(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5590803号
(P5590803)

(45)発行日　平成26年9月17日(2014.9.17)　(24)登録日　平成26年8月8日(2014.8.8)

(51)Int.Cl.		F I		
H04L 9/08	(2006.01)	H04L	9/00	601B
G09C 1/00	(2006.01)	G09C	1/00	660E
H04L 29/08	(2006.01)	H04L	13/00	307Z
H04W 12/02	(2009.01)	H04W	12/02	

請求項の数 5　(全 29 頁)

(21)出願番号　特願2009-5132(P2009-5132)
(22)出願日　平成21年1月13日(2009.1.13)
(65)公開番号　特開2010-166169(P2010-166169A)
(43)公開日　平成22年7月29日(2010.7.29)
審査請求日　平成24年1月11日(2012.1.11)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】通信装置及び通信方法

(57)【特許請求の範囲】
【請求項１】
通信装置であって、
第１無線ネットワークにおいて無線通信するための所定の暗号鍵を他の通信装置と共有する通信パラメータ共有処理を実行する実行手段と、
前記他の通信装置と前記通信パラメータ共有処理において共有した前記所定の暗号鍵に基づいてデータを暗号化する暗号化手段と、
前記通信装置が前記第１無線ネットワークに接続するか、該第１の無線通信ネットワークと異なる第２無線ネットワークに接続するか否かを判定する判定手段と、
前記判定手段により前記通信装置が前記第１無線ネットワークに接続すると判定された場合に、前記他の通信装置を検索する第１の検索手段と、
前記判定手段により前記通信装置が前記第２無線ネットワークに接続すると判定された場合、及び、前記判定手段により前記通信装置が前記第１無線ネットワークに接続すると判定された場合であって前記第１の検索手段により前記他の通信装置が発見されなかった場合に、外部のサーバを検索する第２の検索手段と、
前記第１の検索手段により前記他の通信装置が発見された場合に、前記暗号化手段による暗号化が実行されずにデータを送信し、前記第２の検索手段により前記外部のサーバが発見された場合に、前記暗号化手段により暗号化されたデータを送信する送信手段と、
を有することを特徴とする通信装置。
【請求項２】

前記送信手段は、前記暗号化手段による暗号化が実行されずにデータを送信する場合に、該データを前記他の通信装置に直接送信し、前記暗号化手段により暗号化が実行されたデータを送信する場合に、該データを前記他の通信装置に間接的に送信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】

前記間接的に送信する場合とは、データを転送或いは一時的に保存するプロキシサーバを経由して送信する場合であることを特徴とする請求項２に記載の通信装置。

【請求項４】

通信装置にて実行される通信方法であって、

実行手段が、第１無線ネットワークにおいて無線通信するための所定の暗号鍵を他の通信装置と共有する通信パラメータ共有処理を実行する実行工程と、

暗号化手段が、前記他の通信装置と前記通信パラメータ共有処理において共有した前記所定の暗号鍵に基づいてデータを暗号化する暗号化工程と、

判断手段が、前記通信装置が前記第１無線ネットワークに接続するか、該第１の無線通信ネットワークと異なる第２無線ネットワークに接続するか否かを判定する判定工程と、

第１の検索手段が、前記判断手段により前記通信装置が前記第１無線ネットワークに接続すると判定された場合に、前記他の通信装置を検索する第１の検索工程と、

第２の検索手段が、前記判定手段により前記通信装置が前記第２無線ネットワークに接続すると判定された場合、及び、前記判定手段により前記通信装置が前記第１無線ネットワークに接続すると判定された場合であって前記第１の検索手段により前記他の通信装置が発見されなかった場合に、外部のサーバを検索する第２の検索工程と、

前記第１の検索手段により前記他の通信装置が発見された場合に、前記暗号化手段による暗号化が実行されずにデータを送信し、前記第２の検索手段により前記外部のサーバが発見された場合に、前記暗号化手段により暗号化されたデータを送信する送信工程と、

を有することを特徴とする通信方法。

【請求項５】

コンピュータを請求項１乃至３の何れか１項に記載の通信装置の各手段として機能させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、通信装置及び通信方法に関する。

【背景技術】

【０００２】

データを安全にアップロードしたい場合など、データを暗号化する技術がある。また、データに関係なく、常にＳＳＬ、ＩＰＳｅｃなどで通信路を暗号化する技術もある。

【０００３】

既に、安全な通信路を構築している場合、データそのものの暗号化及び通信路の暗号化といった二重の暗号化が行われている。従来、機器が接続するネットワークとは関係なしに同様の動作を行っている。

【０００４】

オフィス環境と移動環境の両方に接続可能な無線移動端末がオフィス環境と移動環境の判別を行い、移動環境に接続した場合、暗号化してオフィス内に設置された情報処理装置にデータを送信する技術が提案されている（例えば、特許文献１参照）。

【０００５】

オープンなネットワークに送信されるデータの場合は暗号化を行い、ユーザアクセスが制限されるネットワークに送信されるデータの場合は暗号化を行わない技術が提案されている（例えば、特許文献２参照）。

【特許文献１】特開平１０－１５０４５３号公報

【特許文献２】特開２０００－１３８７０３号公報

【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、上記従来例では、現在の接続ネットワーク及び接続先に応じて暗号化を行うか否かを決定していなかった。安全なネットワーク内でも、相手先によっては無駄な暗号化処理が行われるという問題があった。
【０００７】
本発明は、ネットワークに接続する通信装置が送信すべきデータの暗号化を実行するか否かを判定可能とすることを目的とする。
【課題を解決するための手段】
【０００８】
本発明は、通信装置であって、
第１無線ネットワークにおいて無線通信するための所定の暗号鍵を他の通信装置と共有する通信パラメータ共有処理を実行する実行手段と、
前記他の通信装置と前記通信パラメータ共有処理において共有した前記所定の暗号鍵に基づいてデータを暗号化する暗号化手段と、
前記通信装置が前記第１無線ネットワークに接続するか、該第１の無線通信ネットワークと異なる第２無線ネットワークに接続するか否かを判定する判定手段と、
前記判定手段により前記通信装置が前記第１無線ネットワークに接続すると判定された場合に、前記他の通信装置を検索する第１の検索手段と、
前記判定手段により前記通信装置が前記第２無線ネットワークに接続すると判定された場合、及び、前記判定手段により前記通信装置が前記第１無線ネットワークに接続すると判定された場合であって前記第１の検索手段により前記他の通信装置が発見されなかった場合に、外部のサーバを検索する第２の検索手段と、
前記第１の検索手段により前記他の通信装置が発見された場合に、前記暗号化手段による暗号化が実行されずにデータを送信し、前記第２の検索手段により前記外部のサーバが発見された場合に、前記暗号化手段により暗号化されたデータを送信する送信手段と、
を有することを特徴とする。
【０００９】
また、本発明は、通信装置にて実行される通信方法であって、
実行手段が、第１無線ネットワークにおいて無線通信するための所定の暗号鍵を他の通信装置と共有する通信パラメータ共有処理を実行する実行工程と、
暗号化手段が、前記他の通信装置と前記通信パラメータ共有処理において共有した前記所定の暗号鍵に基づいてデータを暗号化する暗号化工程と、
判断手段が、前記通信装置が前記第１無線ネットワークと接続するか、該第１の無線通信ネットワークと異なる第２無線ネットワークに接続するか否かを判定する判定工程と、
第１の検索手段が、前記判断手段により前記通信装置が前記第１無線ネットワークに接続すると判定された場合に、前記他の通信装置を検索する第１の検索工程と、
第２の検索手段が、前記判定手段により前記通信装置が前記第２無線ネットワークに接続すると判定された場合、及び、前記判定手段により前記通信装置が前記第１無線ネットワークに接続すると判定された場合であって前記第１の検索手段により前記他の通信装置が発見されなかった場合に、外部のサーバを検索する第２の検索工程と、
前記第１の検索手段により前記他の通信装置が発見された場合に、前記暗号化手段による暗号化が実行されずにデータを送信し、前記第２の検索手段により前記外部のサーバが発見された場合に、前記暗号化手段により暗号化されたデータを送信する送信工程と、
を有することを特徴とする。
【発明の効果】
【００１０】
本発明によれば、ネットワークに接続する通信装置が送信すべきデータの暗号化を実行

するか否かを判定可能とすることで、処理を軽減することができる。
【発明を実施するための最良の形態】
【００１１】
以下、図面を参照しながら発明を実施するための最良の形態について詳細に説明する。
【００１２】
［第１の実施形態］
図１は、第１の実施形態におけるネットワーク構成の一例を示す図である。図１に示すＬＡＮ１０１には、ＤＭＳ（デジタルメディアサーバ）１０３、アクセスポイント１０４、ルータ１０５が接続されている。また、ＬＡＮ１０１は、イーサネット（登録商標）、bluetooth（登録商標）、Zigbee、ＵＷＢの複合などでも良い。
【００１３】
そして、インターネット１００には、ルータ１０５、ホットスポット１０６、プロキシサーバ１０７が接続され、インターネット１００はＷＡＮ（ワイドエリアネットワーク）、ＬＡＮ（ローカルエリアネットワーク）、或いはそれらの複合でも良い。
【００１４】
通信装置であるネットワーク接続装置１０２は、アクセスポイント１０４を介してＬＡＮ１０１に接続可能である。また、ネットワーク接続装置１０２は、ＤＭＳ１０３の検索やＭ－ＤＭＵ（モバイルデジタルメディアアップローダ）機能を利用してＤＭＳ１０３に画像をアップロードすることができる。更に、ネットワーク接続装置１０２は、プロキシサーバ１０７の検索、ＴＣＰを利用してプロキシサーバ１０７にアップロードすることができる。
【００１５】
尚、ＤＭＳへのアップロード方法は、Ｍ－ＤＭＵに限らず、＋ＵＰ＋でも良く、ＴＣＰやＵＤＰを利用した他のアップロード方法などでも良い。また、プロキシサーバ１０７へのアップロード方法は、ＴＣＰに限らず、ＵＤＰ、ＵＤＰ／ＩＰＳｅｃ、ＴＣＰ／ＩＰＳｅｃ、ＳＳＬ、ＴＬＳ、ＤＴＬＳを利用した他のアップロード方法などでも良い。
【００１６】
ＤＭＳ１０３は、ＤＬＮＡ（デジタルリビングネットワークアライアンス）に対応し、ＤＭＳ＋Ｕｐｌｏａｄを利用してアップロードされたデータを受信する機能や、データを復号化する機能を備えている。尚、第１の実施形態のＤＭＳ１０３は、ＤＭＳに限らず、Ｍ－ＤＭＳ（モバイルデジタルメディアサーバ）を利用しても良い。
【００１７】
また、アップロードされたデータを受信する機能は、ＤＭＳ＋Ｕｐｌｏａｄに限らず、Ｍ－ＤＭＳ＋Ｕｐｌｏａｄでも良いし、ＴＣＰやＵＤＰを利用した他のアップロード方法などでも良い。
【００１８】
アクセスポイント１０４は、ＬＡＮ１０１における有線ＬＡＮと無線ＬＡＮに接続している。ルータ１０５は、インターネット１００とＬＡＮ１０１の両方に接続し、パケット転送などを制御する。ホットスポット１０６は、インターネット１００と接続された公衆ホットスポットである。また、ホットスポット１０６は、公衆ホットスポットに限らず、ホテル等の公衆ではない無線ＬＡＮ、携帯電話を利用した無線ＬＡＮなどでも良い。
【００１９】
プロキシサーバ１０７は、インターネット１００と接続され、ネットワーク接続装置１０２からデータの転送依頼を受けると、ＤＭＳ１０３にデータの転送を行う。
【００２０】
ここで、図１に示すネットワーク接続装置１０２の構成と機能モジュールを、図２及び図３を用いて説明する。
【００２１】
図２は、第１の実施形態におけるネットワーク接続装置１０２の構成の一例を示す図である。ここで第１の実施形態では、ネットワーク接続装置１０２としてデジタルカメラと

して説明するが、これに限定されるものではない。また、図３は、ネットワーク接続装置１０２における機能モジュールの構成の一例を示す図である。

【００２２】

図２に示すネットワーク接続装置１０２において、２００は被写体の光学像を撮像する撮像部、２０１は撮像部２００から出力された撮像画像を所定フォーマットの画像データに変換し、画像データに透かしデータを付与する画像処理部である。２０２は画像処理部２０１から出力された画像データに対して所定の高能率符号化（ＤＣＴ変換、量子化後に可変長符号化）を行う符号化／復号化部である。また、符号化／復号化部２０２は、記録再生部２０３から再生された圧縮画像データを伸長復号化し、その画像データを画像処理部２０１に供給する。

