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

特許第5600407号
(P5600407)

(45)発行日　平成26年10月1日(2014.10.1)　(24)登録日　平成26年8月22日(2014.8.22)

(51)Int.Cl.		F I		
H04L 9/16	(2006.01)	H04L	9/00	643
H04L 9/08	(2006.01)	H04L	9/00	601C
H04W 12/02	(2009.01)	H04W	12/02	
H04W 84/12	(2009.01)	H04W	84/12	

請求項の数 9　(全 21 頁)

(21)出願番号　特願2009-222840 (P2009-222840)
(22)出願日　平成21年9月28日 (2009.9.28)
(65)公開番号　特開2010-114885 (P2010-114885A)
(43)公開日　平成22年5月20日 (2010.5.20)
審査請求日　平成24年9月25日 (2012.9.25)
(31)優先権主張番号　特願2008-264633 (P2008-264633)
(32)優先日　平成20年10月10日 (2008.10.10)
(33)優先権主張国　日本国(JP)

(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、通信装置の制御方法及びコンピュータプログラム

(57)【特許請求の範囲】
【請求項１】
通信装置であって、
他の通信装置との間で第１の暗号鍵を共有する第１の共有手段と、
前記他の通信装置との間で、第２の暗号鍵を前記第１の暗号鍵で暗号化して共有する第２の共有手段と、
前記通信装置と前記他の通信装置とが直接接続してい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他の通信装置と直接接続していると判定された場合には前記第２の暗号鍵を用いてデータの通信路を暗号化して送信し、前記判定手段により前記他の通信装置と直接接続していない判定された場合には前記第１の暗号鍵を用いて前記データを暗号化して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】
通信装置であって、
他の通信装置との間で第１の暗号鍵を共有する第１の共有手段と、
前記他の通信装置との間で、第２の暗号鍵を前記第１の暗号鍵で暗号化して共有する第２の共有手段と、
前記他の通信装置からデータを受信する受信手段と、
前記通信装置と前記他の通信装置とが直接接続してい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他の通信装置と直接接続していると判定された場合には前記第

２の暗号鍵を用いてデータの通信路を復号し、前記判定手段により前記他の通信装置と直接接続していないと判定された場合には前記第１の暗号鍵を用いて前記受信手段により受信したデータを復号する復号手段と、
を有することを特徴とする通信装置。
【請求項３】
前記第１の暗号鍵及び前記第２の暗号鍵を記憶する記憶手段を更に有す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】
前記第１の共有手段は、Diffie-Hellmanの鍵交換アルゴリズムを用いて前記第１の暗号鍵を共有することを特徴とする請求項１乃至３のいずれか１項に記載の通信装置。
【請求項５】
前記通信装置は、前記他の通信装置と前記第２の暗号鍵を用いてＩＥＥＥ８０２．１１シリーズに準拠した無線通信を行うことを特徴とする請求項１乃至４のいずれか１項に記載の通信装置。
【請求項６】
前記第２の暗号鍵は、単一の相手装置に対してデータを送信する際に用いられるセッション鍵と、複数の相手装置に対してデータを送信する際に用いられるグループ鍵と、の少なくともいずれか一方であることを特徴とする請求項１から５のいずれか１項に記載の通信装置。
【請求項７】
通信装置の制御方法であって、
第１の共有手段が、他の通信装置との間で第１の暗号鍵を共有する第１の共有工程と、
第２の共有手段が、前記他の通信装置との間で、第２の暗号鍵を前記第１の暗号鍵で暗号化して共有する第２の共有工程と、
判定手段が、前記通信装置と前記他の通信装置とが直接接続しているか否かを判定する判定工程と、
送信手段が、前記判定工程において前記他の通信装置と直接接続していると判定された場合には前記第２の暗号鍵を用いてデータの通信路を暗号化して送信し、前記判定工程において前記他の通信装置と直接接続していない判定された場合には前記第１の暗号鍵を用いて前記データを暗号化して送信する送信工程と、
を有することを特徴とする通信装置の制御方法。
【請求項８】
通信装置の制御方法であって、
第１の共有手段が、他の通信装置との間で第１の暗号鍵を共有する第１の共有工程と、
第２の共有手段が、前記他の通信装置との間で、第２の暗号鍵を前記第１の暗号鍵で暗号化して共有する第２の共有工程と、
判定手段が、前記通信装置と前記他の通信装置とが直接接続しているか否かを判定する判定工程と、
受信手段が、前記他の通信装置からデータを受信する受信工程と、
復号手段が、前記判定工程において前記他の通信装置と直接接続していると判定された場合には前記第２の暗号鍵を用いてデータの通信路を復号し、前記判定工程において前記他の通信装置と直接接続していない判定された場合には前記第１の暗号鍵を用いて前記受信手段により受信したデータを復号する復号工程と、
を有することを特徴とする通信装置の制御方法。
【請求項９】
コンピュータを請求項１乃至６のいずれか１項に記載の通信装置の各手段として動作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、通信装置の制御方法及びコンピュータプログラムに関する。
【背景技術】
【０００２】
カメラで取った画像データを公衆ネットワーク経由でサーバにアップロードすることで画像を多数の人に参照させるようなサービスが存在する（特許文献１参照）。また、オープンなネットワークに送信されるコンテンツデータの暗号化を行い、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コンテンツデータの暗号化は行わない技術がある（特許文献２参照）。
【０００３】
また、ＩＥＥＥ８０２．１１無線ＬＡＮ（以下、無線ＬＡＮ）による無線ネットワークを構成するための通信パラメータを簡易に複数の通信装置間で共有するための通信パラメータ設定技術が存在する。通信パラメータとしては、ネットワーク識別情報であるＳＳＩＤ、周波数チャネル、暗号鍵、暗号方式、認証方式等がある。該通信パラメータ設定技術は既に標準化されており（Wi-Fi CERTIFIED(TM) for Wi-Fi Protected Setup：Easing the User Experience for Home and Small Office Wi-Fi (R) Networks,http://www.wi-fi.org/files/kc/20090123_Wi-Fi_Protected_Setup.pdf 以下ＷＰＳ）、多くの通信装置に搭載されている。
【０００４】
ＷＰＳによる通信パラメータ設定処理では、特定のプロトコルを用いることにより一方の通信装置から他方の通信装置へ通信パラメータが提供される。ここで、通信パラメータを送受信する際には、Diffie-Hellmanの鍵交換アルゴリズムにより通信装置間で共有された第１の暗号鍵が用いられる。第１の暗号鍵は、通信パラメータ設定が終了、若しくは有効期限が過ぎると破棄される。
また、共有された通信パラメータにより構成された無線ネットワークを介して無線通信を行う場合には、該通信パラメータに基づく第２の暗号鍵が用いられる。第２の暗号鍵は、所望の通信が終了して無線ネットワークが切断される、若しくは有効期間が過ぎると破棄される。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００７－２５１７４８号公報
【特許文献２】特開２０００－１３８７０３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
ここで、通信装置が公衆ネットワークに接続し、画像データ等のコンテンツデータをネットワーク上のサーバ等にアップロードする場合、ＳＳＬ等でＩＰレイヤより上位層の通信路の暗号化を行う場合がある。しかしながら、この場合はコンテンツデータ自体には暗号化を行っていない場合が多く、プロキシサーバ等で該通信路は一度終端されるため、サーバ側でデータを盗み見られるおそれがある。
【０００７】
本発明は、コンテンツデータを他の通信装置との間で共有する際のセキュリティの向上を図ることを目的とする。
【課題を解決するための手段】
【０００８】
上記課題を解決するため、本発明に係る通信装置は、他の通信装置との間で第１の暗号鍵を共有する第１の共有手段と、
前記他の通信装置との間で、第２の暗号鍵を前記第１の暗号鍵で暗号化して共有する第２の共有手段と、
前記通信装置と前記他の通信装置とが直接接続してい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他の通信装置と直接接続していると判定された場合には前記第２の暗号鍵を用いてデータの通信路を暗号化して送信し、前記判定手段により前記他の通信装置と直接接続していない判定された場合には前記第１の暗号鍵を用いて前記データを暗号化して送信する送信手段と、を有することを特徴とする。

【０００９】

また、本発明に係る通信装置は、他の通信装置との間で第１の暗号鍵を共有する第１の共有手段と、

前記他の通信装置との間で、第２の暗号鍵を前記第１の暗号鍵で暗号化して共有する第２の共有手段と、

前記他の通信装置からデータを受信する受信手段と、

前記通信装置と前記他の通信装置とが直接接続してい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他の通信装置と直接接続していると判定された場合には前記第２の暗号鍵を用いてデータの通信路を復号し、前記判定手段により前記他の通信装置と直接接続していない判定された場合には前記第１の暗号鍵を用いて前記受信手段により受信したデータを復号する復号手段と、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、コンテンツデータを他の通信装置との間で共有する際のセキュリティを向上させることができる。

