(19)日本国特許庁(JP)

# (12)特許公報(B2)

(11)特許番号
特許第7113522号
(P7113522)

(45)発行日　令和4年8月5日(2022.8.5)

(24)登録日　令和4年7月28日(2022.7.28)

(51)国際特許分類

| | | | |
|---|---|---|---|
| *Ｇ０６Ｆ　21/60　(2013.01)* | Ｇ０６Ｆ | 21/60 | ３２０ |
| *Ｇ０６Ｆ　21/62　(2013.01)* | Ｇ０６Ｆ | 21/62 | ３０９ |
| *Ｈ０４Ｗ　4/06　(2009.01)* | Ｈ０４Ｗ | 4/06 | １７０ |
| *Ｈ０４Ｗ　12/08　(2021.01)* | Ｈ０４Ｗ | 12/08 | |
| *Ｈ０４Ｗ　48/18　(2009.01)* | Ｈ０４Ｗ | 48/18 | |

ＦＩ

請求項の数　6　（全22頁）　最終頁に続く

(21)出願番号　特願2019-179212(P2019-179212)
(22)出願日　令和1年9月30日(2019.9.30)
(65)公開番号　特開2020-57390(P2020-57390A)
(43)公開日　令和2年4月9日(2020.4.9)
審査請求日　令和4年6月17日(2022.6.17)
(31)優先権主張番号　特願2018-184535(P2018-184535)
(32)優先日　平成30年9月28日(2018.9.28)
(33)優先権主張国・地域又は機関
日本国(JP)
早期審査対象出願

(73)特許権者　500112146
サイレックス・テクノロジー株式会社
京都府相楽郡精華町光台二丁目３番地１
(72)発明者　西原　友美
京都府相楽郡精華町光台２－３－１サイレックス・テクノロジー株式会社内
審査官　平井　誠

最終頁に続く

(54)【発明の名称】　中継装置、通信制御方法、および、通信システム

(57)【特許請求の範囲】
【請求項１】
　通信端末と無線通信を介して接続し、且つネットワークを介してコンテンツデータを格納した通信装置と前記通信端末との間を中継する中継装置であって、
　前記通信端末と無線通信を行う第１通信部と、
　前記通信装置からコンテンツデータを受信する第２通信部と、
　前記受信したコンテンツデータを暗号化する必要があるか否かを判断し、暗号化する場合に前記受信したコンテンツデータを暗号化する暗号化部と、
　前記暗号化されたコンテンツデータを復号化するための復号化用情報をビーコンフレームに含めた特定ビーコンフレームを生成する復号化用情報生成部と、
　前記特定ビーコンフレームを送信すべき機会が到来し、且つ所定の条件を満たす場合に当該特定ビーコンフレームを発信するように制御する制御部と、
を備える中継装置。
【請求項２】
　前記所定の条件は、記憶部に予め設定された特定ビーコンフレームを発信する期間であり、
　前記制御部は、前記期間が終了すると特定ビーコンフレームからビーコンフレームに変更するよう制御する、
　請求項１に記載の中継装置。
【請求項３】