【００２３】

２０３は圧縮符号化された画像データを不図示の記録媒体に記録し、また、記録された画像データを再生する記録再生部である。２０４はネットワーク接続装置１０２における処理動作を指示する操作部である。２０５は制御部であり、マイクロコンピュータと所定のプログラムコードを記憶可能なメモリとを備え、ネットワーク接続装置１０２を構成する各処理部の動作を制御し、UPnPデバイスに関する処理なども行う。

【００２４】

２０６は撮像部２００にて撮像された画像をＥＶＦ（電子ビューファインダ）や、液晶パネル等を用いて表示する表示部、２０７は撮像部２００にて撮像された画像データなどを通信するインタフェースである。

【００２５】

２０８はネットワーク接続装置１０２の機能に関する情報や制御プログラムなどが格納されているＲＯＭである。尚、ネットワーク接続装置１０２は、画像データを符号化する技術として、例えば、ＪＰＥＧ（Joint Photographic Experts Group）方式を用いて圧縮符号化している。２０９はネットワークインターフェース（ＮＥＴＩＦ）であり、ネットワークを介して通信装置間のデータ転送を行うための制御や接続状況の診断を行う。

【００２６】

ここで、図３に示すネットワーク接続装置１０２の機能モジュールは、ＲＯＭ２０８に格納され、制御部２０５によって実行される。また、機能モジュールに含まれる一部或いは全部がハードウェア化されていても良い。

【００２７】

３００はＬＡＮ１０１に接続し、ＴＣＰ／ＩＰの処理を行うＴＣＰ／ＩＰ制御部である。３０１は暗号化判断部である。この暗号化判断部３０１は、通信パラメータ設定実行部３０５から通信パラメータ設定で取得した情報に基づき、ＭＡＣレイヤ検索実行部３０２に接続可能な無線ＬＡＮの検索を依頼する。そして、ＭＡＣレイヤ検索実行部３０２から検索した結果を受信すると、暗号化判断部３０１はその結果から、接続するネットワークを決定し、ネットワークに接続する。

【００２８】

また、暗号化判断部３０１は、ＭＡＣレイヤ検索実行部３０２の検索結果に応じて、ネットワークレイヤ検索実行部３０３に検索を依頼する。登録されたＳＳＩＤのネットワークに接続している場合、ネットワークレイヤ検索実行部３０３にＳＳＤＰによる検索を依頼し、ＤＭＳ１０３を検索する。ＳＳＩＤはService Set Identifierの略であり、ＳＳＤＰはSimple Service Discovery Protocolの略である。ここで、暗号化判断部３０１は、ＤＭＳ１０３を発見すると、データをＤＭＳ１０３に直接送信する。

【００２９】

また、暗号化判断部３０１は，登録されたＳＳＩＤでないネットワークに接続している場合、ネットワークレイヤ検索実行部３０３にＤＮＳ（Domain Name System）による検索を依頼し、プロキシサーバ１０７を検索する。ここで、暗号化判断部３０１は、プロキシサーバ１０７を発見すると、暗号化実行部３０４に送信するデータの暗号化を依頼する。暗号化判断部３０１は、暗号化されたデータをプロキシサーバ１０７に送信し、ＤＭＳ１

０３に転送するように、依頼する。
【００３０】
３０２はＭＡＣレイヤ実行部であり、ＳＳＩＤといったネットワーク識別子を利用したＭＡＣレイヤにおける検索を実行する。第１の実施形態では、無線ＬＡＮを利用しているが、これに限らず、bluetooth（登録商標）、Zigbee、ＵＷＢなどを利用しても良い。
【００３１】
３０３はネットワーク検索実行部であり、ＤＮＳ、ＤＤＮＳ（Dynamic DNS）、ｍＤＮＳ、ＳＳＤＰ、ＷＳ－Ｄｉｓｃｏｖｅｒｙ、ＳＩＰといったネットワークレイヤにおける検索を実行する。第１の実施形態では、ＳＳＤＰ及びＤＮＳを利用しているが、これに限らず、ＤＤＮＳ、ｍＤＮＳ、ＷＳ－Ｄｉｓｃｏｖｅｒｙ、ＳＩＰなどを利用しても良い。ＷＳ－ＤｉｓｃｏｖｅｒｙはWeb Services Dynamic Discoveryの略で、ＳＩＰはSession Initiation Protocolの略である。
【００３２】
３０４は暗号化実行部であり、暗号化判断部３０１の指示を受け、暗号化を実行する。第１の実施形態では、暗号化実行部３０４は、暗号化判断部３０１の依頼を受け、ＡＥＳ（Advanced Encryption Standard）を利用して画像データを暗号化している。しかし、暗号化方式はＡＥＳに限らず、ＤＥＳ（Data Encryption Standard）、Ｔｒｉｐｌｅ－ＤＥＳなどを適用しても良い。
【００３３】
３０５は通信パラメータ設定実行部であり、暗号化判断部３０１の指示を受けて、通信パラメータ設定を実行する。この通信パラメータ設定実行部３０５は、ＤＭＳ１０３からアクセスポイント１０４へ接続するためのパラメータやＤＭＳ１０３へアクセスするためのパラメータを受信し、通信パラメータとして設定する。
【００３４】
図４は、第１の実施形態におけるネットワーク接続装置１０２の設定処理を示すフローチャートである。まず、ユーザがアプリケーションを起動し、暗号化判断部３０１に通信パラメータ設定の開始を要求することで、処理が開始される。
【００３５】
ステップＳ４０１で、暗号化判断部３０１がアクセスポイント１０４とＤＭＳ１０３へアクセスするための通信パラメータ（図５参照）を取得するために、ＤＭＳ１０３と通信パラメータ設定を開始する。そして、暗号化判断部３０１が通信パラメータ設定実行部３０５に通信パラメータ設定の実行を指示する。
【００３６】
次に、ステップＳ４０２では、通信パラメータ設定実行部３０５がＤＭＳ１０３に通信パラメータ設定要求を送信する。一方、ＤＭＳ１０３が通信パラメータ設定実行部３０５からの通信パラメータ設定要求を受信すると、通信パラメータを作成し、通信パラメータ設定実行部３０５に送信する。
【００３７】
そして、ステップＳ４０３で、通信パラメータ設定実行部３０５がＤＭＳ１０３から、通信パラメータを受信し、通信パラメータの保存を行い、この処理を終了する。
【００３８】
図５は、第１の実施形態における通信パラメータの一例を示す図である。ネットワークの種類は、無線ＬＡＮやbluetooth（登録商標）などの無線ネットワークの種類を示し、この例では無線ＬＡＮを利用している。ネットワーク識別子は、ネットワークを判別するための識別子である。この例では、無線ＬＡＮを利用しているので、ＳＳＩＤにより識別される。ここでは、ＳＳＩＤ１が設定されている。
【００３９】
暗号鍵は、無線ネットワークを暗号化するため、或いは画像を暗号化するために用いる鍵である。この例では、ＰＳＫ１が設定されている。ホームサーバの発見プロトコルは、ネットワーク識別子で識別されるネットワーク内でホームサーバを発見するために利用す

るプロトコルである。この例では、ｓｓｄｐが設定されている。ホームサーバ識別子は、ホームサーバの発見プロトコルによってホームサーバを識別するための識別子である。この例では、ｓｓｄｐで利用するｕｕｉｄが設定されている。

【００４０】

外部サーバの発見プロトコルは、ネットワーク識別子に対応したネットワークの外から画像をアップロードする際に利用する外部サーバを発見するために利用するプロトコルである。この例では、ＤＮＳが設定されている。そして、外部サーバ識別子は、外部サーバの発見プロトコルで利用する外部サーバの識別子である。この例では、ＵＲＬが設定されている。

【００４１】

図５に示す例では、通信パラメータはそれぞれ一つであるが、一つに限らず、複数個のパラメータを持っても良い。例えば、パラメータが複数個の外部サーバの発見プロトコルを持ち、それぞれプロトコルに対応する複数の外部サーバの識別子を持っても良い。

【００４２】

図６は、ネットワーク接続装置１０２及びＤＭＳ１０３の設定処理の通信シーケンスを示す図である。まず、ネットワーク接続装置１０２が通信パラメータ取得要求メッセージＭ６０１をＤＭＳ１０３に送信する。これにより、ＤＭＳ１０３は、通信パラメータ取得要求メッセージＭ６０１に応じて、通信パラメータ設定プロトコルを実行する。そして、ＤＭＳ１０３は、アクセスポイント１０４の暗号鍵をネットワーク接続装置１０２に送信する。一方、ネットワーク接続装置１０２は、ＤＭＳ１０３から受信した通信パラメータを設定する。

【００４３】

尚、第１の実施形態では、アクセスポイント１０４の暗号鍵を利用しているが、これに限らず、有線ネットワークに利用する暗号鍵など別の暗号鍵を用いても実現できる。

【００４４】

図７は、ネットワーク接続装置１０２におけるアップロード処理を示すフローチャートである。まず、ステップＳ７０１において、ユーザがアプリケーションから暗号化判断部３０１にアップロードの開始を要求し、暗号化判断部３０１がアップロードの開始要求を受理すると、ステップＳ７０２へ処理を進める。

【００４５】

ステップＳ７０２では、暗号化判断部３０１がＭＡＣレイヤ検索実行部３０２にネットワークへの接続を要求する。そして、ＭＡＣレイヤ検索実行部３０２が通信パラメータのネットワークの種類から検索するネットワークを無線ＬＡＮとする。また、ＭＡＣレイヤ検索実行部３０２は通信パラメータのネットワーク識別子からＳＳＩＤ１を取得し、そのＳＳＩＤ１に該当するネットワークがあるか否かを判別する。

【００４６】

ここでＭＡＣレイヤ検索実行部３０２がＳＳＩＤ１に該当するネットワークを発見すると、登録済みネットワークを発見したとして、ステップＳ７０３へ処理を進める。また、ＭＡＣレイヤ検索実行部３０２がＳＳＩＤ１に該当するネットワークを発見できないと、登録外ネットワークを発見したとして、ステップＳ７０６へ処理を進める。

【００４７】

このステップＳ７０３では、暗号化判断部３０１がＭＡＣレイヤ検索実行部３０２から登録済みネットワークに接続したことを知らされ、暗号化判断部３０１はホームサーバにアップロードすると決定する。そして、暗号化判断部３０１は、ネットワークレイヤ検索実行部３０３に対して、ホームサーバの発見プロトコルのｓｓｄｐと、ホームサーバ識別子を利用したＤＭＳの検索を依頼する。ここで、ホームサーバ識別子は、図５に示すuuid:816c5df0-c2ed-11da-9216-0008741e9394である。

【００４８】

ネットワークレイヤ検索実行部３０３は、ＤＭＳの検索要求に応じてＤＭＳ検索を実行し、ステップＳ７０４へ処理を進める。このステップＳ７０４では、ネットワークレイヤ

検索実行部３０３が対応するＤＭＳを発見した場合、発見したＤＭＳ情報を暗号化判断部３０１に伝え、ステップＳ７０５へ処理を進める。また、ネットワークレイヤ検索実行部３０３が対応するＤＭＳを発見できなかった場合、未発見であることを暗号化判断部３０１に伝え、ステップＳ７０６へ処理を進める。

【００４９】

ステップＳ７０５では、暗号化判断部３０１はＤＭＳ情報に基づき画像をアップロードし、処理を終了する。また、ステップＳ７０６では、暗号化判断部３０１は外部サーバにアップロードすると決定する。そして、暗号化判断部３０１は、ネットワークレイヤ検索実行部３０３に対して、外部サーバのプロトコルのＤＮＳと、外部サーバ識別子を利用した外部サーバの検索を依頼する。外部サーバ識別子は、http://server.canon.com/である。ネットワークレイヤ検索実行部３０３は、外部サーバの検索要求に応じてＤＮＳの検索を実行し、ステップＳ７０７へ処理を進める。

【００５０】

ステップＳ７０７では、ネットワークレイヤ検索実行部３０３が対応する外部サーバを発見した場合、発見した外部サーバ情報を暗号化判断部３０１に送り、ステップＳ７０８へ処理を進める。また、ネットワークレイヤ検索実行部３０３が、対応する外部サーバを発見できなかった場合、未発見であることを暗号化判断部３０１に送り、この処理を終了する。