【図面の簡単な説明】

【００１１】

【図１】発明の第１の実施形態に対応するデータ共有システム構成の一例を示す図である。

【図２】発明の実施形態に対応する通信装置のハードウェア構成の一例を示すブロック図である。

【図３】発明の実施形態に対応する通信装置１０１の機能モジュール構成の一例を記載した図である。

【図４】発明の第１の実施形態に対応する通信装置１０１－１の処理の一例を示すフローチャートである。

【図５】発明の第１の実施形態に対応する通信装置１０１－２における処理の一例を示すフローチャートである。

【図６】発明の第２の実施形態に対応するデータ共有システム構成の一例を示す図である。

【図７】発明の第２の実施形態に対応する通信装置６０１－１の処理の一例を示すフローチャートである。

【図８】発明の第２の実施形態に対応する通信装置６０１－１の画像データアップロード処理の一例を示すフローチャートである。

【図９】発明の第２の実施形態に対応する通信装置６０１－２、または６０１－３の動作の一例を示すフローチャートである。

【図１０】発明の第１、第２の実施形態において暗号化を行う範囲を説明する図である。

【発明を実施するための形態】

【００１２】

以下、本発明の実施形態について、図面を参照して説明する。

【００１３】

［第１の実施形態］

本実施形態では、複数の通信装置が共有したいコンテンツデータの送受信をプロキシサーバを介して行うデータ共有システムを説明する。但し、発明の実施形態はプロキシサーバを有するシステムに限定されず、メールサーバを介してコンテンツデータの送受信を行うメールシステムや、ドキュメントサーバを介してコンテンツデータの送受信を行うドキュメントシステムにも適応可能である。

【００１４】
図１は、発明の第１の実施形態に対応するデータ共有システム構成の一例を示す図である。インターネット１００は、ＴＣＰ／ＩＰプロトコルに従ってノード間の通信を可能とする外部ネットワークである。インターネット１００は、インターネットに限らず、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）やＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、或いは、それらの組合せであってもよい。
【００１５】
通信装置１０１－１及び通信装置１０１－２は、ＩＥＥＥ８０２．１１無線ＬＡＮ（以下、無線ＬＡＮ）による無線通信機能を有する。通信装置１０１－１及び通信装置１０１－２は、公衆無線ＬＡＮ対応アクセスポイント（以下アクセスポイント）１０２－１或いは１０２－２を介してインフラストラクチャモードによる無線通信を行うことができる。また、通信装置１０１－１と通信装置１０１－２は、アクセスポイントを介さずに直接アドホックモードによる無線通信を行うこともできる。以下、複数の通信装置を代表して通信装置１０１といい、複数のアクセスポイントを代表してアクセスポイント１０２という。各通信装置１０１は、無線ネットワークを構成するための通信パラメータの自動設定機能を有している。
【００１６】
また、通信装置１０１－１はアクセスポイント１０２－１に接続を行う権限を有し、アクセスポイント１０２－１が形成するインフラストラクチャモードの無線ネットワークに接続するための通信パラメータを記憶しているものとする。通信装置１０１－２はアクセスポイント１０２－２に接続を行う権限を有し、アクセスポイント１０２－２が形成するインフラストラクチャモードの無線ネットワークに接続するための通信パラメータを記憶しているものとする。なお、通信装置１０１の数は図１に示す２つに限定されるものではなく、より多くの通信装置がアクセスポイントに接続されても良い。その場合、各通信装置は権限を有する限りどのアクセスポイントに接続してもよく、同様の結果が得られることは言うまでもない。
【００１７】
アクセスポイント１０２は、インターネット１００と接続されたアクセスポイントである。アクセスポイント１０２は、無線ＬＡＮ通信接続機能を各通信装置に提供する。アクセスポイント１０２の数は図１に示した２つに限定されるものではなく、より多くのアクセスポイントがインターネット１００に接続されていてもよい。
【００１８】
サーバ１０３はインターネット１００と接続され、インターネット１００を介して通信装置１０１から送信される画像データ等のコンテンツデータを格納するサーバ装置である。
【００１９】
次に、図２を参照して、発明の実施形態に対応する通信装置のハードウェア構成の一例を説明する。図２は発明の実施形態に対応する通信装置のハードウェア構成の一例を示すブロック図である。
【００２０】
本実施形態では、通信装置１０１をデジタルカメラとして説明するが、無線ＬＡＮによる無線通信機能を搭載するデバイスなら同様の効果を得られる。例えば無線ＬＡＮによる無線通信機能をもつパーソナルコンピュータ（ＰＣ）、携帯電話、ＰＤＡ(Personal Digital Assistant)でも構わない。
【００２１】
図２において通信装置１０１は、以下の構成要素を有する。撮像部２０１は被写体の光学像を撮像する撮像部であって、ＣＣＤやＣＭＯＳ等の撮像素子を用いて構成される。画像処理部２０２は、撮像部２０１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。
【００２２】

符号化／復号化部２０３は、画像処理部２０２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２０３はまた、記録再生部２０４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２０２に供給する。

【００２３】

記録再生部２０４は、圧縮符号化された画像データを通信装置１０１に装着された記録媒体（不図示）に記録したり、該画像データを読み出して再生したりする。操作部２０５は、通信装置１０１における処理動作の指示をユーザから受け付けるためのユーザインタフェースである。制御部２０６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、通信装置１０１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を行う。表示部２０７は撮像部２０１にて撮像された画像を、ＥＶＦ（Electronic View Finder）や液晶パネル等を用いて表示する。インターフェース２０８は撮像部２０１にて撮像された画像データなどを外部装置へ送信するための通信インターフェースである。

【００２４】

ＲＯＭ２０９は、通信装置１０１の機能に関する情報を格納する記憶装置である。本実施形態の通信装置は、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。ネットワークインターフェース（ＮＥＴＩＦ）２１０は、無線ＬＡＮによる無線通信を行うためのインターフェースであり、無線ネットワークを介してデータ転送を行うための制御や無線ネットワークへの接続状況の診断を行う。

【００２５】

次に図３を参照して、本実施形態に対応する通信装置１０１の機能モジュール構成について説明する。図３は発明の実施形態に対応する通信装置１０１の機能モジュール構成の一例を記載した図である。本実施形態において、通信装置１０１の各モジュールは、ＲＯＭ２０９に記憶されたプログラムを制御部２０６が実行して、各ハードウェアブロックを制御することにより実現される。なお、図３に示した各機能モジュールは、全てがソフトウェアモジュール化される必要はなく、一部乃至全部がハードウェアモジュール化されてもよい。

【００２６】

ＴＣＰ／ＩＰ制御部３０１は、ＴＣＰ／ＩＰプロトコルに従った処理を行う制御モジュールである。記憶部３０２には、暗号鍵、通信パラメータ自動設定機能により取得した無線ネットワーク構成に必要な通信パラメータ、サーバのＵＲＬ情報乃至データ保持通信装置のアドレス情報等が記憶される。通信パラメータとしては、ネットワーク識別情報であるＳＳＩＤ、周波数チャネル、暗号方式、認証方式等が挙げられる。なお、データ保持通信装置とは、通信装置１０１－１と通信装置１０１－２間で共有するコンテンツデータを保持する通信装置を指す。

【００２７】

通信部３０３は通信プロトコルに従って通信を行う。通信パラメータ設定実行部３０４は、対向の通信装置同士で無線ネットワークを構成するために必要な通信パラメータを暗号化して送受信を行う。なお、本実施形態では、サーバやデータ保持装置を特定するための情報が、通信パラメータと共に送受信されるものとする。ネットワーク判断部３０５は、通信装置１０１が参加しているネットワークが、アドホック、インフラストラクチャ、公衆ネットワークのうちのいずれの種類か、及びネットワーク内の通信装置についての判断処理を行う。暗号化／復号化判断部３０６は、ネットワーク判断部３０５における判断結果に基づいて、コンテンツデータの暗号化や復号化を行うか否かを判断する。暗号化／復号化判断部３０６はまた、記憶部３０２に記憶されている暗号鍵のうち暗号化／復号化に使用する暗号鍵を決定する。暗号化／復号化実行部３０７は、暗号化・復号化判断部３０６における判断結果に基づいてコンテンツデータの暗号化／復号化を行う。

【００２８】

次に、本実施形態に対応する処理の概要を説明する。本実施形態では、最初に通信装置１０１－１と通信装置１０１－２間でアドホックネットワークを形成するための通信パラメータ自動設定を行う。この自動設定の際にサーバ１０３の情報も通信装置１０１－１と通信装置１０１－２との間で共有する。その後、通信装置１０１－１はアクセスポイント１０２－１に接続してインターネット１００経由でサーバ１０３に画像データをアップロード（送信）する。そして、通信装置１０１－２はアクセスポイント１０２－２に接続し、インターネット１００経由でサーバ１０３にある画像データをダウンロード（受信）するものとする。尚、通信装置１０１－２が画像データをサーバ１０３にアップロードし、通信装置１０１－１がサーバ１０３から画像データを受信する形でも構わない。

【００２９】

本実施形態では、通信パラメータ設定処理につきＷＰＳ(Wi-Fi Protected Setup)をアドホックモードに適用した場合を例にして説明する。また、本実施形態では、アクセスポイント１０２に接続してインターネット１００に接続する形態で説明を行うが、携帯電話などの公衆網を介してインターネット１００に接続しても構わない。

【００３０】

次に図４を参照して本実施形態に対応する通信装置１０１の処理の一例を説明する。ここでは特に、画像データの送信側である通信装置１０１－１における処理を説明する。図４は、発明の実施形態に対応する通信装置１０１－１の処理の一例を示すフローチャートである。

【００３１】

ステップＳ４０１において通信装置１０１－１は、通信パラメータの設定処理が開始されたか否かを判断する。本実施形態ではＷＰＳが開始されたかどうかを判断する。次にステップＳ４０２では通信装置１０１－１は、通信パラメータ設定を行う対向通信装置が存在するかどうかを判断する。ここでは実行主体が通信装置１０１－１であるので、対向通信装置は通信装置１０１－２となる。ステップＳ４０２では、例えば、ＷＰＳを起動中であることを示す情報が付加されたビーコンを受信したか否かにより、対向通信装置が存在するか否かを判断することができる。また、プローブリクエストを送信し、ＷＰＳを起動中であることを示す情報が付加されたプローブレスポンスを受信したか否かにより、対向通信装置が存在するか否かを判断することもできる。