通信端末と無線通信を介して接続し、且つネットワークを介してコンテンツデータを格納した通信装置と前記通信端末との間を中継する中継装置の通信制御方法であって、
前記通信端末と無線通信を行う通信ステップと、
前記通信装置からコンテンツデータを受信する受信ステップと、
前記受信したコンテンツデータを暗号化する必要があるか否かを判断し、暗号化する場合に前記受信したコンテンツデータを暗号化する暗号化ステップと、
前記暗号化されたコンテンツデータを復号化するための復号化用情報をビーコンフレームに含めた特定ビーコンフレームを生成する生成ステップと、
前記特定ビーコンフレームを送信すべき機会が到来し、且つ所定の条件を満たす場合に当該特定ビーコンフレームを発信するように制御する制御ステップと、
を含む通信制御方法。
【請求項４】
ネットワークを介して、通信装置と通信端末との間の通信を中継する中継装置と、を備える通信システムであって、
前記中継装置は、
前記通信端末と無線通信を行う第１通信部と、
前記通信装置からコンテンツデータを受信する第２通信部と、
前記受信したコンテンツデータを暗号化する必要があるか否かを判断し、暗号化する場合に前記受信したコンテンツデータを暗号化する暗号化部と、
前記暗号化されたコンテンツデータを復号化するための復号化用情報をビーコンフレームに含めた特定ビーコンフレームを生成する復号化用情報生成部と、
前記特定ビーコンフレームを送信すべき機会が到来し、且つ所定の条件を満たす場合に当該特定ビーコンフレームを発信するように制御する制御部と、
を備え、
前記通信端末は、
前記暗号化されたコンテンツデータを受信する第３通信部と、
前記特定ビーコンフレームを受信した場合には、当該特定ビーコンフレームから復号化用情報を抽出し、前記暗号化されたコンテンツデータを復号する復号化部と、
を備える通信システム。
【請求項５】
ネットワークを介して、通信装置と通信端末との間の通信を中継する中継装置と、を備える通信システムであって、
前記中継装置は、
前記通信端末と無線通信を行う第１通信部と、
前記通信装置からコンテンツデータを受信する第２通信部と、
前記受信したコンテンツデータを暗号化する必要があるか否かを判断し、暗号化する場合に前記受信したコンテンツデータを暗号化する暗号化部と、
前記暗号化されたコンテンツデータを復号化するための復号化用情報を所定の形式で生成する復号化用情報生成部と、
ＰｒｏｂｅＲｅｓｐｏｎｓｅの特定箇所に前記所定の形式で生成された情報を格納し当該ＰｒｏｂｅＲｅｓｐｏｎｓｅを通信端末に向けて送信するように制御する制御部と、
を備え、
前記通信端末は、
前記暗号化されたコンテンツデータを受信する第３通信部と、
前記中継装置との間で無線通信を行うための無線接続処理に必要となる秘密鍵および公開鍵を生成する鍵生成部と、
前記公開鍵を、前記中継装置に向けて送信するＰｒｏｂｅＲｅｑｕｅｓｔの特定箇所に格納する制御部と、
前記中継装置から受信したＰｒｏｂｅＲｅｓｐｏｎｓｅの特定箇所から前記所定の形式で生成された復号化用情報を抽出する復号化部と、

を備える通信システム。
【請求項６】
前記中継装置の制御部は、前記通信端末から受信したＰｒｏｂｅＲｅｑｕｅｓｔの特定箇所から前記公開鍵を取得し、
前記中継装置の復号化用情報生成部は、前記復号化用情報を前記公開鍵を用いて暗号化し、
かつ、
前記通信端末の復号化部は、
前記秘密鍵を用いて、前記所定の形式で生成された復号化用情報を復号し、前記暗号化されたコンテンツデータを復号する、
請求項５に記載の通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線ＬＡＮ通信システムにおけるデータのセキュリティに関する。
【背景技術】
【０００２】
近年、ＰＣ（パーソナルコンピュータ）の小型化や持ち運び可能で大容量化した記憶媒体が普及しており、これら記憶媒体を紛失、盗難、盗聴される、あるいは悪意のあるソフトウェアなどにより、記憶媒体内の機密情報、個人情報など秘匿、または記憶媒体のみが記憶できることを認められた電子情報が外部に漏洩してしまうという事態が発生している。これらを防止するために種々の方法が提案され、実施されている。
【０００３】
ところで、近年、学校や塾など教育の現場（例えば教室など）でタブレットＰＣ（Personal Computer）のような携帯型の通信端末の普及に伴って、指導者（教師）の通信端末と各学習者（生徒）に与えられた複数の通信端末を利用して、無線通信（無線ＬＡＮ（Local Area Network）等）でネットワークを構築する通信システムが増えている。このような通信システムでは、教師用の通信端末や構内に設置された管理サーバから各授業に必要なコンテンツデータ（画像、動画、テキストファイルなど）を各生徒用の通信端末にダウンロードして、教師と各生徒が共に同じコンテンツデータを閲覧しながら、授業を行うこともある。
【０００４】
ここで、教師用や各生徒用の通信端末が、管理サーバから必要なコンテンツデータを無線通信でダウンロードを行い各通信端末のメモリーに格納する場合には、盗聴防止などセキュリティ向上のために無線通信を暗号化して通信する（例えば、ＷＰＡ等のプロトコルを用いるなど）などが行われている。
【０００５】
しかしながら、教師用や各生徒用の通信端末が必要なコンテンツデータを内部記憶媒体（メモリー）に格納してしまうと、通信端末の紛失、盗難、および通信端末内に存在する（知らないうちに侵入）悪意のあるソフトウェアなどにより、外部にコンテンツデータが漏洩する可能性がある。
【先行技術文献】
【特許文献】
【０００６】
【文献】特開２０１４－１８６５２９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
上記問題を解決するために、例えば、特許文献１に記載のデータ管理システムでは、位置情報に基づいて、予め登録された登録エリア内に対象データを備えた携帯端末が存在す