【００５１】

ステップＳ７０８で、暗号化判断部３０１は、暗号化実行部３０４に画像データの暗号化を依頼する。暗号化実行部３０４は、暗号鍵であるＰＳＫ１を利用して、画像データの暗号化を行う。そして、暗号化実行部３０４は、暗号化された画像データを暗号化判断部３０１に送る。これにより、暗号化判断部３０１は暗号化された画像データを外部サーバにアップロードし、この処理を終了する。

【００５２】

次に、ネットワーク接続装置１０２における動作概要を説明する。画像をアップロードする先の設定指示が行われると、ネットワーク接続装置１０２は、図４及び図６に従ってＤＭＳ１０３から通信パラメータを受信する。そして、ネットワーク接続装置１０２は、通信パラメータに含まれる暗号鍵を利用して、アクセスポイント１０４に接続することができる。

【００５３】

ネットワーク接続装置１０２が画像のアップロードを開始する際に、アクセスポイント１０４の電波を受信可能な状況な場合、ネットワーク接続装置１０２は、ＤＭＳ１０３に画像をアップロードする。

【００５４】

図８は、ネットワーク接続装置１０２がアクセスポイント１０４に接続し、ＤＭＳ１０３に画像をアップロードするシーケンスを示す図である。ここで、ネットワーク接続装置１０２は、暗号化判定を行い、画像アップロードメッセージＭ８０１をアクセスポイント１０４を介してＤＭＳ１０３へ送り、画像を平文のままＤＭＳ１０３にアップロードする。尚、ネットワーク接続装置１０２は、アクセスポイント１０４に無線接続されている。また、ネットワーク接続装置１０２とアクセスポイント１０４の間の無線区間は、暗号鍵によって暗号化されている。

【００５５】

図９は、ネットワーク接続装置１０２が、ホットスポット１０６の近くに移動した場合を示す構成図である。図９において、ネットワーク接続装置１０２が画像のアップロード指示を受け付けると、図６に示すフローチャートに従って、登録外のネットワークであるホットスポット１０６を発見する。ネットワーク接続装置１０２は、そのホットスポット１０６に接続し、暗号化した画像をプロキシサーバ１０７にアップロードする。

【００５６】

プロキシサーバ１０７は、暗号化された画像データを受信し、ＤＭＳ１０３に転送する

。ＤＭＳ１０３は、暗号化された画像データを取得する。ＤＭＳ１０３は、必要に応じて暗号化された画像データを共通鍵ＰＳＫ１により復号化を行う。

【００５７】

図１０は、ネットワーク接続装置１０２がホットスポット１０６に接続し、プロキシサーバ１０７に画像をアップロードするシーケンスを示す図である。ネットワーク接続装置１０２は、検索の結果、プロキシサーバ１０７に画像をアップロードすると判断すると、画像の暗号化処理を行う。そして、ネットワーク接続装置１００２は、画像アップロードメッセージＭ１０００をプロキシサーバ１０７に送信する。画像アップロードメッセージＭ１０００には、暗号化処理が行われたアップロード対象の画像が含まれている。

【００５８】

一方、プロキシサーバ１０７では、画像アップロードメッセージＭ１０００に含まれる暗号化処理が行われたアップロード対象の画像をＤＭＳ１０３に転送する。これにより、ＤＭＳ１０３は、暗号化処理が行われた画像データを取得することができる。

【００５９】

プロキシサーバ１０７上では、暗号化された画像データしかないので、画像そのものを覗き見ることができない。このように、本発明では、プロキシサーバ１０７が悪意のあるサーバであった場合も、画像そのものは暗号化されているため、覗き見られることがなくなるという効果がある。

【００６０】

以上のように、ネットワーク接続装置１０２は、安全にプロキシサーバ１０７を介したアップロードを行うことができる。

【００６１】

［第２の実施形態］

次に、図面を参照しながら本発明に係る第２の実施形態を詳細に説明する。第２の実施形態のネットワーク接続装置１０２は、無線ネットワークインターフェースと有線ネットワークインターフェースを保持している。尚、第２の実施形態におけるネットワーク構成は、図１に示す第１の実施形態と同じであり、説明は省略する。

【００６２】

図１１は、第２の実施形態におけるネットワーク接続装置１０２の機能モジュール構成の一例を示す図である。図１１に示す１１０１は有線ネットワークと無線ネットワークを判別するネットワークインターフェース判断部である。ＬＡＮにおける有線ネットワークと無線ネットワークの判別を行っているが、これに限るものではない。

【００６３】

図１２は、第２の実施形態におけるネットワーク接続装置１０２のアップロード処理を示すフローチャートである。ステップＳ１２０１で、ユーザがアプリケーションから暗号化判断部３０１にアップロードの開始を要求する。暗号化判断部３０１は、アップロードの開始要求を受理すると、ステップＳ１２０２で、ネットワークインターフェース判別部１１０１に現在利用するネットワークインターフェースの判断を依頼する。ネットワークインターフェース判断部１１０１は、有線ＬＡＮを利用すると判断すると、暗号化判断部３０１に判断結果を伝え、ステップＳ１２０４へ処理を進める。また、ネットワークインターフェース判断部１１０１が無線ＬＡＮを利用すると判断すると、暗号化判断部３０１に判断結果を伝え、ステップＳ１２０３へ処理を進める。

【００６４】

このステップＳ１２０３では、暗号化判断部３０１は、ＭＡＣレイヤ検索実行部３０２にネットワークへの接続を要求する。ＭＡＣレイヤ検索実行部３０２が通信パラメータのネットワークの種類から検索するネットワークを無線ＬＡＮとする。また、ＭＡＣレイヤ検索実行部３０２は、通信パラメータのネットワーク識別子からＳＳＩＤ１を取得して、ＳＳＩＤ１に該当するネットワークがあるか否かを判別する。ここで、ＭＡＣレイヤ検索実行部３０２がＳＳＩＤ１に該当するネットワークを発見すると、登録済みネットワークを発見したとしてステップＳ１２０４へ処理を進める。ＭＡＣレイヤ検索実行部３０２が

、ＳＳＩＤ１に該当するネットワークを発見できないと、登録外ネットワークを発見したとしてステップＳ１２０７へ処理を進める。

【００６５】

ステップＳ１２０４で、暗号化判断部３０１がＭＡＣレイヤ検索実行部３０２から登録済みネットワークに接続したことを知らされ、ホームサーバにアップロードすると決定する。暗号化判断部３０１は、ネットワークレイヤ検索実行部３０３に対してホームサーバの発見プロトコルのｓｓｄｐと、ホームサーバ識別子を利用したＤＭＳの検索を依頼する。ここで、ホームサーバ識別子はuuid:816c5df0-c2ed-11da-9216-0008741e9394である。ネットワークレイヤ検索実行部３０３は、ＤＭＳの検索要求に応じて、ＤＭＳ検索を実行し、ステップＳ１２０５へ処理を進める。

【００６６】

ステップＳ１２０５では、ネットワークレイヤ検索実行部３０３が、対応するＤＭＳを発見した場合、発見したＤＭＳ情報を暗号化判断部３０１に伝え、ステップＳ１２０６へ処理を進める。また、ネットワークレイヤ検索実行部３０３が、対応するＤＭＳを発見できなかった場合、未発見であることを暗号化判断部３０１に伝え、ステップＳ１２０７へ処理を進める。

【００６７】

ステップＳ１２０６で、暗号化判断部３０１は、ＤＭＳ情報を元に画像をアップロードし、処理を終了する。

【００６８】

ステップＳ１２０７で、暗号化判断部３０１は、外部サーバにアップロードすると決定する。暗号化判断部３０１は、ネットワークレイヤ検索実行部３０３に対して、外部サーバのプロトコルのＤＮＳと、外部サーバ識別子のhttp://server.canon.com/を利用した外部サーバの検索を依頼する。ネットワークレイヤ検索実行部３０３は、外部サーバの検索要求に応じて、ＤＮＳの検索を実行し、ステップＳ１２０８へ処理を進める。

【００６９】

ステップＳ１２０８で、ネットワークレイヤ検索実行部３０３が対応する外部サーバを発見した場合、発見した外部サーバ情報を暗号化判断部３０１に送り、ステップＳ１２０９へ処理を進める。ネットワークレイヤ検索実行部３０３が、対応する外部サーバを発見できなかった場合、未発見であることを暗号化判断部３０１に送り、処理を終了する。

【００７０】

ステップＳ１２０９で、暗号化判断部３０１がアップロードの方法を判断する。ＤＭＳ１０３がウェブサーバの機能を持ち、ルータによってＮＡＴ設定などが行われている場合、外部に公開することができる。このように、ＤＭＳ１０３が公開されている場合、外部にいるネットワーク接続装置１０２は直接ＤＭＳ１０３にアップロードすることが可能になる。また、暗号化判断部３０１は、ＤＭＳ１０３に直接アップロードと判断した場合、ステップＳ１２１０へ処理を進める。

【００７１】

暗号化判断部３０１は、プロキシサーバ１０７を経由してアップロードすると判断した場合、ステップＳ１２１１へ処理を進める。尚、プロキシは一例であり、間接的にデータを送信する方法であれば、これに限るものではない。例えば、一時的にサーバに保存した後、ＤＭＳ１０３に転送する等を適用することもできる。

【００７２】

ステップＳ１２１０で、暗号化判断部３０１は、ＤＭＳ１０３とのアップロードに利用する通信路が暗号化されているか否かを判断する。ここで、ネットワーク接続装置１０２とＤＭＳ１０３の間で既にＩＰＳｅｃが利用されている場合、通信路が暗号化されていると判断する。尚、ＩＰＳｅｃは一実施例であり、ＩＰＳｅｃに限らず、ＳＳＬなどの他の通信路を暗号化する方式を適用することもできる。

【００７３】

暗号化判断部３０１が、アップロードに利用する通信路が暗号化されていると判断する

と、ステップＳ１２０６へ処理を進める。暗号化判断部３０１が、アップロードに利用する通信路が暗号化されていないと判断するとステップＳ１２１１へ処理を進める。

【００７４】

ステップＳ１２１１で、暗号化判断部３０１は、暗号化実行部３０４に画像データの暗号化を依頼する。暗号化実行部３０４は、暗号鍵であるＰＳＫ１を利用して、画像データの暗号化を行う。暗号化実行部３０４は、暗号化された画像データを暗号化判断部３０１に送る。暗号化判断部３０１は、暗号化された画像データを外部サーバにアップロードし、処理を終了する。

【００７５】

図１３は、ネットワーク接続装置１０２がホットスポット１０６に接続し、ＩＰＳｅｃを利用して画像をアップロードするシーケンスを示す図である。この場合、ネットワーク接続装置１０２はＤＭＳ１０３とＩＰＳｅｃによる安全な通信路を確保している。即ち、ネットワーク接続装置１０２は安全な通信路を確保していると判断し、アップロードする画像の暗号化を行わない。

【００７６】

ネットワーク接続装置１０２は、安全な通信路を利用して、暗号化されていない画像をコンテンツ取得要求メッセージＭ１３００によりＤＭＳ１０３にアップロードする。ＤＭＳ１０３は、画像データを取得することができる。

【００７７】

第２の実施形態によれば、二重暗号化などの無駄な処理を抑制し、暗号化処理のオーバヘッドを小さくするといった効果がある。更に、有線ネットワーク、無線ネットワークに対応しており、有線ネットワーク、無線ネットワークを意識する事無く利用でき、操作が簡単になるといった効果がある。

【００７８】

［第３の実施形態］

次に、図面を参照しながら本発明に係る第３の実施形態を詳細に説明する。尚、第３の実施形態におけるネットワーク接続装置１０２の構成は、第２の実施形態と同様であり、その説明は省略する。

【００７９】

第３の実施形態の通信パラメータは、複数のホームサーバの発見プロトコルと対応するホームサーバ識別子及び複数の外部サーバの発見プロトコルと対応する外部サーバ識別子を含む。

【００８０】

図１４は、第３の実施形態における通信パラメータの一例を示す図である。第３の実施形態でも、ネットワーク接続装置１０２が取得するものとする。

【００８１】

ネットワークの種類は、無線ＬＡＮやbluetooth（登録商標）など無線ネットワークの種類を示す。この例では、無線ＬＡＮを利用している。説明の便宜上、一つのネットワークの種類しか含まないが、ネットワークの種類を複数個有し、最適なものを選択しても良い。ネットワーク識別子は、ネットワークを判別するための識別子である。この例では、無線ＬＡＮを利用しているので、ＳＳＩＤにより識別される。ＳＳＩＤ１が設定されている。説明の便宜上、一つネットワーク識別子しか含まないが、ネットワーク識別子を複数個有し、最適なものを選択しても良い。