【００３２】

通信装置１０１－１は、対向通信装置１０１－２が存在しなければ（ステップＳ４０２において「ＮＯ」）、ＵＩ等で発見できなかった旨をユーザに伝えて、ステップＳ４０３で通信パラメータ設定処理をエラー終了する。通信装置１０１－１は、通信パラメータ設定処理がエラー終了した場合、ステップＳ４０１の初期状態に遷移する。

【００３３】

一方、対向通信装置１０１－２が存在する場合（ステップＳ４０２において「ＹＥＳ」）、ステップＳ４０４に移行する。ステップＳ４０４では、通信装置１０１－１は第１の暗号鍵を対向通信装置１０１－２と共有する。具体的には、Diffie-Hellmanの鍵交換アルゴリズムを用いることにより、第１の暗号鍵が共有される。ここで第１の暗号鍵は、通信パラメータ設定処理において、通信パラメータ等の各種情報を送受信する際の暗号化、及び復号化に使用される。

【００３４】

続いてステップＳ４０５において通信装置１０１－１は、通信装置１０１－２との間でサーバ１０３のＵＲＬ情報及びＩＰアドレス等の共有を行う。本実施形態では、サーバ１０３に画像データを置くことで画像データの共有を行うため、サーバ１０３のＵＲＬ情報及びＩＰアドレス等を取得する。サーバ１０３以外のデータ保持通信装置を介してコンテンツデータの共有を行うときは、ステップＳ４０６で該データ保持通信装置のアドレス情報（ＵＲＬ，ＩＰアドレスなど）を共有する。

【００３５】

ステップＳ４０７において、通信装置１０１－１は通信装置１０１－２との間で無線ネ

ットワーク構成に必要な通信パラメータを共有する。なお、Ｓ４０５～Ｓ４０７でＵＲＬ、データ保持通信装置、通信パラメータ等の各種情報を共有する際には、第１の暗号鍵で該情報の暗号化、及び復号化を行う。また、ここではＳ４０５～４０７を別々の処理として説明したが、これらの処理をまとめて行っても構わない。即ち、ＵＲＬ、データ保持通信装置、通信パラメータ等を１つのフレームに格納して送受信するようにしても構わない。また、必ずしもＵＲＬ、及びデータ保持通信装置の情報を通信パラメータ設定時に共有するのではなく、予め通信装置１０１－１と通信装置１０１－２に記憶させておいても構わない。

【００３６】

上記処理により通信装置１０１間で共有された第１の暗号鍵、通信パラメータ、サーバ１０３のＵＲＬやデータ保持通信装置のアドレス情報等は記憶部３０２に記憶される。続くステップＳ４０８において通信装置１０１－１は、通信パラメータ設定処理を終了する。

【００３７】

続く、ステップＳ４０９において通信装置１０１－１は、ネットワーク判断部３０５によりネットワークに接続したか否かを判断する。本実施形態では通信装置１０１－１は、アクセスポイント１０２－１が形成する無線ネットワークへの接続、又は通信装置１０１－２との間での無線ネットワーク接続を行う。ネットワーク接続が確認されれば（ステップＳ４０９において「ＹＥＳ」）、ステップＳ４１０に移行する。ステップＳ４１０では通信装置１０１－１は、通信装置１０１－２との間で共有したい画像データがあるか否か判断を行う。ここでの判断は、例えばユーザの選択や、通信装置１０１－１内に新しい画像データが追加されたかどうかに基づいて行うことができる。

【００３８】

ステップＳ４１１では、通信装置１０１－１は画像データを共有したい通信装置１０１－２と直接通信できるかどうかを判定する（第１の判定）。直接通信できるか否かは、通信装置１０１－１が存在するネットワーク内でＭＡＣレイヤでの検知処理を行い、画像データを共有したい通信装置を発見できるか否かで判定する。本実施形態では、通信パラメータ設定処理により共有された通信パラメータを用いた無線ネットワークに接続している場合に、直接通信可能と判定される。つまり、通信装置１０１－１が通信装置１０１－２とアドホックネットワーク接続をした場合は直接通信可能と判定され、アクセスポイント１０２－１に接続した場合には、直接通信不可能と判定されることになる。

【００３９】

ここで、本実施形態における暗号化について詳細に説明する。通信装置１０１－１と通信装置１０１－２間でアドホックモードによる無線通信を行う場合は、ＷＰＳにより共有された通信パラメータが用いられる。該無線通信に用いる暗号鍵に関しては、暗号方式によって大きく二種類に分類される。１つ目の方法は、ＷＰＳにより共有された通信パラメータに含まれる暗号鍵をそのまま使用する場合である。２つ目の方法は、共有された通信パラメータに含まれる暗号鍵を種として通信装置間で認証処理を行うことにより新たにセッション鍵、グループ鍵を生成し、該セッション鍵、グループ鍵を使用する場合である。なお、セッション鍵とは、特定の単一の相手装置との間でユニキャスト通信する際に使用する暗号鍵であり、２台の通信装置間で共通の暗号鍵である。一方、グループ鍵とは複数の通信相手との間でマルチキャスト通信する際に使用する暗号鍵であり、無線ネットワークを構成する全ての通信装置間で共通の暗号鍵である。本実施形態では、１つ目の方法、及び２つ目の方法で使用する暗号鍵を全てまとめて第２の暗号鍵として説明する。

【００４０】

次に、図１０を用いて、本実施形態において画像データを送信する際に暗号化を行う範囲について説明する。図１０（ａ）～（ｄ）は夫々ＭＡＣフレーム、ＩＰパケット、ＴＣＰパケット、ＨＴＴＰパケットを示している。通信装置１０１－１と通信装置１０１－２間でアドホックモードによる無線通信を行う場合は、図１０（ａ）に示すようにＭＡＣヘッダとＭＡＣペイロードが第２の暗号鍵で暗号化される。本実施形態においては、ＭＡＣ

ヘッダとＭＡＣペイロードが暗号化されていることを、「無線通信路の暗号化」として説明する。また、「コンテンツデータ（画像データ）の暗号化」とは、図１０（ｄ）に示すように、ＨＴＴＰペイロードの一部であるコンテンツデータ（画像データ）のみを暗号化している場合である。また、「ＳＳＬによる暗号化」とは、図１０（ｃ）に示すようにＴＣＰペイロードのみ暗号化している場合である。

【００４１】

このように、無線通信路の暗号化とコンテンツデータの暗号化、及びＳＳＬによる暗号化は同一の処理ではなく、夫々独立した処理である。例えば、コンテンツデータを暗号化しているか否かに拘らず、無線通信路の暗号化を行うことができる。また、無線通信路が暗号化されているか否かに拘らず、コンテンツデータを暗号化することもできる。

【００４２】

図４の説明に戻る。Ｓ４１１における判定結果に基づき、通信装置１０１－２と直接通信可能な場合（ステップＳ４１１において「ＹＥＳ」）、ステップＳ４１２に進む。通信装置１０１－１と通信装置１０１－２間でアドホックモードにより直接無線通信を行う場合は、上述のように第２の暗号鍵を用いることにより無線通信路が暗号化される。そのため、画像データ単体で暗号化されていなくても該画像データを含むＭＡＣペイロードの全体が暗号化されているのでセキュリティは確保される。よって、ステップＳ４１２では、通信装置１０１－１は、画像データに暗号化をかけずに通信装置１０１－２にデータを送信する。

【００４３】

一方、通信装置１０１－１は、通信装置１０１－２と直接通信できないと判断したら（ステップＳ４１１において「ＮＯ」）、画像データを第１の暗号鍵で暗号化して通信を行う。つまり、直接通信できない場合は、第２の暗号鍵により無線通信路が暗号化されないので、画像データを暗号化することによりセキュリティを確保する。

このように、コンテンツデータの提供先が、共有済みの通信パラメータにより構成された無線ネットワークを介して接続されているか否かに応じて、第１の暗号鍵を用いてコンテンツデータを暗号化するか否かを切替える。

【００４４】

ステップＳ４１３では、通信装置１０１－１は通信装置１０１－２と通信パラメータ設定処理の際に共有した第１の暗号鍵が有効か否かを判断する。ここで「有効」とは使用可能（破棄されていない、或いは、正しい暗号鍵）であることを意味する。

【００４５】

もし第１の暗号鍵が無効だった場合（ステップＳ４１３において「ＮＯ」）、処理を終了する。この時、ＵＩ等でエラーの旨をユーザに通知する。一方、第１の暗号鍵が有効だった場合（ステップＳ４１３において「ＹＥＳ」）、ステップＳ４１４に移行して通信装置１０１－１は第１の暗号鍵で画像データを暗号化する。

【００４６】

このように本実施形態では通信パラメータ設定処理において通信パラメータの送受信のために使用した第１の暗号鍵を、コンテンツデータを送信する際にコンテンツデータ自体の暗号化にも用いる。なお、コンテンツデータを暗号化する際には、ＳＳＬ等による上位レイヤでの通信路の暗号化を行わなくていいが、より強固なセキュリティをかけたい場合は、上位レイヤでの通信路の暗号化を行っても良い。上位レイヤでの通信路の暗号化を行うか否かは、通信速度とセキュリティのいずれを重視するかに応じてユーザが選択的に切替えられるようにしても良い。

【００４７】

ステップＳ４１５において通信装置１０１－１は、サーバ１０３のＵＲＬ及びＩＰアドレス情報等を基に、第１の暗号鍵で暗号化した画像データをサーバ１０３に送信する。このとき、サーバ１０３に送信した画像データを通信装置１０１－２が復号できるか否かの判断を可能にするために、データフレームに復号可能な暗号鍵の識別情報を紐づけておいても構わない。