るか否かを判断し、登録エリア外であると判断されると、削除対象となるデータを携帯端末から削除されるようになっている。

【０００８】

しかしながら、特許文献１に記載のデータ管理システムでは、コンテンツそのものを削除してしまうため、例えば、教師が、外出（例えば出張、自宅など）などでコンテンツデータが格納された通信端末を特定エリア外（例えば、学校の外）に持ち出すたびに、コンテンツデータが削除されてしまい、その度、管理サーバから削除されたコンテンツデータを再取得する必要があり、使用者の利便性を損なう。つまり、ユーザが通信端末に取得したコンテンツデータを特定エリア内のみで、閲覧できるようにすればよい。

【０００９】

本発明は、上述の問題を解決するためになされたものであり、ユーザが取得した漏洩させたくないコンテンツデータを特定エリアでのみ閲覧できるようにセキュリティ保護することができる通信システムなどを提供することを目的とする。

【課題を解決するための手段】

【００１０】

本発明の一態様に係る中継装置は、通信端末と無線通信を介して接続し、且つネットワークを介してコンテンツデータを格納した通信装置と前記通信端末との間を中継する中継装置であって、通信端末と無線通信を行う第１通信部と、通信装置からコンテンツデータを受信する第２通信部と、受信したコンテンツデータを暗号化する必要があるか否かを判断し、暗号化する場合に受信したコンテンツデータを暗号化する暗号化部と、暗号化されたコンテンツデータを復号化するための復号化用情報をビーコンフレームに含めた特定ビーコンフレームを生成する復号化用情報生成部と、特定ビーコンフレームを送信すべき機会が到来し、且つ所定の条件を満たす場合に特定ビーコンフレームを発信するように制御する制御部と、を備える。

【００１１】

これによれば、中継装置は、通信端末のユーザが取得したい通信装置に格納されたコンテンツデータをネットワークを介して通信装置から取得し、自装置内で暗号化し、通信端末に向けて送信する。さらに、中継装置は、暗号化したコンテンツデータを復号するために用いる復号化用情報を作成し、特定ビーコンフレームに格納して、通信端末に提供する。これにより、通信端末は、通信端末で受信した暗号化されたコンテンツデータを特定ビーコンに含まれる復号化用情報を用いてコンテンツデータを利用できるようになる。このように、特定ビーコンを受信できるときのみ、暗号化されたコンテンツデータを利用することができ、コンテンツデータの運用におけるセキュリティ性を向上できる。よって、コンテンツデータの管理者は、漏洩させたくないコンテンツデータを特定エリア（特定ビーコンが受信可能な範囲）でのみ、ユーザ利用させることができる。

【００１２】

また、所定の条件は、記憶部に予め設定された特定ビーコンフレームを発信する期間であり、制御部は、前記期間が終了すると特定ビーコンフレームからビーコンフレームに変更するよう制御するようにしてもよい。

【００１３】

これによれば、中継装置は、特定ビーコンフレームを発信し続ける期間を設定できる。このように、特定ビーコンフレームを発信する期間を設定することで、ユーザは中継装置を使用する場合に、使用環境によって、従来の中継装置としても使用でき、ユーザの利便性が向上する。また、特定ビーコンの発信の期間のみ、暗号化されたコンテンツデータを利用できることから、コンテンツデータの運用におけるセキュリティを向上できる。

【００１４】

また、本発明の一態様に係る通信制御方法は、通信端末と無線通信を介して接続し、且つネットワークを介してコンテンツデータを格納した通信装置と通信端末との間を中継する中継装置の通信制御方法であって、通信端末と無線通信を行う通信ステップと、通信装置からコンテンツデータを受信する受信ステップと、受信したコンテンツデータを暗号化

する必要があるか否かを判断し、暗号化する場合に受信したコンテンツデータを暗号化する暗号化ステップと、暗号化されたコンテンツデータを復号化するための復号化用情報をビーコンフレームに含めた特定ビーコンフレームを生成する生成ステップと、特定ビーコンフレームを送信すべき機会が到来し、且つ所定の条件を満たす場合に特定ビーコンフレームを発信するように制御する制御ステップと、を含む。

【００１５】

これによれば、上記中継装置と同様の効果を奏する。

【００１６】

また、本発明の一態様に係る通信システムは、ネットワークを介して、通信装置と通信端末との間の通信を中継する中継装置と、を備える通信システムであって、中継装置は、通信端末と無線通信を行う第１通信部と、通信装置からコンテンツデータを受信する第２通信部と、受信したコンテンツデータを暗号化する必要があるか否かを判断し、暗号化する場合に受信したコンテンツデータを暗号化する暗号化部と、暗号化されたコンテンツデータを復号化するための復号化用情報をビーコンフレームに含めた特定ビーコンフレームを生成する復号化用情報生成部と、特定ビーコンフレームを送信すべき機会が到来し、且つ所定の条件を満たす場合に特定ビーコンフレームを発信するように制御する制御部と、を備え、通信端末は、暗号化されたコンテンツデータを受信する第３通信部と、特定ビーコンフレームを受信した場合には、特定ビーコンフレームから復号化用情報を抽出し、暗号化されたコンテンツデータを復号する復号化部と、を備える。