【００８２】

暗号鍵は、無線ネットワークを暗号化するためや画像を暗号化するために利用する鍵である。この例では、ＰＳＫ１が設定されている。第一のホームサーバの発見プロトコルは、ネットワーク識別子に示したネットワーク内でホームサーバを発見するために利用するプロトコルである。この例では、ｓｓｄｐが設定されている。第一のホームサーバ識別子は、ホームサーバの発見プロトコルによってホームサーバを識別するための識別子である。この例では、ｓｓｄｐで利用するｕｕｉｄが設定されている。

【００８３】
第二のホームサーバの発見プロトコルは、ネットワーク識別子に示すネットワーク内でホームサーバを発見するために利用するプロトコルである。この例では、ｍＤＮＳが設定されている。第二のホームサーバ識別子は、ホームサーバの発見プロトコルによってホームサーバを識別するための識別子である。この例では、ｍＤＮＳで利用するＵＲＬが設定されている。
【００８４】
第一の外部サーバの発見プロトコルは、ネットワーク識別子に対応したネットワーク外から画像をアップロードする際に利用する外部サーバを発見するために利用するプロトコルである。この例では、ＤＮＳが設定されている。第一の外部サーバ識別子は、外部サーバの発見プロトコルで利用する外部サーバの識別子である。この例では、ＵＲＬが設定されている。
【００８５】
第二の外部サーバの発見プロトコルは、ネットワーク識別子に対応したネットワーク外から画像をアップロードする際に利用する外部サーバを発見するために利用するプロトコルである。この例では、ＳＩＰが設定されている。第二の外部サーバ識別子は、外部サーバの発見プロトコルで利用する外部サーバの識別子である。この例では、ＳＩＰのＵＲＩが設定されている。
【００８６】
図１５は、第３の実施形態におけるネットワーク接続装置１０２のアップロード処理を示すフローチャートである。ステップＳ１５０１で、ユーザがアプリケーションから暗号化判断部３０１にアップロードの開始を要求する。暗号化判断部３０１が、アップロードの開始要求を受理すると、ステップＳ１５０２へ処理を進める。
【００８７】
ステップＳ１５０２で、暗号化判断部３０１は、ネットワークインターフェース判別部１１０１に現在利用するネットワークインターフェースの判断を依頼する。ネットワークインターフェース判別部１１０１が、有線ＬＡＮを利用すると判断すると、暗号化判断部３０１に判断結果を伝え、ステップＳ１５０４へ処理を進める。ネットワークインターフェース判別部１１０１が無線ＬＡＮを利用すると判断すると、暗号化判断部３０１に判断結果を伝え、ステップＳ１５０３へ処理を進める。
【００８８】
説明の便宜上、ネットワークの種類とネットワーク識別子を一つしか持っていないが、一つに限らず、複数のネットワークの種類とネットワーク識別子を保持しても良い。その場合、ステップＳ１５０２で、複数のネットワークの種類とネットワーク識別子から最適なネットワークを選択し、複数のネットワークの内、一つ以上のネットワークを検索する。
【００８９】
ステップＳ１５０３で、暗号化判断部３０１は、ＭＡＣレイヤ検索実行部３０２にネットワークへの接続を要求する。ＭＡＣレイヤ検索実行部３０２は、通信パラメータのネットワークの種類から検索するネットワークを無線ＬＡＮとする。また、ＭＡＣレイヤ検索実行部３０２は、通信パラメータのネットワーク識別子からＳＳＩＤ１を取得し、ＳＳＩＤ１に該当するネットワークがあるか否かを判別する。ＭＡＣレイヤ検索実行部３０２が、ＳＳＩＤ１に該当するネットワークを発見すると、登録済みネットワークを発見したとしてステップＳ１５０４へ処理を進める。ＭＡＣレイヤ検索実行部３０２が、ＳＳＩＤ１に該当するネットワークを発見できないと、登録外ネットワークを発見したとしてステップＳ１５０９へ処理を進める。
【００９０】
ステップＳ１５０４で、暗号化判断部３０１は、ＭＡＣレイヤ検索実行部３０２から登録済みネットワークに接続したことを知らされる。暗号化判断部３０１は、ＤＭＳ１０３にアップロードすると決定する。次に、暗号化判断部３０１は、通信パラメータからＤＭ

Ｓ１０３を発見するパラメータを決定する。ここでは、第一のホームサーバの発見プロトコルと第一のホームサーバ識別子を利用する。これらの第一の発見プロトコルを実行済みの場合、暗号化判断部３０１は、第二のホームサーバの発見プロトコルと第二のホームサーバ識別子を利用する。

【００９１】

説明の便宜上、順番に実行しているが、これに限らず、同時に検索を行っても良いし、第二のホームサーバの発見プロトコルと第二のホームサーバ識別子から利用しても良い。また、パラメータの選択方法による制限はない。例えば、どのネットワークに接続しているかにより、検索方法を変更しても良い。また、前回検索で発見できたパラメータを記憶しておき、そのパラメータで実行しても良い。

【００９２】

ステップＳ１２０５で、暗号化判断部３０１は、ＭＡＣレイヤ検索実行部３０２から登録済みネットワークに接続したことを知らされる。暗号化判断部３０１は、ホームサーバにアップロードすると決定する。暗号化判断部３０１は、ネットワークレイヤ検索実行部３０３に対して、ステップＳ１５０４で決定されたホームサーバの発見プロトコルと、ステップＳ１５０４で決定されたホームサーバ識別子を利用したＤＭＳの検索を依頼する。ネットワークレイヤ検索実行部３０３は、ＤＭＳの検索要求に応じて、ＤＭＳ検索を実行し、ステップＳ１５０６へ処理を進める。

【００９３】

ステップＳ１５０６で、ネットワークレイヤ検索実行部３０３が、対応するＤＭＳを発見した場合、発見したＤＭＳ情報を暗号化判断部３０１に伝え、ステップＳ１５０７に進む。ネットワークレイヤ検索実行部３０３が、対応するＤＭＳを発見できなかった場合、未発見であることを暗号化判断部３０１に伝え、ステップＳ１５０８へ処理を進める。

【００９４】

ステップＳ１５０７で、暗号化判断部３０１は、発見されたＤＭＳ情報を元に画像をアップロードし、処理を終了する。

【００９５】

ステップＳ１５０８で、暗号化判断部３０１は、検索を実行していないホームサーバのパラメータが存在するか否かを判断する。暗号化判断部３０１が検索を実行していない自宅パラメータが存在すると判断すると、ステップＳ１５０４へ処理を進める。暗号化判断部３０１が検索を実行していないホームサーバのパラメータが存在すると判断すると、ステップＳ１５０９へ処理を進める。

【００９６】

ステップＳ１５０９で、暗号化判断部３０１は、登録外ネットワークに接続したと判断する。暗号化判断部３０１は、プロキシサーバ１０７にアップロードすると決定する。次に、暗号化判断部３０１は、通信パラメータからプロキシサーバ１０７を発見するパラメータを決定する。ここでは、第一の外部サーバの発見プロトコルと第一の外部サーバ識別子を利用する。第一の外部サーバの発見プロトコルを実行済みの場合、暗号化判断部３０１は、第二の外部サーバの発見プロトコルと第二の外部サーバ識別子を利用する。

【００９７】

説明の便宜上、順番に実行しているが、これに限らず、同時に検索を行っても良いし、第二の外部サーバの発見プロトコルと第二の外部サーバ識別子から利用しても良い。この例では、パラメータの選択方法による制限はない。例えば、どのネットワークに接続しているかにより、検索方法を変更しても良い。また、前回検索で発見できたパラメータを記憶しておき、そのパラメータで実行しても良い。

【００９８】

ステップＳ１５１０で、暗号化判断部３０１は、ネットワークレイヤ検索実行部３０３に対して、ステップＳ１５０９で決定した外部サーバの発見プロトコルと、外部サーバ識別子を利用した外部サーバの検索を依頼する。ネットワークレイヤ検索実行部３０３は、外部サーバの検索要求に応じて、プロキシサーバ１０７の検索を実行し、ステップＳ１５

１１へ処理を進める。
【００９９】
ステップＳ１５１１で、ネットワークレイヤ検索実行部３０３が、対応する外部サーバを発見した場合、発見した外部サーバ情報を暗号化判断部３０１に送り、ステップＳ１５１３へ処理を進める。ネットワークレイヤ検索実行部３０３が、対応する外部サーバを発見できなかった場合、未発見であることを暗号化判断部３０１に送り、ステップＳ１５１２へ処理を進める。
【０１００】
ステップＳ１５１２で、暗号化判断部３０１は、検索を実行していない外部サーバのパラメータが存在するか否かを判断する。暗号化判断部３０１が検索を実行していない自宅パラメータが存在すると判断すると、ステップＳ１５０４へ処理を進める。暗号化判断部３０１が検索を実行していない外部サーバのパラメータが存在すると判断すると、ステップＳ１５０９へ処理を進める。
【０１０１】
ステップＳ１５１３で、暗号化判断部３０１が、アップロードの方法を判断する。ＤＭＳ１０３がウェブサーバの機能を持ち、ルータによってＮＡＴ設定などが行われている場合、外部に公開することができる。このようにＤＭＳ１０３が公開されている場合、外部にいるネットワーク接続装置１０２は直接ＤＭＳ１０３にアップロードすることが可能になる。
【０１０２】
暗号化判断部３０１は、ＤＭＳ１０３に直接アップロードと判断した場合、ステップＳ１５１４へ処理を進める。暗号化判断部３０１は、プロキシサーバ１０７を経由してアップロードすると判断した場合、ステップＳ１５１５へ処理を進める。プロキシは一例であり、間接的にデータを送信する方法であれば、これに限るものではない。例えば、一時的にサーバに保存した後、ＤＭＳ１０３に転送する等を適用することもできる。
【０１０３】
ステップＳ１５１４で、暗号化判断部３０１は、ＤＭＳ１０３とのアップロードに利用する通信路が暗号化されているか否かを判断する。ネットワーク接続装置１０２とＤＭＳ１０３の間で既にＩＰＳｅｃが利用されている場合、通信路が暗号化されていると判断する。本実施形態において、ＩＰＳｅｃは一例であり、ＩＰＳｅｃに限らず、ＳＳＬなどの他の通信路を暗号化する方式を適用することもできる。暗号化判断部３０１が、アップロードに利用する通信路が暗号化されていると判断すると、ステップＳ１５０７へ処理を進める。暗号化判断部３０１が、アップロードに利用する通信路が暗号化されていないと判断するとステップＳ１５１５へ処理を進める。
【０１０４】
ステップＳ１５１５で、暗号化判断部３０１は、暗号化実行部３０４に画像データの暗号化を依頼する。暗号化実行部３０４は、暗号鍵であるＰＳＫ１を利用して、画像データの暗号化を行う。暗号化実行部３０４は、暗号化された画像データを暗号化判断部３０１に送る。暗号化判断部３０１は、暗号化された画像データを外部サーバにアップロードし、処理を終了する。
【０１０５】
第３の実施形態によれば、複数の検索を実行することによる無駄な処理を抑制するといった効果がある。結果として、暗号化判断までの時間が短くなり、データ送信までの時間を短縮できるという効果がある。
【０１０６】
［第４の実施形態］
次に、図面を参照しながら本発明に係る第４の実施形態を詳細に説明する。
【０１０７】
図１６は、第４の実施形態におけるネットワークの構成の一例を示す図である。ネットワーク接続装置１６００及びＶｉｅｗｅｒ１６０１以外は第１の実施形態と同様の構成に