【００４８】
次に、図５を参照して本実施形態における通信装置１０１－２における処理の一例を説明する。図５は発明の実施形態に対応する通信装置１０１－２における処理の一例を示すフローチャートである。図５において、ステップＳ５０１以前の処理は図４のステップＳ４０１からＳ４０９までの処理と同様であるので説明を省略する。
【００４９】
通信装置１０１－２はステップＳ４０９でネットワークに接続したことを確認すると、ステップＳ５０１に移行する。ステップＳ５０１において通信装置１０１－２は、ユーザからの指示に基づいて画像データをダウンロードするか否かを判断する。もし、ダウンロードを希望する場合（ステップＳ５０１において「ＹＥＳ」）、ステップＳ５０２に移行する。
【００５０】
ステップＳ５０２では、通信装置１０１－２がデータ送信装置と直接通信できるか否かを判断する。本実施形態ではデータ送信装置は、通信装置１０１－１が該当する。直接通信できるか否かは、通信装置１０１－２が存在するネットワーク内でＭＡＣレイヤでの検知処理を行い、データ送信装置（通信装置１０１－１）を発見できるか否かで判断する。本実施形態では、通信パラメータ設定処理により共有された通信パラメータを用いた無線ネットワークに接続している場合に、直接通信可能と判断される。つまり、通信装置１０１－２が通信装置１０１－１とアドホックネットワーク接続をした場合は直接通信可能と判断され、アクセスポイント１０２－２に接続した場合には、直接通信不可能と判断されることになる。
【００５１】
もし、直接通信ができる場合は（ステップＳ５０２において「ＹＥＳ」）、ステップＳ５０３に移行する。ステップＳ５０３では、通信装置１０１－２は、データ送信装置（通信装置１０１－１）に画像データ要求を送信して、画像データを受信する。続くステップＳ５０４では通信装置１０１－２はデータ送信装置（通信装置１０１－１）から画像データの受信が完了したか否かを判定する。もし、画像データの受信が完了した場合は（ステップＳ５０４において「ＹＥＳ」）、処理を終了する。上述したように、直接通信する場合には無線通信路が第２の暗号鍵で暗号化されており、画像データ自体は暗号化されていない。よって通信装置１０１－２は第２の暗号鍵により無線通信路を復号化し、画像データを得る。
【００５２】
一方、直接通信ができない場合（ステップＳ５０２において「ＮＯ」）、ステップＳ５０５に移行する。ステップＳ５０５では、共有すべき画像データが存在する指定の場所にアクセスする。具体的には、サーバ１０３のＵＲＬ情報及びIPアドレスを利用してサーバ１０３にアクセスする。続くステップＳ５０６では、通信装置１０１－２は、サーバ１０３に通信装置１０１－１が送信した画像データが存在するか否かを判定する。
【００５３】
もし、サーバ１０３に通信装置１０１－１が送信した画像データが存在する場合（ステップＳ５０６において「ＹＥＳ」）、ステップＳ５０７に移行する。ステップＳ５０７では通信装置１０１－１と通信パラメータ設定処理を行った際に共有した第１の暗号鍵が有効か否かを判断する。ここで「有効」とは使用可能（破棄されていない、正しい暗号鍵）であることを意味する。
【００５４】
もし、第１の暗号鍵が無効だった場合（ステップＳ５０７において「ＮＯ」）、ＵＩ等でユーザに処理がエラーになったことを通知して処理を終了する。一方、第１の暗号鍵が有効だった場合（ステップＳ５０７において「ＹＥＳ」）、ステップＳ５０８において通信装置１０１－２は画像データをダウンロードする。ダウンロードした画像データは暗号化されているので、通信装置１０１－２はステップＳ５０９において、該画像データを第１の暗号鍵を使って復号化し、元の画像データを取得する。

【００５５】
以上のように、第１の実施形態では、通信パラメータの設定処理において通信パラメータを共有するために利用した第１暗号鍵を記憶しておく。そして、該通信パラメータを用いて構成される無線ネットワークとは異なるネットワークに接続されたサーバ等の外部装置にコンテンツデータを送信する際には、該第１の暗号鍵をコンテンツデータの暗号化に利用する。当該第１の暗号鍵は通信パラメータの設定処理を行った通信装置同士でしか知り得ない情報であるので、外部装置に一時的にコンテンツデータがアップロードされた場合でも、第三者が該コンテンツデータを盗み見ることを効果的に防止することができる。
【００５６】
［第２の実施形態］
以下、本発明の第２の実施形態を説明する。図６は、発明の第２の実施形態に対応するデータ共有システム構成の一例を示す図である。インターネット６００は、ＴＣＰ／ＩＰプロトコルに従ってノード間の通信を可能とするネットワークである。インターネット６００は、インターネットに限らず、ＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）やＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）、或いは、それらの組合せであってもよい。
【００５７】
通信装置６０１－１、６０１－２及び６０１－３は、公衆無線ＬＡＮ対応アクセスポイント（以下アクセスポイント）６０２－１、６０２－２或いは６０２－３を介して無線通信を行う通信装置である。以下、複数の通信装置を代表して通信装置６０１といい、複数のアクセスポイントを代表してアクセスポイント６０２という。通信装置６０１は、無線ネットワークを構成するための通信パラメータの自動設定機能を有している。
【００５８】
本実施形態では、通信装置６０１－１はアクセスポイント６０２－１に接続を行う権限を有し、アクセスポイント６０２－１が形成するインフラストラクチャモードの無線ネットワークに接続するための通信パラメータを記憶しているものとする。通信装置６０１－２はアクセスポイント６０２－２に接続を行う権限を有し、アクセスポイント６０２－２が形成するインフラストラクチャモードの無線ネットワークに接続するための通信パラメータを記憶しているものとする。通信装置６０１－３はアクセスポイント６０２－３に接続を行う権限を有し、アクセスポイント６０２－３が形成するインフラストラクチャモードの無線ネットワークに接続するための通信パラメータを記憶しているものとする。なお、通信装置６０１の数は図６に示す３つに限定されるものではなく、より多くの通信装置がアクセスポイントに接続されても良い。その場合、各通信装置は権限を有する限りどのアクセスポイントに接続してもよく、同様の結果が得られることは言うまでもない。
【００５９】
アクセスポイント６０２は、インターネット６００と接続されたアクセスポイントである。アクセスポイント６０２は、無線ＬＡＮ通信接続機能を各通信装置に提供する。アクセスポイント６０２の数は図６に示した３つに限定されるものではなく、より多くのアクセスポイントがインターネット６００に接続されていてもよい。又、本実施形態では、アクセスポイント６０２に接続してインターネット６００に接続する形態で説明を行うが、携帯電話などの公衆網を介してインターネット６００に接続しても構わない。
【００６０】
サーバ６０３は、インターネット６００と接続され、インターネット６００を介して通信装置６０１から送信される画像データ等のコンテンツデータが格納される。ネットワーク６０４は、通信装置６０１－１と通信装置６０１－３が通信パラメータ設定後に構築したアドホックネットワークである。当該ネットワーク６０４を介して通信装置６０１－１と６０１－３は直接通信を行うことができる。なお、アドホックネットワークを構築する通信装置６０１の数は２つに限定されるものではなく、３つ以上の通信装置６０１で構築しても良い。
【００６１】

なお、本実施形態の通信装置６０１のハードウェア構成や機能モジュール構成は第１の実施形態において図２、図３を参照して説明したものと同様であるので、ここでの説明は省略する。

【００６２】

次に本実施形態における処理の概要を説明する。本実施形態では、最初に各通信装置６０１間でアドホックネットワークを形成するための通信パラメータ自動設定を行う。この自動設定の際に、サーバ６０３の情報も通信装置６０１間で共有する。通信パラメータ設定後、通信装置６０１－１と通信装置６０１－３は共有した通信パラメータを利用してアドホック接続を行い、アドホックネットワーク６０４を形成する。通信装置６０１－２は該アドホックネットワーク６０４には参加せず、アクセスポイント６０２－２が形成する無線ネットワークに接続する。

【００６３】

通信装置６０１－１と通信装置６０１－３のアドホック接続が終了すると、アドホック切断処理を行ってネットワーク６０４を解消する。その後、通信装置６０１－１はアクセスポイント６０２－１に接続する。通信装置６０１－３はアクセスポイント６０２－３に接続する。

【００６４】

以下、ある通信装置６０１がインターネット６００経由でサーバ６０３に画像データを送信し、他の通信装置６０１がサーバ６０３にある画像データを受信する場合を説明する。本実施形態では特に、通信装置６０１－１がサーバ６０３に画像データをアップロードし、通信装置６０１－２、６０１－３がサーバ６０３から画像データをダウンロードする場合を説明する。本実施形態の通信装置６０１－１は画像データ送信時に、通信装置６０１－２及び６０１－３が復号できる暗号化、通信装置６０１－３のみが復号できる暗号化をかける点に特徴を有する。これにより画像データを参照できる通信装置をグループ分けすることができる。尚、通信装置６０１－１が画像データの受信側となり、通信装置６０１－２又は６０１－３が画像データの送信側となってもよい。

【００６５】

本実施形態では、通信パラメータ設定処理につきＷＰＳ(Wi-Fi Protected Setup)をアドホックモードに適用した場合を例にして説明する。また、本実施形態では、アクセスポイント６０２に接続してインターネット６００に接続する形態で説明を行うが、携帯電話などの公衆網を介してインターネット６００に接続しても構わない。

【００６６】

次に、図７を参照して本実施形態に対応する通信装置６０１の処理の一例を説明する。ここでは特に、画像データの送信側である通信装置６０１－１における処理を説明する。図７は、発明の実施形態に対応する通信装置６０１－１の処理の一例を示すフローチャートである。

