態で、前記他の通信装置と

通信を行う際に、前記複数のリンクの少なくとも1つで使用される周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記第1のセキュリティ方式を用いて認証を実行し、前記複数のリンクで使用される周波数チャネルがいずれも前記特定の周波数帯に含まれる周波数チャネルでないことに基づいて、前記第1のセキュリティ方式または前記第2のセキュリティ方式を用いて認証を実行することを特徴とする通信装置の通信方法。

[請求項21]

第1のセキュリティ方式を用いた認証と第2のセキュリティ方式を用いた認証を実行可能で、通信のアクセスポイントとして動作する通信装置の通信方法であって、

通信のアクセスポイントとして動作する他の通信装置と通信を行う通信工程と、

前記他の通信装置との通信の認証を制御する制御工程と、  
を有し、

前記制御工程は、前記通信装置と前記他の通信装置とが協調動作を行う通信で使用する周波数チャネルが特定の周波数帯に含まれる周波数チャネルであることに基づいて、前記第1のセキュリティ方式を用いて認証を実行し、前記協調動作を行う通信で使用する周波数チャネルが前記特定の周波数帯に含まれる周波数チャネルでないことに基づいて、前記第1のセキュリティ方式または前記第2のセキュリティ方式を用いて認証を実行することを特徴とする通信装置の通信方法。

[請求項22]

コンピュータを、請求項1、5、8、12のいずれか1項に記載された通信装置の各手段として機能させるためのプログラム。