なっている。
【０１０８】
ネットワーク接続装置１６００は、ＬＡＮ１０１を介してアクセスポイント１０４と接続している。また、ＬＡＮ１０１を介してルータ１０５に接続しており、インターネット１００を介した通信が可能である。
【０１０９】
更に、ネットワーク接続装置１６００は無線ＬＡＮの通信パラメータ提供機能も所持しており、無線ＬＡＮの通信パラメータ設定プロトコルを用いて、通信パラメータの提供を行う。この例では、無線ＬＡＮの通信パラメータ設定プロトコルを用いてアクセスポイント１０４の無線ＬＡＮ通信パラメータが提供可能である。
【０１１０】
更に、ネットワーク接続装置１６００はＤＭＳの機能を有しており、画像等のコンテンツをＤＭＰ（デジタルメディアプレーヤ）等に提供可能である。
【０１１１】
Ｖｉｅｗｅｒ１６０１は無線ＬＡＮ通信機能を有しており、アクセスポイント１０４を介してＬＡＮ１０１に接続することができる。また、Ｖｉｅｗｅｒ１６０１は、ＤＭＰの機能を有しており、ＤＭＳ（ネットワーク接続装置）１６００を検索し、ＤＭＳのコンテンツを再生することができる。
【０１１２】
また、Ｖｉｅｗｅｒ１６０１は無線ＬＡＮの通信パラメータ設定プロトコルを有しており、ネットワーク接続装置１６００との間で通信パラメータ設定プロトコルの実行が可能である。
【０１１３】
尚、ネットワーク接続装置１６００及びＶｉｅｗｅｒ１６０１以外は第１の実施形態と同様であり、説明は省略する。
【０１１４】
図１７は、第４の実施形態におけるネットワーク接続装置１６００の構成の一例を示す図である。１７００は通信等によってネットワーク装置１６００に転送された画像を所定フォーマットの画像データに変換し、画像データに透かしデータを付与する画像処理部である。１７０１は画像処理部１７００から出力された画像データに対して所定の高能率符号化（例えば、ＤＣＴ変換、量子化後に可変長符号化）を行う符号化／復号化部である。符号化／復号化部１７０１は圧縮画像データを画像記憶部１７０２へ転送或いは画像記憶部１７０２から取得した画像データの符号化／復号化も行う。画像記憶部１７０２は画像を記憶し、要求に応じて画像の供給を行う。
【０１１５】
また、１７０３はネットワーク接続装置１６００における処理動作を指示する操作部である。１７０４はマイクロコンピュータと所定のプログラムコードを記憶可能なメモリとを具備し、ネットワーク接続装置１６００を構成する各処理部の動作を制御し、ＵＰｎＰデバイスに関する処理なども行う。
【０１１６】
１７０５は画像処理部１７００にて画像記憶部１７０２から取得され、画像処理された画像データなどを通信するインタフェースである。１７０６はネットワーク接続装置１６００の機能に関する情報が格納されているＲＯＭである。１７０７はネットワークインタフェースであり、ネットワークを介して情報処理装置間のデータ転送を行うための制御や接続状況の診断を行う。尚、ネットワーク接続装置１６００は、画像データを符号化する技術として、例えばＪＰＥＧ方式を用いて圧縮符号化している。
【０１１７】
図１８は、第４の実施形態におけるネットワーク接続装置１６００のモジュール構成を示す図である。ネットワーク接続装置１６００のモジュールは、ＲＯＭ１７０６に記憶され、制御部１７０４によって実行される。ネットワーク接続装置１６００のモジュールに

含まれる一部或いは全部がハードウェア化されていても良い。

【０１１８】

通信制御部１８００は、ＬＡＮ１０１に接続し、他の通信装置と通信処理を行う。要求元判断部１８０１は他の通信装置からの画像データの要求メッセージを受信し、その要求メッセージの要求元が同一のサブネットワーク内にあるか否かを判断する。また、要求元とセキュアな通信が確立されているか否かの判断や要求元に画像データを送信するか否かの判定も可能である。

【０１１９】

暗号化判断部１８０２は、要求元判断部１８０１及び管理部１８０５の情報に基づいて要求された画像データの暗号化を行うか否かの判断を行う。暗号化実行部１８０３は暗号化判断部１８０２により暗号化を行うことが決定された場合に、管理部１８０５の情報を用いて画像データの暗号化を行う。

【０１２０】

通信パラメータ設定プロトコル実行部１８０４は、通信パラメータ設定プロトコルの開始メッセージを受信し、通信パラメータ設定プロトコル処理を行う。通信パラメータ設定プロトコル処理が正常に終了した端末装置にアクセスポイントの通信パラメータの提供を行う。

【０１２１】

管理部１８０５は、通信パラメータ設定プロトコル実行部１８０４にて通信パラメータ設定を行った端末情報の登録及び管理を行う。ここで、端末の管理情報として、端末識別子と提供した通信パラメータ内に含まれる共通鍵の情報が登録端末リストとして登録及び管理される。また、管理情報は暗号化判断部１８０２及び暗号化実行部１８０３にて利用される。

【０１２２】

ここで、第４の実施形態では、Ｖｉｅｗｅｒ１６０１がアクセスポイント１０４に無線ＬＡＮで接続し、ネットワーク接続装置１６００から画像コンテンツをダウンロードし、Ｖｉｅｗｅｒ１６０１にて画像の再生を行うものとする。

【０１２３】

この際、Ｖｉｅｗｅｒ１６０１は、アクセスポイント１０４との無線ＬＡＮの通信パラメータをアクセスポイント１０４及びネットワーク接続装置１６００との間で通信パラメータ設定プロトコルによって取得する。

【０１２４】

以下、第４の実施形態における動作例を、図１９、図２０、図２１、図２２及び図２３を用いて説明する。

【０１２５】

図１９は、第４の実施形態におけるネットワーク接続装置１６００の通信パラメータ設定処理を示すフローチャートである。ネットワーク接続装置１６００が無線ＡＬＮ端末から通信パラメータ取得要求を受信すると（Ｓ１９０１）、通信パラメータ設定プロトコル処理を開始する（Ｓ１９０２）。通信パラメータ設定プロトコル処理が正常に処理されると、ネットワーク接続装置１６００に登録されているアクセスポイントの通信パラメータを通信パラメータ取得要求元へ転送する。

【０１２６】

次に、通信パラメータ設定プロトコル処理の後、登録端末リストに登録されている端末か否かの判定を行う（Ｓ１９０３）。判定の結果、登録端末リストに未登録の端末である場合は、端末情報（端末識別子）及び送信した通信パラメータ内に含まれる共通鍵を登録端末リストに新規登録端末として登録する（Ｓ１９０５）。一方、登録端末リストに登録済みの端末の場合には、端末情報に応じた共通鍵の更新を行う（Ｓ１９０４）。そして、端末リストへの登録が終了後、通信パラメータ設定処理を終了する。

【０１２７】

図２０は、第４の実施形態におけるネットワーク接続装置１６００のダウンロード処理

を示すフローチャートである。ステップＳ２００１で、ダウンロード要求を受信すると、ステップＳ２００２へ処理を進める。ステップＳ２００２では、受信したダウンロード要求の要求元端末が登録端末リストに登録済みの端末か否かの判定を行う。この登録済みの端末か否かはＭＡＣアドレスを登録端末識別子として判定処理に用いる。ここでは、ダウンロード要求のメッセージに要求元端末のＭＡＣアドレスを含め、そのＭＡＣアドレスと登録端末リストのＭＡＣアドレスとの比較により、登録端末か否かの判定を行う。

【０１２８】

判定の結果、登録端末と判定された場合には、ステップＳ２００３へ処理を進めるが、登録端末ではないと判定された場合には、ステップＳ２００７へ処理を進める。ステップＳ２００７では、ダウンロード拒否の旨を含めたダウンロード応答を送信し、この処理を終了する。

【０１２９】

一方、ステップＳ２００３では、ダウンロード要求送信元端末が同一のサブネット内にあるか否かのネットワーク判定処理を行う。このネットワーク判定処理において、同一のサブネット内であると判定された場合には、ステップＳ２００５へ処理を進めるが、同一のサブネット内でないと判定された場合には、ステップＳ２００４へ処理を進める。

【０１３０】

ステップＳ２００４では、要求元との通信がセキュアか否かの判定を行う。セキュアか否かとは、例えばＳＳＬを用いた通信か否かを判定する。判定の結果、通信がセキュアであると判定された場合は、ステップＳ２００５へ処理を進める。一方、通信がセキュアでないと判定された場合は、ステップＳ２００６へ処理を進める。

【０１３１】

ステップＳ２００５では、要求された画像を暗号化せずに送信する旨を含めたダウンロード応答を送信し、ステップＳ２００９へ処理を進める。一方、ステップＳ２００６では、要求された画像を暗号化して送信する旨を含めたダウンロード応答を送信し、ステップＳ２００８へ処理を進める。そして、ステップＳ２００８で、要求された画像を登録端末リストに登録されている端末識別子に対応した共通鍵を用いて画像を暗号化し、ステップＳ２００９へ処理を進める。最後に、ステップＳ２００９では、要求された画像の送信を行い、この処理を終了する。

【０１３２】

図２１は、Ｖｉｅｗｅｒ１６０１、アクセスポイント１０４、ネットワーク接続装置１６００間の通信パラメータ設定及びコンテンツ転送のシーケンスを示す図である。まず、Ｖｉｅｗｅｒ１６０１がアクセスポイント１０４との通信パラメータを取得するために、通信パラメータ取得要求メッセージＭ２１０１を送信する。そして、アクセスポイント１０４が通信パラメータ取得要求メッセージＭ２１０１をネットワーク接続装置１６００へ転送する。

【０１３３】

次に、ネットワーク接続装置１６００が通信パラメータ取得要求メッセージＭ２１０１を受信すると、Ｖｉｅｗｅｒ１６０１とアクセスポイント１０４を介して通信パラメータ設定プロトコルＭ２１０２を開始する。そして、通信パラメータ設定プロトコル処理によりＶｉｅｗｅｒ１６０１はアクセスポイント１０４の通信パラメータを取得する。第４の実施形態におけるアクセスポイント１０４の通信パラメータを図２２に示す。

【０１３４】

図２２は、第４の実施形態におけるネットワーク接続装置１６００が所持するアクセスポイント１０４の通信パラメータを示す図である。

【０１３５】

ネットワーク識別子は、ネットワークを判別するための識別子である。ここでは、無線ＬＡＮを利用しているため、ＳＳＩＤにより識別される。ＳＳＩＤ２が設定される。

【０１３６】

暗号鍵は無線ＬＡＮネットワークを暗号化するための共通鍵である。この共通鍵を用い

てコンテンツの暗号化も行われる。
【０１３７】
認証方式は無線ＬＡＮネットワーク暗号化に用いられる認証方式が記載される。ここでは、ＷＰＡ－ＰＳＫが設定されている。
【０１３８】
暗号方式は無線ＬＡＮネットワークの暗号化に用いられる暗号方式である。ここでは、ＴＫＩＰが設定されている。
【０１３９】
更には、拡張としてデバイス情報等も含むことが可能である。ここでは、ネットワーク接続装置１６００のデバイス情報としてＤＭＳである旨が設定されている。
【０１４０】
次に、Ｖｉｅｗｅｒ１６０１はアクセスポイント１０４の通信パラメータを取得した後、自機器にこの通信パラメータを設定することによりアクセスポイント１０４を介したデータ通信が可能になる。その際、Ｖｉｅｗｅｒ１６０１とアクセスポイント１０４との間は、通信パラメータに設定されている暗号方式・暗号鍵等によってセキュアな通信路が確立される。
【０１４１】
その後、ネットワーク接続装置１６００は通信パラメータ設定プロトコル処理が正常に終了した端末を登録端末リスト（図２３）に登録する。第４の実施形態では、登録端末として端末のＭＡＣアドレスを登録する。
【０１４２】
図２３に示す例では、Ｖｉｅｗｅｒ１６０１のＭＡＣアドレス００：ＦＥ：９８：ＤＣ：７６：ＢＡが登録端末リストに登録される。また、登録には提供した通信パラメータの共通鍵（ＰＳＫ２）も共に登録される。
【０１４３】
Ｖｉｅｗｅｒ１６０１は通信パラメータ設定処理が終了した後、ネットワーク接続装置１６００が所持するコンテンツの取得要求として、コンテンツ取得要求メッセージＭ２１０３を送信する。ここで、Ｖｉｅｗｅｒ１６０１は自ＭＡＣアドレス（００：ＦＥ：９８：ＤＣ：７６：ＢＡ）をコンテンツ取得要求メッセージＭ２１０１のペイロード内に含めて送信するものとする。
【０１４４】
そして、ネットワーク接続装置１６００がコンテンツ取得要求メッセージＭ２１０３を受信すると、コンテンツの暗号化を行うか否かの暗号化判定処理を行う。
【０１４５】
まず、登録端末か否かの登録端末判定処理（図２０のＳ２００２）を行う。コンテンツ取得要求メッセージＭ２１０１のペイロード内に含まれるＭＡＣアドレスが登録端末リストに登録されているか否かの判定を行う。ここでＶｉｅｗｅｒ１６０１のＭＡＣアドレスは登録端末リストに登録されているので、登録端末リストに登録済みの端末であると判定される。
【０１４６】
次に、ネットワーク接続装置１６００は登録端末判定処理の後、ネットワーク判定処理を行う。ここでは、登録端末リストに登録された端末かをコンテンツ取得要求メッセージＭ２１０１のＥｔｈｅｒヘッダに含まれる送信元ＭＡＣアドレスと登録端末リストの登録端末のＭＡＣアドレスとの比較を行う。
【０１４７】
ここで、コンテンツ取得要求メッセージのＥｔｈｅｒヘッダの送信元ＭＡＣアドレスはＶｉｅｗｅｒ１６０１のＭＡＣアドレス（００：ＦＥ：９８：ＤＣ：７６：ＢＡ）であり、登録端末のＭＡＣアドレスであると判定される。従って、Ｖｉｅｗｅｒ１６０１は同一のサブネット内の端末と判断され、コンテンツの暗号化は行わないと判定される。
【０１４８】