【００６７】

ステップＳ７０１では、通信装置６０１－１は通信パラメータの設定処理が開始されたか否かを判断する。本実施形態ではＷＰＳが開始されたかを判断する。次にステップＳ７０２では通信送置６０１－１は、通信パラメータ設定を行う対向通信装置が存在するかどうかを判断する。ここでは実行主体が通信装置６０１－１であり、対向通信装置は通信装置６０１－２及び６０１－３とする。ステップＳ７０２では、例えば、ＷＰＳを起動中であることを示す情報が付加されたビーコンを受信したか否かにより、対向通信装置が存在するか否かを判断することができる。また、プローブリクエストを送信し、ＷＰＳを起動中であることを示す情報が付加されたプローブレスポンスを受信したか否かにより、対向通信装置が存在するか否かを判断することもできる。

【００６８】

通信装置６０１－１は、対向通信装置６０１－２や６０１－３が存在しなければ（ステップＳ７０２において「ＮＯ」）、ＵＩ等で発見できなかった旨を伝えて、ステップＳ７０３で通信パラメータ設定処理をエラー終了する。通信装置６０１－１は、通信パラメー

タ設定処理がエラー終了した場合、ステップＳ７０１の初期状態に遷移する。

【００６９】

一方、対向通信装置が存在する場合（ステップＳ７０２において「ＹＥＳ」）、ステップＳ７０４に移行する。ステップＳ７０４で通信装置６０１－１は第１の暗号鍵を対向通信装置６０１－２、６０１－３と共有する。具体的には、Diffie-Hellmanの鍵交換アルゴリズムを用いることにより、第１の暗号鍵が共有される。ここで第１の暗号鍵は、通信パラメータ設定処理において、通信パラメータ等の各種情報を送受信する際の暗号化、及び復号化に使用される。

【００７０】

続いてステップＳ７０５において通信装置６０１－１は、通信装置６０１－２、６０１－３との間でサーバのＵＲＬ及びＩＰアドレス情報等の共有を行う。本実施形態では、サーバ６０３に画像データを置くことで、画像データの共有を行うためサーバ６０３のＵＲＬ情報及びＩＰアドレス等を取得する。サーバ６０３以外のデータ保持通信装置でコンテンツデータの共有を行うときは、ステップＳ７０６でデータ保持通信装置のアドレス情報（ＵＲＬ，ＩＰアドレスなど）を共有する。

【００７１】

続くステップＳ７０７において通信装置６０１－１は、通信装置６０１－２、６０１－３との間で無線ネットワーク構成に必要な通信パラメータを共有する。なお、Ｓ７０５～Ｓ７０７でＵＲＬ、データ保持通信装置、通信パラメータ等の各種情報を共有する際には、第１の暗号鍵で該情報の暗号化、及び復号化を行う。また、ここではＳ７０５～Ｓ７０７を別々の処理として説明したが、これらの処理をまとめて行っても構わない。即ち、ＵＲＬ、データ保持通信装置、通信パラメータ等を１つのフレームに格納して送受信するようにしても構わない。また、必ずしもＵＲＬ、及びデータ保持通信装置の情報を通信パラメータ設定時に共有するのではなく、予め通信装置６０１－１と通信装置６０１－２、６０１－３に記憶させておいても構わない。

【００７２】

上記処理により通信装置６０１間で共有された第1の暗号鍵、通信パラメータ、サーバ６０３のＵＲＬやデータ保持通信装置のアドレス情報は記憶部３０２に記憶される。ステップＳ７０８では、通信装置６０１－１は、通信パラメータ設定処理を終了する。次いでステップＳ７０９では通信装置６０１－１は、ネットワーク判断部３０５によりアドホックネットワークの接続が行われたか否かを判断する。本実施形態では通信装置６０１－１は、通信装置６０１－２、又は通信装置６０１－３の少なくともいずれか一方との間で無線ネットワーク接続が行われたかを判断する。

【００７３】

アドホックネットワーク接続した場合は（ステップＳ７０９において「ＹＥＳ」）、ステップＳ７１０に移行する。ステップＳ７１０では、対向通信装置との間でアドホックモードによる無線通信に使用する第２の暗号鍵を共有して記憶する。ここで共有される第２の暗号鍵は、第1の実施形態で説明したセッション鍵（ユニキャスト通信用の第２の暗号鍵）、及びグループ鍵（マルチキャスト通信用の第２の暗号鍵）である。

【００７４】

次に図８を参照して通信装置６０１－１がアクセスポイント６０２－１と接続してサーバ６０３に画像データをアップロードする場合の処理を説明する。なお、図８の処理は、通信パラメータの設定処理が完了した後であれば（図７のステップＳ７０８以降であれば）いつでも実行可能である。

【００７５】

ステップＳ８０１において通信装置６０１－１は他の通信装置と共有したい画像データがあるかどうかを判断する。ここでの判断は、例えばユーザの選択や、通信装置６０１－１内に新しい画像データが追加されかどうかに基づいて行うことができる。もし共有したい画像データがある場合（ステップＳ８０１において「ＹＥＳ」）、ステップＳ８０２に移行する。

【００７６】
ステップＳ８０２では、通信装置６０１－１は、画像データを共有したい通信装置と、直接通信できるかどうかを判定する（第２の判定）。本実施形態では、通信装置６０１－１が画像データを共有したい通信装置は、通信装置６０１－２又は通信装置６０１－３とする。直接通信できるか否かは、通信装置が存在するネットワーク内でＭＡＣレイヤでの検知処理を行い、画像データを共有したい他の通信装置を発見できるか否かで判定する。本実施形態では、通信パラメータ設定処理により共有された通信パラメータを用いた無線ネットワークを確立済みの場合に、直接通信可能と判定される。つまり、通信装置６０１－１が通信装置６０１－２、又は通信装置６０１－３とアドホックネットワーク接続をしている場合は直接通信可能と判定され、アクセスポイント６０２－１に接続している場合には、直接通信不可能と判定されることになる。

【００７７】
Ｓ８０２の判定結果に基づき、もし、直接通信が可能な場合（ステップＳ８０２において「ＹＥＳ」）、ステップＳ８０３に移行して画像データを共有したい通信装置はグループ（複数）か単体かの判断を行う。この判断は、例えばユーザ操作により複数の通信装置が選択されたか１つの通信装置が選択されたかに基づいて行う。もし、グループの場合（ステップＳ８０３において「ＹＥＳ」）、ステップＳ８０４に移行する。ステップＳ８０４では、通信装置６０１－１は画像データに暗号化をかけずに共有したい通信装置のグループに、マルチキャストで画像データを送信する。なお、この場合はグループ鍵（マルチキャスト通信用の第２の暗号鍵）により暗号化された無線通信路を介して画像データが送信される。一方、データを共有したい通信装置６０１が単体の場合（ステップＳ８０３において「ＮＯ」）、ステップＳ８０５に移行する。ステップＳ８０５では、画像データに暗号化をかけずに共有したい単体の通信装置に、ユニキャストで画像データを送信する。なお、この場合はセッション鍵（ユニキャスト通信用の第２の暗号鍵）により暗号化された無線通信路を介して画像データが送信される。このように、直接通信可能な場合は、無線通信路に暗号化がかかっており、かつサーバなどの中継装置を介さずに送信されるため、画像データに暗号化をかけずに送信する。

【００７８】
ステップＳ８０２において直接通信が不可能な場合（ステップＳ８０２において「ＮＯ」）、ステップＳ８０６に移行する。ステップＳ８０６では、通信装置６０１－１は画像データを共有したい通信装置が、通信パラメータ設定処理のみを実行した通信装置であるか否かを判断する。つまり、通信パラメータの設定処理により通信パラメータは共有されているものの、該共有された通信パラメータを用いた無線ネットワーク接続を未だしていない他の通信装置との間で画像データを共有するか否かが判断される。図７のステップＳ７０９、Ｓ７１０の処理を実行済みの場合はステップＳ８０６の「ＮＯ」に進み、実行済みでない場合はステップＳ８０６の「ＹＥＳ」に進むこととなる。なお、ステップＳ８０６における判断に基づいて、データを暗号化するための暗号鍵が選別されることとなる。

【００７９】
もし、通信パラメータ設定処理のみを実行した通信装置との間で画像データを共有したい場合（ステップＳ８０６において「ＹＥＳ」）、ステップＳ８０７に移行して第１の暗号鍵が有効か否かを判断する。ここで「有効」とは使用可能（破棄されていない、正しい第１の暗号鍵）ことを意味する。通信装置６０１－１は、第１の暗号鍵が無効だった場合（ステップＳ８０７において「ＮＯ」）、ＵＩ等でユーザに処理がエラーになったことを通知して処理を終了する。

【００８０】
一方、第１の暗号鍵が有効だった場合（ステップＳ８０７において「ＹＥＳ」）、ステップＳ８０８において通信装置６０１－１は第１の暗号鍵で画像データを暗号化する。

【００８１】
このように本実施形態でも通信パラメータ設定処理時に通信パラメータの送受信のために使用した第１の暗号鍵を、コンテンツデータを送信する際にコンテンツデータ自体の暗

号化にも用いる。なお、コンテンツデータそのものに暗号化をかける場合は、ＳＳＬ等による上位レイヤでの通信路の暗号化を行わなくていいが、より強固なセキュリティをかけたい場合は、上位レイヤでの通信路の暗号化をかけても良い。上位レイヤでの通信路の暗号化を行うか否かは、通信速度とセキュリティのいずれを重視するかに応じてユーザが選択的に切替えられるようにしてもよい。