ネットワーク接続装置１６００はコンテンツ取得要求メッセージＭ２１０３の応答として、コンテンツ取得応答メッセージＭ２１０４をＶｉｅｗｅｒ１６０１へ送信する。第４の実施形態では、コンテンツ取得応答メッセージＭ２１０４にはコンテンツを非暗号化で送信する旨のメッセージが含まれる。

【０１４９】

次に、コンテンツ取得応答メッセージＭ２１０４を送信した後、ネットワーク接続装置１６００は要求されたコンテンツを暗号化せずに、Ｖｉｅｗｅｒ１６０１へ送信する（Ｍ２１０４）。

【０１５０】

次に、第４の実施形態における他の動作例を説明する。この例では、ネットワーク接続装置１６００の登録端末リストに登録済みのＶｉｅｗｅｒ１６０１がホットスポット１０６のエリアに移動し、ホットスポット１０６からインターネットを経由してコンテンツをダウンロードする。

【０１５１】

また、Ｖｉｅｗｅｒ１６０１がホットスポット１０６に無線ＬＡＮにて接続しており、ネットワーク接続装置１６００と接続するための情報が予め設定されているものとする。ここで、接続するための情報は、例えばルータ１０５を介してネットワーク接続装置１６００と通信可能なポート情報やネットワーク接続装置１６００のｄＤＮＳ（ｄｙｎａｍｉｃ　ＤＮＳ）情報・ＵＲＬ情報などである。この情報を用いてＶｉｅｗｅｒ１６０１はネットワーク接続装置１６００と接続し、通信路が確立されているものとする。

【０１５２】

図２４は、Ｖｉｅｗｅｒ１６０１、ホットスポット１０６、ルータ１０５、ネットワーク接続装置１６００間の通信パラメータ設定及びダウンロードのシーケンスを示す図である。まず、Ｖｉｅｗｅｒ１６０１からホットスポット１０６、インターネット１００、ルータ１０５を介してネットワーク接続装置１６００にコンテンツ取得要求メッセージＭ２２０１を送信する。ここでは、Ｖｉｅｗｅｒ１６０１は自ＭＡＣアドレス（００：ＦＥ：９８：ＤＣ：７６：ＢＡ）をコンテンツ取得要求メッセージＭ２２０１のペイロード内に含めて送信するものとする。

【０１５３】

ネットワーク接続装置１６００はコンテンツ取得要求メッセージＭ２２０１を受信すると、暗号化判定処理を行う。まず、登録端末か否かの登録端末判定処理を行う。具体的には、コンテンツ取得要求メッセージＭ２２０１のペイロード内に含まれるＭＡＣアドレスが登録端末リストに登録されているか否かの判定を行う。ここで、Ｖｉｅｗｅｒ１６０１のＭＡＣアドレスは登録端末リストに登録されているので、登録端末リストに登録済みの端末であると判定される。

【０１５４】

次に、ネットワーク接続装置１６００は登録端末判定処理の後、ネットワーク判定処理を行う。ここでは、登録端末リストに登録された端末かをコンテンツ取得要求メッセージＭ２２０１のＥｔｈｅｒヘッダに含まれる送信元ＭＡＣアドレスと登録端末リストの登録端末のＭＡＣアドレスとの比較を行う。

【０１５５】

コンテンツ取得要求メッセージのＥｔｈｅｒヘッダの送信元ＭＡＣアドレスはＶｉｅｗｅｒ１６０１から送信された直後は、Ｖｉｅｗｅｒ１６０１のＭＡＣアドレス（００：ＦＥ：９８：ＤＣ：７６：ＢＡ）である。しかし、コンテンツ取得要求メッセージのＥｔｈｅｒヘッダの送信元ＭＡＣアドレスは、ルータ１０５を介した際にルータ１０５のＭＡＣアドレスに書き換えられる。

【０１５６】

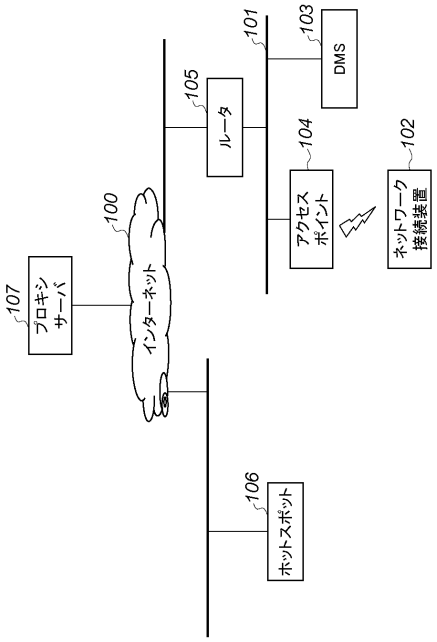
そのため、ネットワーク接続装置１６００に到着したコンテンツ取得要求メッセージＭ２２０１のＥｔｈｅｒヘッダの送信元ＭＡＣアドレスはＶｉｅｗｅｒ１６００のＭＡＣアドレスと異なるため、同一のサブネット外からの要求であると判定する。

【０１５７】
第４の実施形態では、登録端末判定処理の後にネットワーク判定処理を行っているが、先にネットワーク判定処理を行っても良く、これに限るものではない。
【０１５８】
ここで、同一のサブネット外からのコンテンツ取得要求であると判定されると、ネットワーク接続装置１６００とＶｉｅｗｅｒ１６０１間の通信がセキュアか否かが判定される。これは、例えばＳＳＬやＩＰｓｅｃ等による通信が行われている否かである。セキュアか否かはポリシー等によって判断しても良い。
【０１５９】
第４の実施形態では、セキュアな通信は行われていないものとする。セキュアな通信が行われていないと判定されたため、ネットワーク接続装置１６００は登録端末リストに登録されている端末に対応した共通鍵（ＰＳＫ２）にて要求されたコンテンツを暗号化して送信を行うと判定する。
【０１６０】
次に、ネットワーク接続装置１６００はコンテンツを暗号化して送信する旨を含めたコンテンツ取得応答メッセージＭ２２０２をＶｉｅｗｅｒ１６０１に送信する。そして、ネットワーク接続装置１６００は要求されたコンテンツを共通鍵（ＰＳＫ２）で暗号化し、Ｖｉｅｗｅｒ１６０１に送信する。
【０１６１】
尚、実施形態では、登録端末でない端末にはデータ提供を拒否するようにしているが、登録端末でない場合には、画像データを暗号化せずに送信するようにしても良い。
【０１６２】
また、登録端末判定処理を行っているが、登録端末判定を行わずに処理を継続しても良い。
【０１６３】
更に、通信がセキュアか否かの判定によって、暗号化を行うか否かを判定しているが、通信がセキュアか否かの判定を行わずに処理を継続しても良い。
【０１６４】
また、コンテンツ取得応答メッセージにコンテンツ暗号化有無のメッセージを含んでいるが、暗号化の有無を含まなくても良く、コンテンツ取得応答メッセージを送信しなくても良い。
【０１６５】
更に、登録端末判定処理にコンテンツ取得要求メッセージ内のペイロードにＭＡＣアドレスを含めることで登録端末か否かの判定を行ったが、登録端末を識別できるものであれば良く、これに限るものではない。
【０１６６】
また、ネットワーク判定処理にＥｔｈｅｒフレームの送信元ＭＡＣアドレスと登録端末リストに登録されているＭＡＣアドレスの比較を行ったが、同一のサブネットか否か判別できれば良く、これに限るものではない。例えば、ＩＰアドレスを用いて判別しても良く、サブネットマスクやＩＰｖ６のＲＡ（Router Advertise）等で同一のサブネットか否かを判別しても良い。
【０１６７】
更に、同一のサブネットワーク内にある端末か否かを判定できるプロトコルを用いて判別してもよい。例えば、ＬＬＤＰ（Link Layer Discovery Protocol :IEEE802.1AB）等のプロトコルを用いて、同一のサブネットワークか否かを判定しても良い。更に、特定プロトコルを受信した場合に同一のサブネットワークかを判定しても良い。例えば、ｓｓｄｐを受信した場合は同一のサブネットワークと判定しても良い。
【０１６８】
また、通信パラメータとして無線ＬＡＮの場合を示したが、これに限るものではなく、例えばBluetooth（登録商標）でも良い。

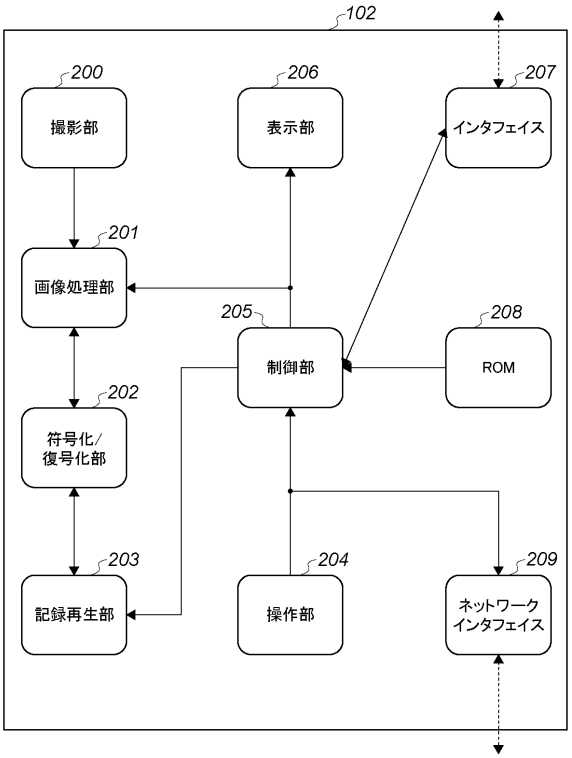
【０１６９】
更に、通信パラメータの提供方法に無線ＬＡＮを用いた提供方法を説明したが、これに限るものではなく、端末装置に通信パラメータを提供可能であれば良い。例えば、ＵＳＢメモリやＮＦＣ（Near Field Communication）等でパラメータの提供を行っても良い。
【０１７０】
上述したように、通信パラメータ設定時に通信パラメータ内の共通鍵を登録端末リストに端末毎に記録する。そして、コンテンツ要求があった場合に、同一のサブネット内からの要求かを判断し、同一のサブネット外からの要求である場合に端末毎の共通鍵でコンテンツを暗号化して送信を行うため、セキュリティ性及び利便性が向上する。
【０１７１】
［他の実施形態］
前述した実施形態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、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（ＣＰＵ若しくはＭＰＵ）が記録媒体に格納されたプログラムコードを読出し実行する。これによっても、本発明の目的が達成されることは言うまでもない。
【０１７２】
この場合、コンピュータ読み取り可能な記録媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記録媒体は本発明を構成することになる。
【０１７３】
このプログラムコードを供給するための記録媒体として、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、不揮発性のメモリカード、ＲＯＭなどを用いることができる。
【０１７４】
また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、次の場合も含まれることは言うまでもない。即ち、プログラムコードの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）などが実際の処理の一部又は全部を行い、その処理により前述した実施形態の機能が実現される場合である。
【０１７５】
更に、記録媒体から読出されたプログラムコードが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込む。その後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部又は全部を行い、その処理により前述した実施形態の機能が実現される場合も含まれることは言うまでもない。
【図面の簡単な説明】
【０１７６】
【図１】第１の実施形態におけるネットワーク構成の一例を示す図である。
【図２】第１の実施形態におけるネットワーク接続装置１０２の構成の一例を示す図である。
【図３】第１の実施形態におけるネットワーク接続装置１０２の機能モジュールを示す図である。
【図４】第１の実施形態におけるネットワーク接続装置１０２の設定処理を示すフローチャートである。
【図５】第１の実施形態における通信パラメータの一例を示す図である。
【図６】ネットワーク接続装置１０２及びＤＭＳ１０３の設定処理の通信シーケンスを示す図である。
【図７】ネットワーク接続装置１０２におけるアップロード処理を示すフローチャートである。
【図８】ネットワーク接続装置１０２がアクセスポイント１０４に接続し、ＤＭＳ１０３

に画像をアップロードするシーケンスを示す図である。
【図９】ネットワーク接続装置１０２が、ホットスポット１０６の近くに移動した場合を示す構成図である。
【図１０】ネットワーク接続装置１０２がホットスポット１０６に接続し、プロキシサーバ１０７に画像をアップロードするシーケンスを示す図である。
【図１１】第２の実施形態におけるネットワーク接続装置１０２の機能モジュール構成の一例を示す図である。
【図１２】第２の実施形態におけるネットワーク接続装置１０２のアップロード処理を示すフローチャートである。
【図１３】ネットワーク接続装置１０２がホットスポット１０６に接続し、ＩＰＳｅｃを利用して画像をアップロードするシーケンスを示す図である。
【図１４】第３の実施形態における通信パラメータの一例を示す図である。
【図１５】第３の実施形態におけるネットワーク接続装置１０２のアップロード処理を示すフローチャートである。
【図１６】第４の実施形態におけるネットワークの構成の一例を示す図である。
【図１７】第４の実施形態におけるネットワーク接続装置１６００の構成の一例を示す図である。
【図１８】第４の実施形態におけるネットワーク接続装置１６００のモジュール構成を示す図である。
【図１９】第４の実施形態におけるネットワーク接続装置１６００の通信パラメータ設定処理を示すフローチャートである。
【図２０】第４の実施形態におけるネットワーク接続装置１６００のダウンロード処理を示すフローチャートである。
【図２１】Ｖｉｅｗｅｒ１６０１、アクセスポイント１０４、ネットワーク接続装置１６００間の通信パラメータ設定及びコンテンツ転送のシーケンスを示す図である。
【図２２】第４の実施形態におけるネットワーク接続装置１６００が所持するアクセスポイント１０４の通信パラメータを示す図である。
【図２３】第４の実施形態における登録端末リストを示す図である。
【図２４】Ｖｉｅｗｅｒ１６０１、ホットスポット１０６、ルータ１０５、ネットワーク接続装置１６００間の通信パラメータ設定及びダウンロードのシーケンスを示す図である。
【符号の説明】
【０１７７】
１００　インターネット
１０１　ＬＡＮ
１０２　ネットワーク接続装置
１０３　ＤＭＳ（デジタルメディアサーバ）
１０４　アクセスポイント
１０５　ルータ
１０６　ホットスポット
１０７　プロキシサーバ

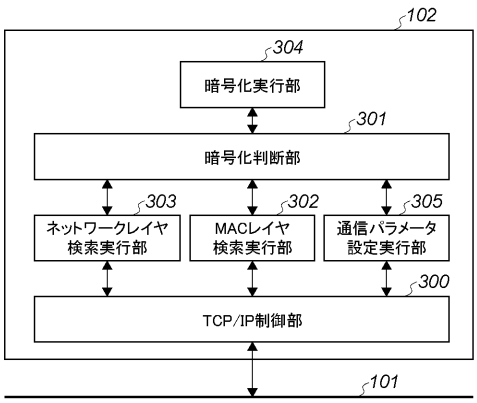
【図１】


101
103
DMS
105
ルータ
104
アクセス
ポイント
102
ネットワーク
接続装置
100
インターネット
107
プロキシ
サーバ
106
ホットスポット

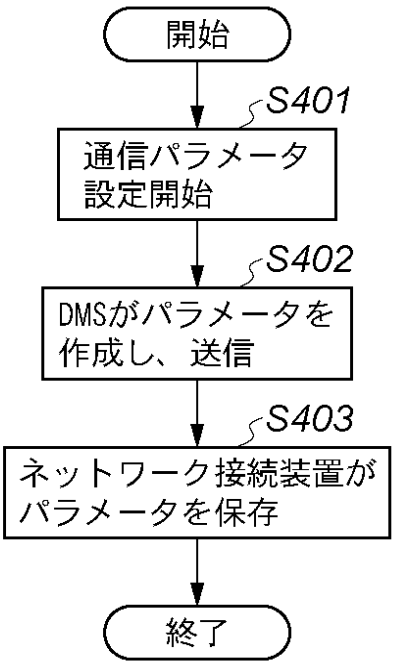
【図２】


102
200
撮影部
206
表示部
207
インタフェイス
201
画像処理部
205
制御部
208
ROM
202
符号化/
復号化部
203
記録再生部
204
操作部
209
ネットワーク
インタフェイス

【図３】


102
304
暗号化実行部
301
暗号化判断部
303
ネットワークレイヤ
検索実行部
302
MACレイヤ
検索実行部
305
通信パラメータ
設定実行部
300
TCP/IP制御部
101

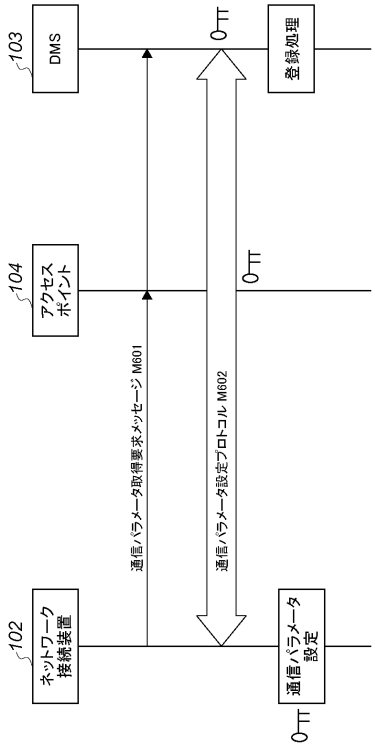
【図４】


開始
S401
通信パラメータ
設定開始
S402
DMSがパラメータを
作成し、送信
S403
ネットワーク接続装置が
パラメータを保存
終了

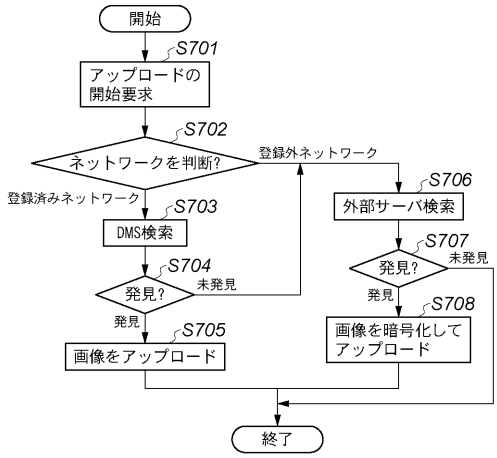
【図５】

ネットワークの種類	無線LAN
ネットワーク識別子	SSID1
暗号鍵	PSK1
ホームサーバの発見プロトコル	ssdp
ホームサーバ識別子	uuid:816c5df0-c2ed-11da-9216-0008741e9394
外部サーバの発見プロトコル	DNS
外部サーバ識別子	http://server.xxxxx.com/