【００８２】

続くステップＳ８０９において通信装置６０１－１は、サーバ６０３のURL及びＩＰアドレス情報等を基に、第１の暗号鍵で暗号化を行った画像データをサーバ６０３に送信する。このとき、サーバ６０３に送信した画像データを通信装置６０１－２や通信装置６０１－３が復号できるか否かの判断を可能にするために、データフレームに復号可能な暗号鍵の識別情報を紐づけておいても構わない。送信が完了したら処理を終了する。

【００８３】

本実施形態では、通信装置６０１－１は６０１－３との間ではアドホックネットワーク６０４を形成済みであるが、通信装置６０１－２とはアドホック接続を行っていない。一方で通信パラメータの共有のために使用した第1の暗号鍵は共に保持しているため、通信装置６０１－２との間でデータを共有したい場合は第１の暗号鍵で画像データの暗号化を行う。画像データを共有したい通信装置が、通信パラメータ設定処理後に無線ネットワーク接続を実行した通信装置であると判断された場合（ステップＳ８０６において「ＮＯ」）、ステップＳ８１０に移行する。ステップＳ８１０では、一度アドホックネットワーク６０４を構成した（通信パラメータ設定処理によって取得した通信パラメータを利用して接続処理を行った）通信装置全体（グループ）で画像データを共有するか否かを判定する。

【００８４】

もし、グループで共有する場合は（ステップＳ８１０において「ＹＥＳ」）、ステップＳ８１１に移行し、単体の通信装置と共有する場合は（ステップＳ８１０において「ＮＯ」）、ステップＳ８１４に移行する。

【００８５】

ステップＳ８１１では、通信装置６０１のグループが復号化できるグループ鍵（マルチキャスト通信用の第２の暗号鍵）が有効か否かを判断する。ここでの「有効」とは使用可能（破棄されていない、正しいグループ鍵）を意味する。もしグループ鍵が無効だった場合（ステップＳ８１１で「ＮＯ」）、ＵＩ等でユーザに処理がエラーになったことを通知して処理を終える。グループ鍵が有効だった場合（ステップＳ８１１で「ＹＥＳ」）、ステップＳ８１２に移行して通信装置６０１－１は、グループ鍵で画像データの暗号化を行う。

【００８６】

続くステップＳ８１３において通信装置６０１－１は、サーバ６０３のURL及びＩＰアドレス情報等を基に、グループ鍵で暗号化を行った画像データをサーバ６０３に送信する。

【００８７】

ステップＳ８１４では、単体の通信装置（本実施形態では通信装置６０１－３）が復号化できるセッション鍵（ユニキャスト通信用の第２の暗号鍵）が有効か否かを判断する。ここでの「有効」とは使用可能（破棄されていない、正しいセッション鍵）を意味する。もしセッション鍵が無効だった場合（ステップＳ８１４で「ＮＯ」）、ＵＩ等でユーザに処理がエラーになったことを通知して処理を終える。セッション鍵が有効だった場合（ステップＳ８１４で「ＹＥＳ」）、ステップＳ８１５に移行して通信装置６０１－１は、データを共有させたい通信装置６０１－３が復号可能なセッション鍵で画像データの暗号化を行う。

【００８８】

続くステップＳ８１６において通信装置６０１－１は、サーバ６０３のURL及びIPアドレス情報等を基に、セッション鍵で暗号化を行った画像データをサーバ６０３に送信する

。このとき画像データの共有を行う通信装置６０１－３が、画像データを復号できるか否かの判断を可能にするために、データフレームに復号可能な暗号鍵の識別情報を紐づけておいても構わない。

【００８９】

次に、通信装置６０１－２、及び通信装置６０１－３の動作について図９を参照して説明する。

【００９０】

なお、本実施形態では、通信装置６０１－２は図９のステップＳ９０１の前に図７のステップＳ７０１からステップＳ７０８までの処理を行い、通信装置６０１－３はステップＳ７０１からステップＳ７１０までの処理を行っているものとする。

【００９１】

通信装置６０１－２、又は６０１－３は、ステップＳ９０１においてデータをダウンロードするか否かを判断する。ここでの判断は、例えばユーザ選択に基づいて行う。もしダウンロードを行う場合は（ステップＳ９０１において「ＹＥＳ」）、ステップＳ９０２に移行する。ステップＳ９０２では、通信装置６０１－２、又は６０１－３は、画像データの送信装置と直接通信できるか否かを判断する。本実施形態ではデータ送信装置には通信装置６０１－１が該当する。直接通信できるか否かは、通信装置６０１－２、又は６０１－３が存在するネットワーク内で、ＭＡＣレイヤでの検知処理を行い、データ送信装置（通信装置６０１－１）を発見できるか否かで判断する。本実施形態では、通信パラメータ設定処理により共有された通信パラメータを用いた無線ネットワークに接続している場合に、直接通信可能と判断される。つまり、通信装置６０１－２、６０１－３が通信装置６０１－１とアドホックネットワーク接続をしている場合は直接通信可能と判断され、アクセスポイント６０２－２、６０２－３に接続している場合には、直接通信不可能と判断されることになる。

【００９２】

もし、直接通信ができない場合は（ステップＳ９０２において「ＹＥＳ」）、ステップＳ９０５に移行し、直接通信ができる場合は（ステップＳ９０２において「ＮＯ」）、ステップＳ９０３に移行する。

【００９３】

ステップＳ９０３では、通信装置６０１－２、６０１－３は画像データ要求をデータ送信装置（通信装置６０１－１）に送信し、対応する画像データを通信装置６０１－１から受信する。上述したように、直接通信する場合には無線通信路がセッション鍵、もしくはグループ鍵で暗号化されており、画像データ自体は暗号化されていない。よって通信装置６０１－２、６０１－３は第２の暗号鍵により無線通信路を復号化し、画像データを得る。ステップＳ９０４では、画像データの受信が完了したか否かを判定し、完了した場合は（ステップＳ９０４で「ＹＥＳ」）、処理を終える。

【００９４】

ステップＳ９０５では、通信装置６０１－２、又は６０１－３は、サーバ６０３のURL及びＩＰアドレス情報等に基づいてサーバ６０３にアクセスする。ステップＳ９０６では、通信装置６０１－２、６０１－３は、サーバ６０３に通信装置６０１－１が送信した画像データが存在するかを判定する。もしサーバ６０３に通信装置６０１－１が画像送信したデータが存在すれば（ステップＳ９０６において「ＹＥＳ」）、ステップＳ９０７に移行する。該画像データが存在しなければ（ステップＳ１００６において「ＮＯ」）、ＵＩ等でユーザに通知して処理を終了する。

【００９５】

続くステップＳ９０７では、通信装置６０１－２、又は６０１－３は、通信装置６０１－１と共有した暗号鍵が有効か否かを判定する。ここで「有効」とは使用可能（破棄されていない、正しい暗号鍵）を意味する。本実施形態では、通信装置６０１－２は第1の暗号鍵が有効か否かを確認する。又、通信装置６０１－３は第１の暗号鍵（通信パラメータ設定処理時に共有）と第２の暗号鍵（無線ネットワーク構成時に共有）とを持っている。

そこで、データの復号に必要な暗号鍵が有効かを判断する。

【００９６】

もしデータの復号に必要な暗号鍵が無効だった場合（ステップＳ９０７において「ＮＯ」）、ＵＩ等でユーザに処理がエラーになったことを通知して処理を終える。一方、暗号鍵が有効だった場合（ステップＳ９０７において「ＹＥＳ」）、ステップＳ１００８において画像データをサーバ６０３からダウンロードする。

【００９７】

ダウンロードした画像データは暗号化されているので、通信装置６０１－２、または６０１－３はステップＳ９０９において、当該画像データを対応する暗号鍵を使って復号化し、元の画像データを取得する。　本実施形態では、通信装置６０１－１は通信装置６０１－２と画像データを共有するために第１の暗号鍵で暗号化した画像データと、通信装置６０１－３と共有するために第２の暗号鍵で暗号化した画像データと、をサーバ６０３に送信している。よって通信装置６０１－２は、第１の暗号鍵で画像データを復号化することにより、元の画像データを取得できる。一方、通信装置６０１－３は、第１の暗号鍵、第２の暗号鍵を両方保持しているため、第１の暗号鍵、及び第２の暗号鍵のどちらを使用しても画像データを復号化することができる。

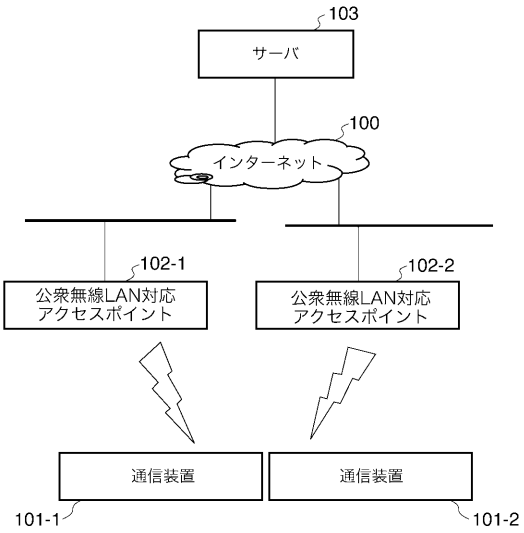
【００９８】

以上のように、第２の実施形態によれば、第１の暗号鍵に加え、通信パラメータ設定処理によって共有された通信パラメータを用いて構成される無線ネットワークでの無線通信路の暗号化に使用した第２の暗号鍵も記憶しておく。そして、該通信パラメータを用いて構成される無線ネットワークとは異なるネットワークに接続されたサーバ等の外部装置にコンテンツデータを送信する際には、該第１の暗号鍵、または第２の暗号鍵を用いてコンテンツデータを暗号化する。その際、第１、第２の暗号鍵のいずれを用いるかは、共有された通信パラメータを用いた無線ネットワーク接続を既に行ったか否かに応じて切替えることにより、コンテンツデータ毎に共有する通信装置の対象を絞り込むことができる。また、利用される暗号鍵はコンテンツデータを共有しようとする通信装置しか知り得ない情報であるので、外部装置に一時的にコンテンツデータがアップロードされた場合でも、第三者が該コンテンツデータを盗み見ることを効果的に防止することができる。