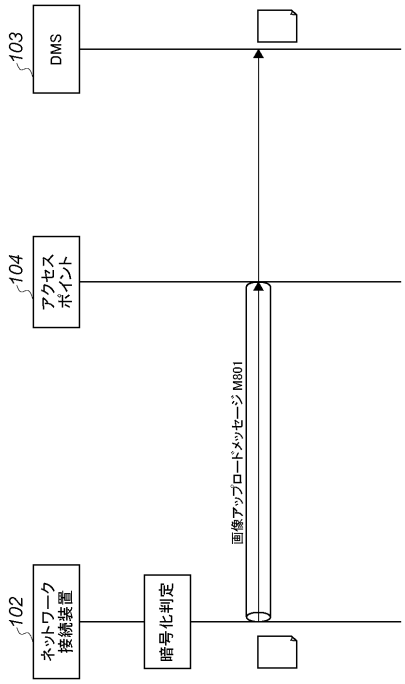
【図６】



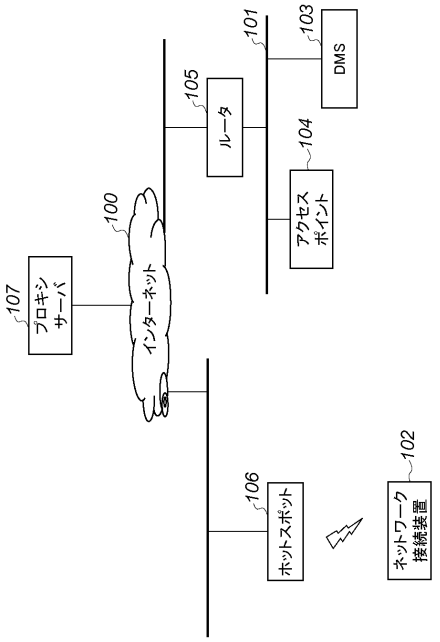
【図７】



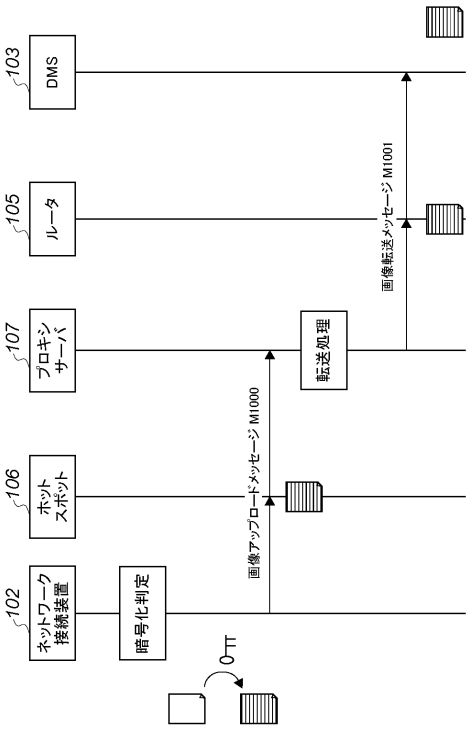
【図８】



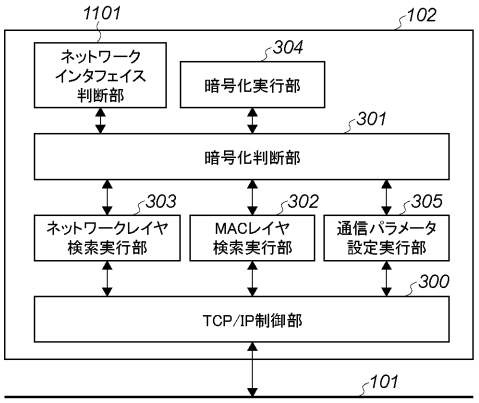
【図９】



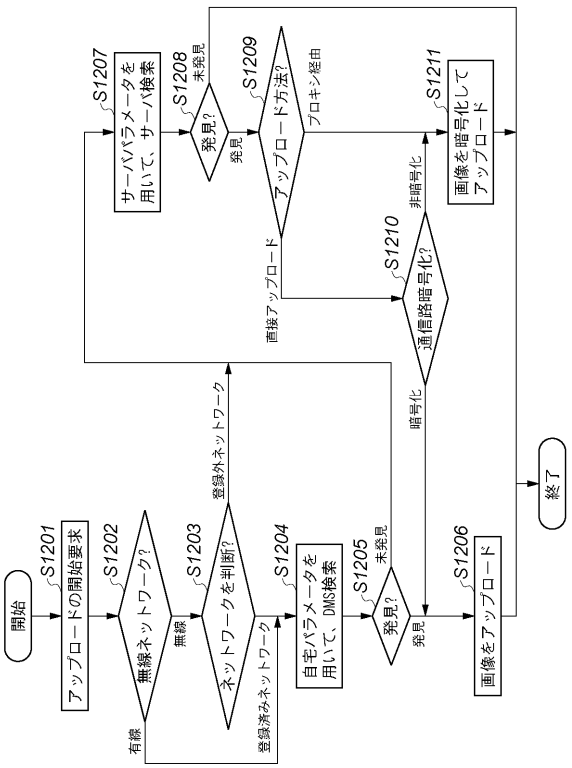
【図１０】



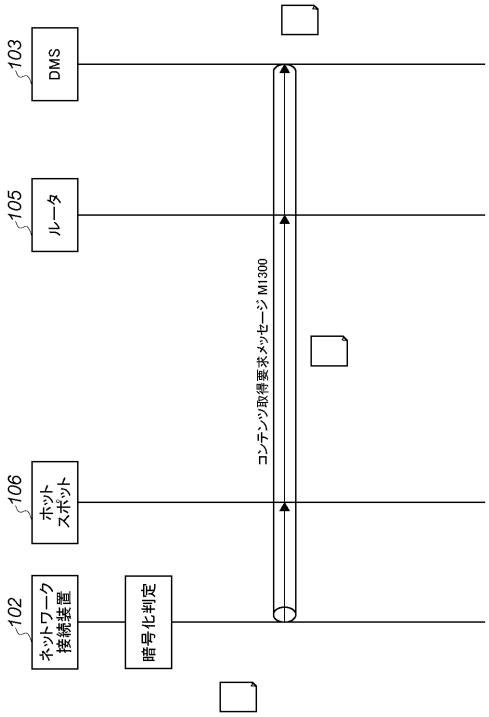
【図１１】



【図１２】



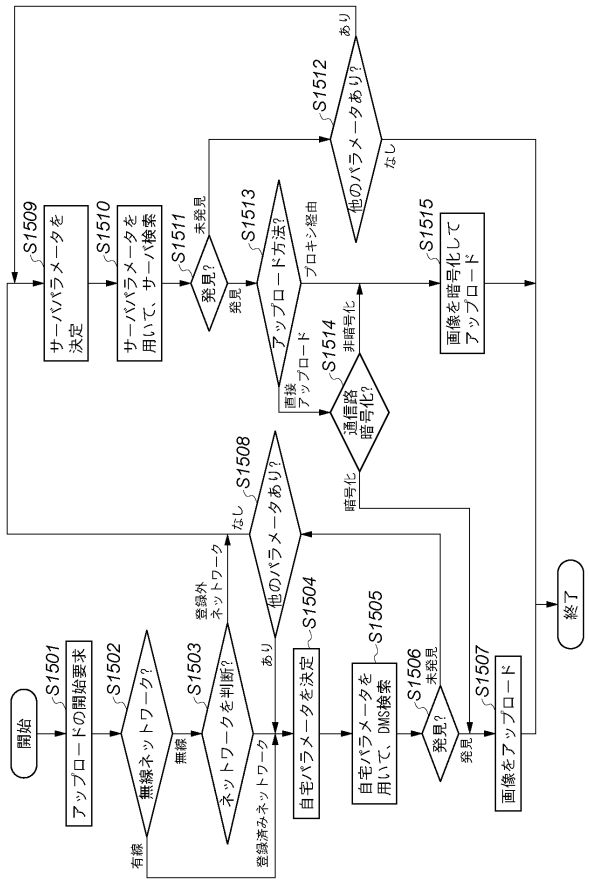
【図１３】



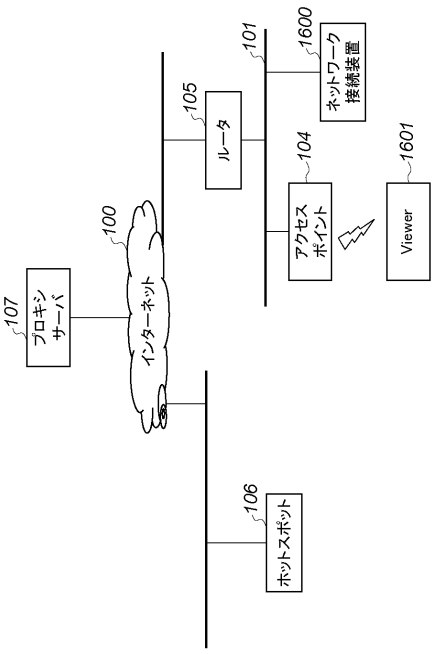
【図１４】

ネットワークの種類	無線LAN
ネットワーク識別子	SSID1
暗号鍵	PSK1
第一のホームサーバの発見プロトコル	ssdp
第一のホームサーバ識別子	uuid:816c5df0-c2ed-11da-9216-0008741e9394
第二のホームサーバの発見プロトコル	mDNS
第二のホームサーバ識別子	dns.home.ne.jp
第一の外部サーバの発見プロトコル	DNS
第一の外部サーバ識別子	http://server.xxxxx.com/
第二の外部サーバの発見プロトコル	SIP
第二の外部サーバ識別子	sip:server@xxxxx.com

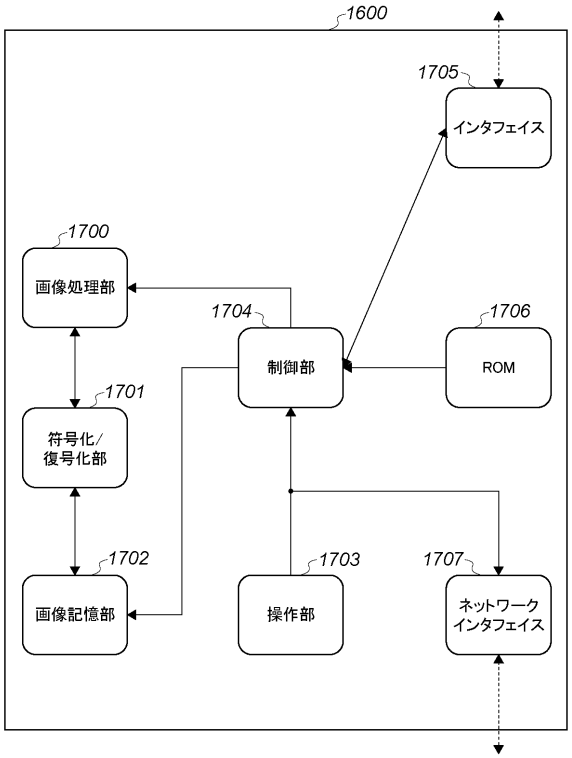
【図１５】



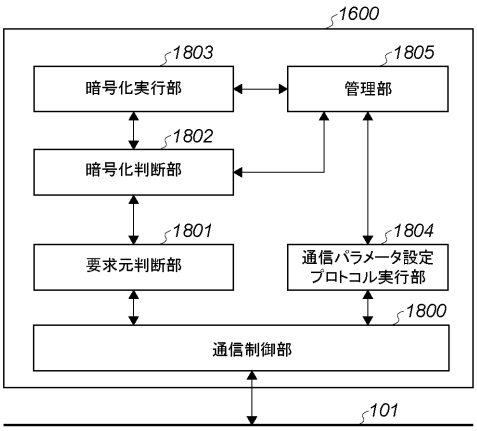
【図１６】



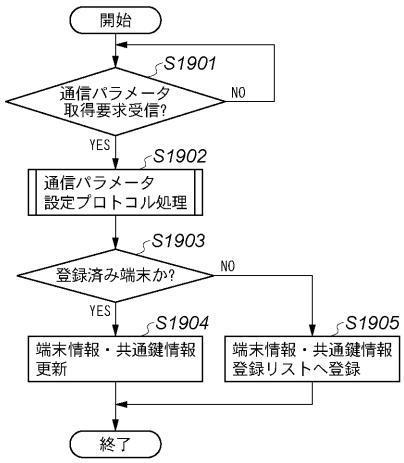
【図１７】



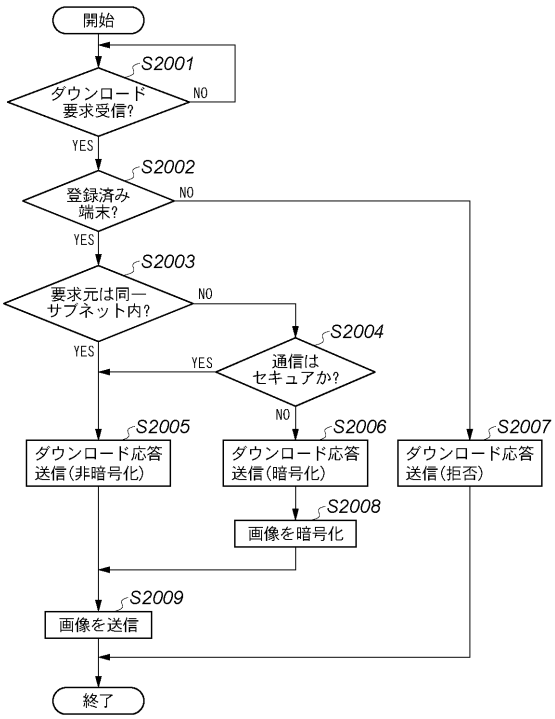
【図１８】



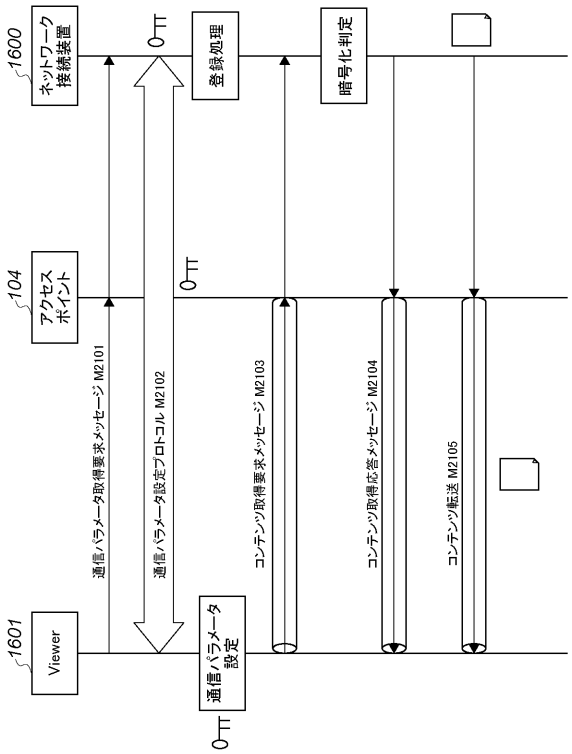
【図１９】



【図２０】



【図２１】



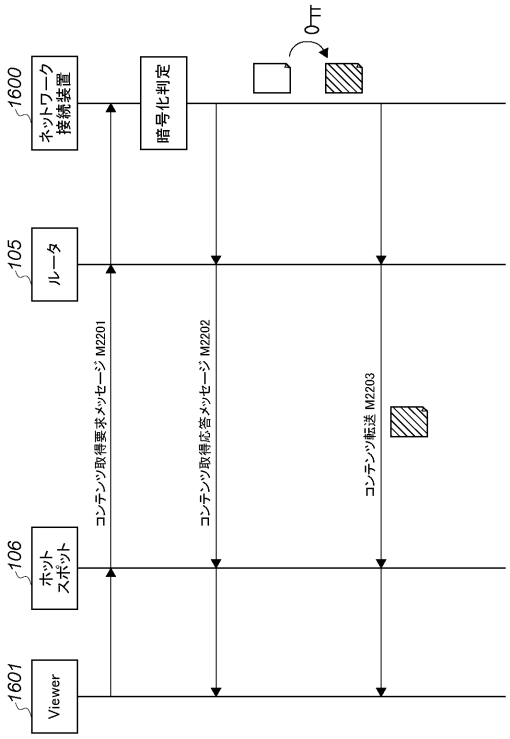
【図２２】

ネットワーク識別子	SSID2
暗号鍵	PSK2
認証方式	WPA-PSK
暗号方式	TKIP
デバイス情報	DMS

【図２３】

登録端末リスト	共通鍵情報
00:01:02:03:04:05	PSK2
00:0A:0B:0C:0D:0E	PSK2
00:12:AB:34:CD:56	PSK1
00:FE:98:DC:76:BA	PSK2

【図２４】



フロントページの続き

(72)発明者　安間　健介
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
(72)発明者　中島　孝文
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　金沢　史明

(56)参考文献　特開２００６－２４６０９８（ＪＰ，Ａ）
特開２００２－３１２１４６（ＪＰ，Ａ）
特開２０００－１３８７０３（ＪＰ，Ａ）
特開２００１－１７７５１４（ＪＰ，Ａ）
特開平０９－１６７０９８（ＪＰ，Ａ）
特開２００４－３２０１３９（ＪＰ，Ａ）
特開２００８－２９４８１４（ＪＰ，Ａ）
特開２００８－０２２１６５（ＪＰ，Ａ）
特開２００４－０５６３２５（ＪＰ，Ａ）
特開２０００－１３８６６５（ＪＰ，Ａ）
特開２０００－３３２８２５（ＪＰ，Ａ）
国際公開第２００７／０４３９２７（ＷＯ，Ａ１）
国際公開第２００８／０７２５７６（ＷＯ，Ａ１）
特開２００４－１２０４６２（ＪＰ，Ａ）
特開平１０－１５０４５３（ＪＰ，Ａ）
特開２００６－１５７４５４（ＪＰ，Ａ）
特開２００８－３０６５７３（ＪＰ，Ａ）
特開２００７－３３４７５３（ＪＰ，Ａ）
特開２００６－１４８６６０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｗ　１２／００－１２／１２