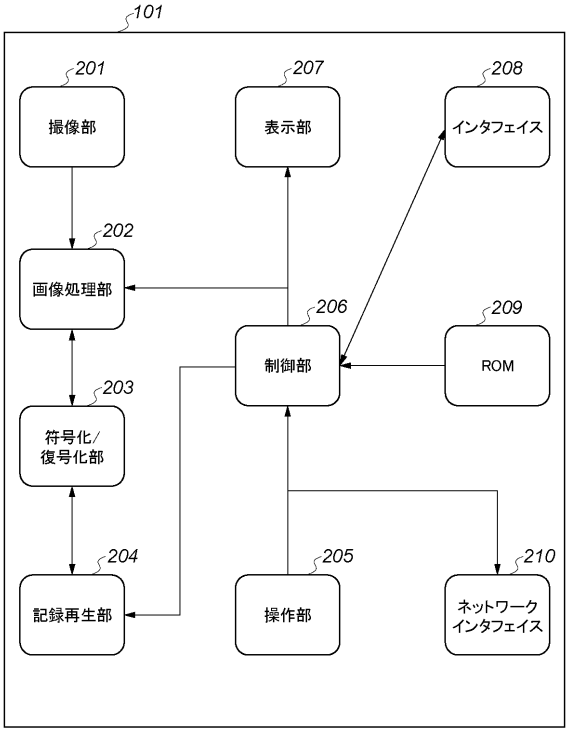
【００９９】

なお、本実施形態の機能を実現するソフトウェアのコンピュータプログラム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。

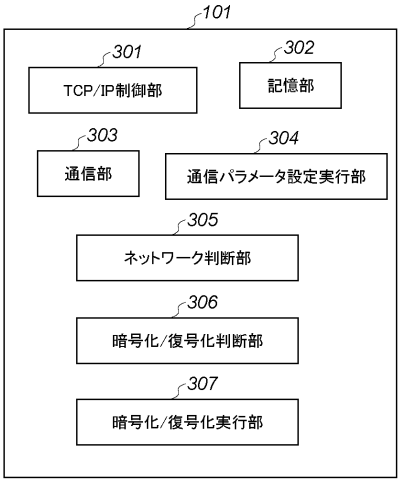
【図１】


103
サーバ
100
インターネット
102-1
公衆無線LAN対応
アクセスポイント
102-2
公衆無線LAN対応
アクセスポイント
通信装置
通信装置
101-1
101-2

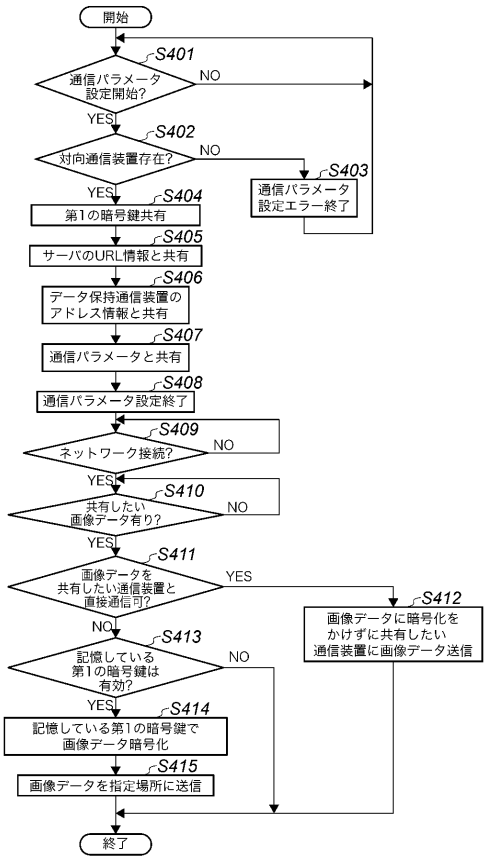
【図２】


101
201
撮像部
207
表示部
208
インタフェイス
202
画像処理部
206
制御部
209
ROM
203
符号化/
復号化部
204
記録再生部
205
操作部
210
ネットワーク
インタフェイス

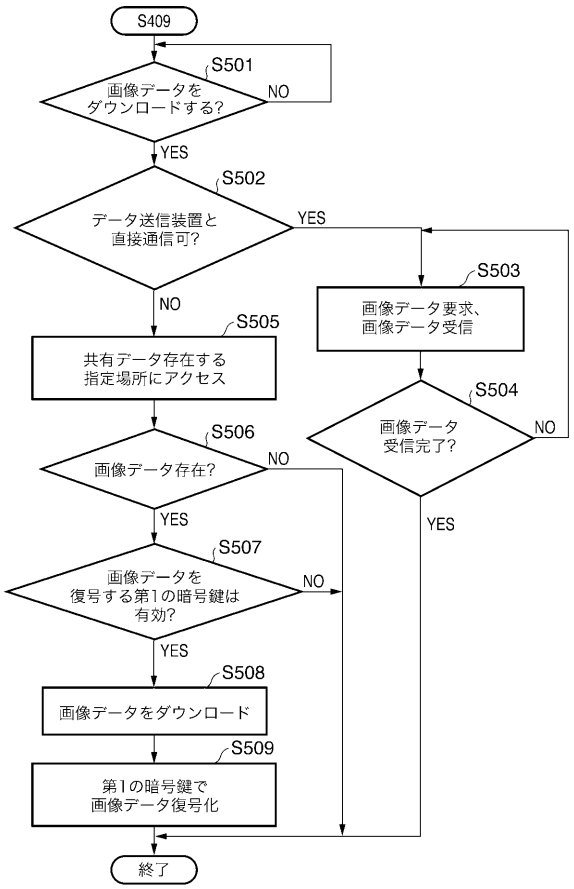
【図３】


101
301
TCP/IP制御部
302
記憶部
303
通信部
304
通信パラメータ設定実行部
305
ネットワーク判断部
306
暗号化/復号化判断部
307
暗号化/復号化実行部

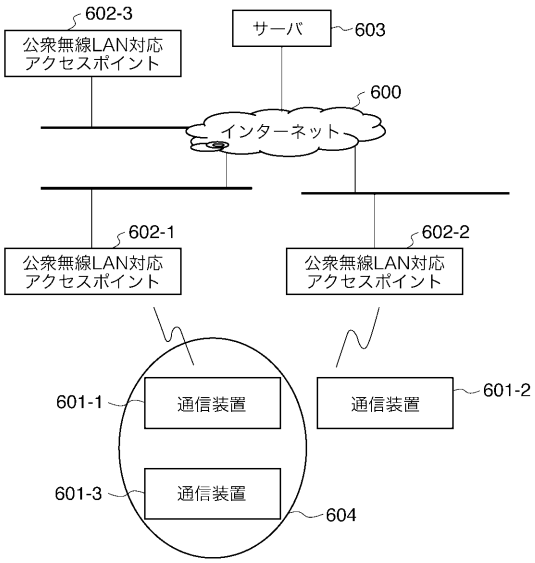
【図４】


開始
S401
通信パラメータ
設定開始?
NO
YES
S402
対向通信装置存在?
NO
S403
通信パラメータ
設定エラー終了
YES
S404
第1の暗号鍵共有
S405
サーバのURL情報と共有
S406
データ保持通信装置の
アドレス情報と共有
S407
通信パラメータと共有
S408
通信パラメータ設定終了
S409
ネットワーク接続?
NO
YES
S410
共有したい
画像データ有り?
NO
YES
S411
画像データを
共有したい通信装置と
直接通信可?
YES
S412
画像データに暗号化を
かけずに共有したい
通信装置に画像データ送信
NO
S413
記憶している
第1の暗号鍵は
有効?
NO
YES
S414
記憶している第1の暗号鍵で
画像データ暗号化
S415
画像データを指定場所に送信
終了

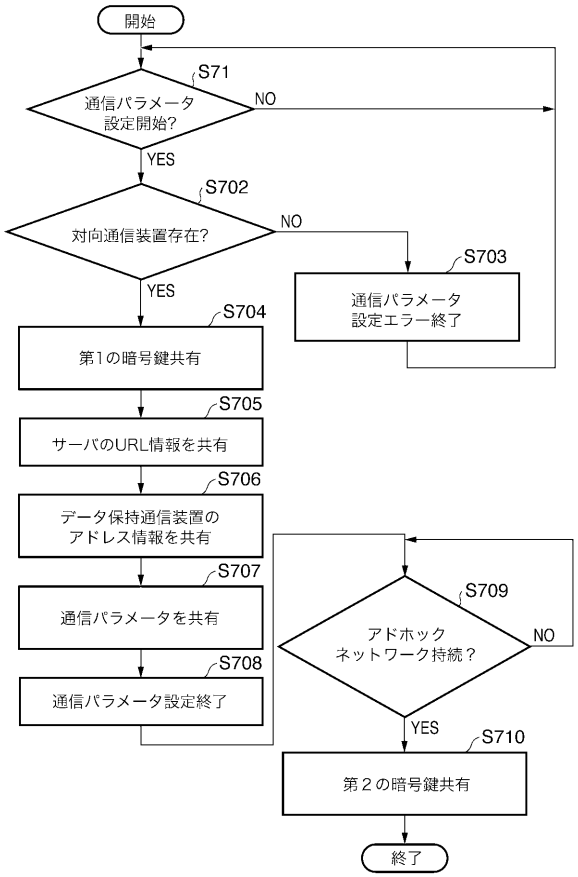
【図５】


S409
S501
画像データを
ダウンロードする?
NO
YES
S502
データ送信装置と
直接通信可?
YES
NO
S503
画像データ要求、
画像データ受信
S504
画像データ
受信完了?
NO
YES
S505
共有データ存在する
指定場所にアクセス
S506
画像データ存在?
NO
YES
S507
画像データを
復号する第1の暗号鍵は
有効?
NO
YES
S508
画像データをダウンロード
S509
第1の暗号鍵で
画像データ復号化
終了

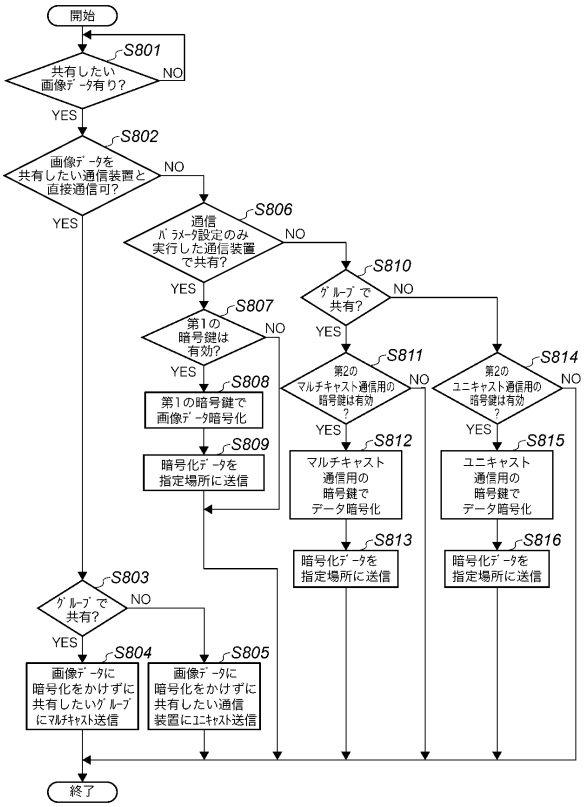
【図６】


602-3
公衆無線LAN対応
アクセスポイント
サーバ
603
600
インターネット
602-1
公衆無線LAN対応
アクセスポイント
602-2
公衆無線LAN対応
アクセスポイント
601-1
通信装置
通信装置
601-2
601-3
通信装置
604

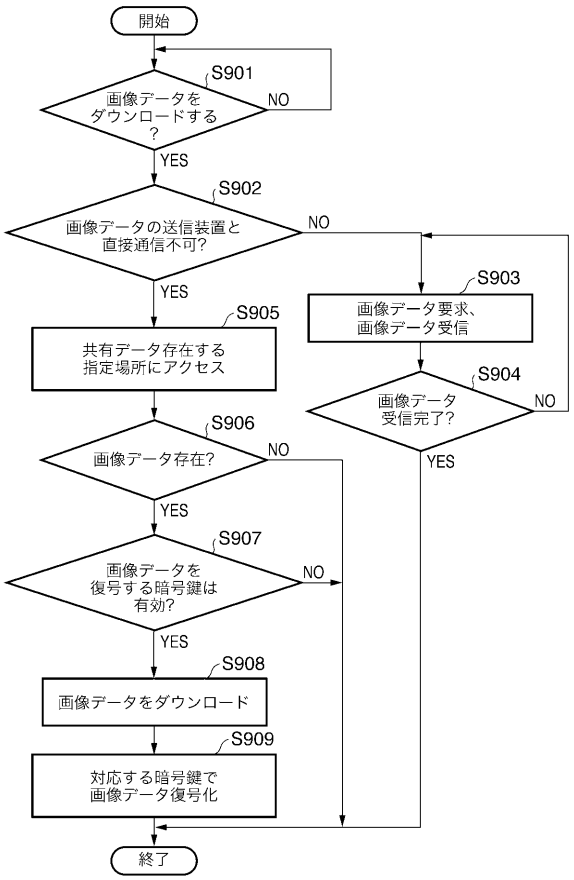
【図７】


開始
S71
通信パラメータ
設定開始?
NO
YES
S702
対向通信装置存在?
NO
YES
S703
通信パラメータ
設定エラー終了
S704
第1の暗号鍵共有
S705
サーバのURL情報を共有
S706
データ保持通信装置の
アドレス情報を共有
S707
通信パラメータを共有
S708
通信パラメータ設定終了
S709
アドホック
ネットワーク持続?
NO
YES
S710
第２の暗号鍵共有
終了

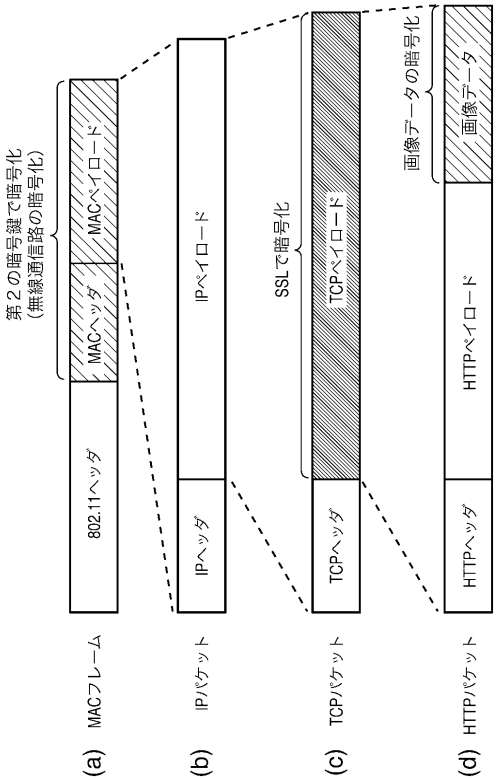
【図８】


開始
S801
共有したい
画像ﾃﾞｰﾀ有り?
NO
YES
S802
画像ﾃﾞｰﾀを
共有したい通信装置と
直接通信可?
NO
YES
S806
通信
ﾊﾟﾗﾒｰﾀ設定のみ
実行した通信装置
で共有?
NO
YES
S807
第1の
暗号鍵は
有効?
NO
YES
S808
第1の暗号鍵で
画像ﾃﾞｰﾀ暗号化
S809
暗号化ﾃﾞｰﾀを
指定場所に送信
S810
ｸﾞﾙｰﾌﾟで
共有?
NO
YES
S811
第2の
マルチキャスト通信用の
暗号鍵は有効
?
NO
YES
S812
マルチキャスト
通信用の
暗号鍵で
データ暗号化
S813
暗号化ﾃﾞｰﾀを
指定場所に送信
S814
第2の
ユニキャスト通信用の
暗号鍵は有効
?
NO
YES
S815
ユニキャスト
通信用の
暗号鍵で
データ暗号化
S816
暗号化ﾃﾞｰﾀを
指定場所に送信
S803
ｸﾞﾙｰﾌﾟで
共有?
NO
YES
S804
画像ﾃﾞｰﾀに
暗号化をかけずに
共有したいｸﾞﾙｰﾌﾟ
にﾏﾙﾁｷｬｽﾄ送信
S805
画像ﾃﾞｰﾀに
暗号化をかけずに
共有したい通信
装置にﾕﾆｷｬｽﾄ送信
終了

【図９】


開始
S901
画像データを
ダウンロードする
?
NO
YES
S902
画像データの送信装置と
直接通信不可?
NO
YES
S903
画像データ要求、
画像データ受信
S904
画像データ
受信完了?
NO
YES
S905
共有データ存在する
指定場所にアクセス
S906
画像データ存在?
NO
YES
S907
画像データを
復号する暗号鍵は
有効?
NO
YES
S908
画像データをダウンロード
S909
対応する暗号鍵で
画像データ復号化
終了

【図１０】


第２の暗号鍵で暗号化
(無線通信路の暗号化)
802.11ヘッダ
MACヘッダ
MACペイロード
IPヘッダ
IPペイロード
SSLで暗号化
TCPヘッダ
TCPペイロード
画像データの暗号化
HTTPヘッダ
HTTPペイロード
画像データ
(a) MACフレーム
(b) IPパケット
(c) TCPパケット
(d) HTTPパケット

フロントページの続き

(72)発明者　橘　秀明
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　青木　重徳

(56)参考文献　特開２００８－２１１６３８（ＪＰ，Ａ）
特開２００７－１６５９７７（ＪＰ，Ａ）
特開２００４－１２８７８５（ＪＰ，Ａ）
特開２００２－０９５０４７（ＪＰ，Ａ）
特開２００８－０６０７０４（ＪＰ，Ａ）
特開２００７－０２０７１７（ＪＰ，Ａ）
特開２００６－１５７６３５（ＪＰ，Ａ）
特開２００５－１６０００５（ＪＰ，Ａ）
特開２００４－１９９４１４（ＪＰ，Ａ）
特開２００６－８７０３２（ＪＰ，Ａ）
特開２００８－２２１６５（ＪＰ，Ａ）
特開２００４－４８４５８（ＪＰ，Ａ）
特表２００３－５０６９７２（ＪＰ，Ａ）
米国特許第６３６７０１８（ＵＳ，Ｂ１）
池野　信一，小山　謙二，“現代暗号理論”，日本，社団法人電子情報通信学会，１９９７年１１月１５日，初版第６刷，ｐ．２６３－２６４，２８１－２８２

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１６
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｗ　１２／０２
Ｈ０４Ｗ　８４／１２