【００１７】

これによれば、上記中継装置と同様の効果を奏する。

【００１８】

また、本発明の別の一態様に係る通信システムは、ネットワークを介して、通信装置と通信端末との間の通信を中継する中継装置と、を備える通信システムであって、中継装置は、通信端末と無線通信を行う第１通信部と、通信装置からコンテンツデータを受信する第２通信部と、受信したコンテンツデータを暗号化する必要があるか否かを判断し、暗号化する場合に受信したコンテンツデータを暗号化する暗号化部と、暗号化されたコンテンツデータを復号化するための復号化用情報を所定の形式で生成する復号化用情報生成部と、ＰｒｏｂｅＲｅｓｐｏｎｓｅの特定箇所に前記所定の形式で生成された情報を格納し当該ＰｒｏｂｅＲｅｓｐｏｎｓｅを通信端末に向けて送信するように制御する制御部と、を備え、通信端末は、暗号化されたコンテンツデータを受信する第３通信部と、中継装置との間で無線通信を行うための無線接続処理に必要となる秘密鍵および公開鍵を生成する鍵生成部と、公開鍵を、中継装置に向けて送信するＰｒｏｂｅＲｅｑｕｅｓｔの特定箇所に格納する制御部と、中継装置から受信したＰｒｏｂｅＲｅｓｐｏｎｓｅの特定箇所から所定の形式で生成された復号化用情報を抽出する復号化部と、を備える。

【００１９】

これによれば、通信システムは、無線接続処理中に中継装置から通信端末に復号化用情報を送信することができる。これにより、通信システムは、無線通信におけるセキュリティを担保しつつ、暗号化されたコンテンツデータを復号することができ、結果、ユーザの利便性が向上する。

【００２０】

さらに、本発明の別の一態様に係る通信システムは、中継装置の制御部は通信端末から受信したＰｒｏｂｅＲｅｑｕｅｓｔの特定箇所から公開鍵を取得し、中継装置の復号化用情報生成部は復号化用情報を公開鍵を用いて暗号化し、かつ、通信端末の復号化部は、秘密鍵を用いて、所定の形式で生成された復号化用情報を復号し、暗号化されたコンテンツデータを復号するとしてもよい。

【００２１】

これによれば、通信システムは、暗号化されたコンテンツデータを復号化するための復号化用情報を、無線接続処理における公開鍵および秘密鍵を用いて暗号化および復号化することができるため、中継装置と通信端末との無線通信において、たとえ当該復号化用情

報が奪取されても、システムのセキュリティを担保できる。
【発明の効果】
【００２２】
本発明にかかる通信システムは、漏洩させたくないコンテンツデータを特定エリアでのみ閲覧できる。
【図面の簡単な説明】
【００２３】
【図１】図１は、本発明の実施の形態１にかかる通信システムの全体図である。
【図２】図２は、本発明の実施の形態１にかかる通信端末、中継装置のハードウェア構成図である。
【図３】図３は、本発明の実施の形態１にかかる中継装置の機能ブロック図である。
【図４】図４は、本発明の実施の形態１にかかる通信端末の機能ブロック図である。
【図５】図５は、本発明の実施の形態１にかかる中継装置が管理サーバからコンテンツデータ取得し通信端末に送信する処理のフロー図である。
【図６】図６は、本発明の実施の形態１にかかる通信端末が中継装置を介して管理サーバからコンテンツデータ取得し閲覧する処理のフロー図である。
【図７】図７は、本発明の実施の形態１にかかる中継装置が送信する特定ビーコンのフォーマットを説明した図の一例である。
【図８】図８は、本発明の実施の形態２にかかる通信システムの全体図である。
【図９】図９は、本発明の実施の形態２にかかる中継装置の機能ブロック図である。
【図１０】図１０は、本発明の実施の形態２にかかる通信端末の機能ブロック図である。
【図１１】図１１は、本発明の実施の形態２にかかる通信端末がユーザからの暗号化されたコンテンツデータを閲覧する旨の要求を受けてから閲覧できるまでの処理の一例を示すシーケンス図である。
【発明を実施するための形態】
【００２４】
以下、実施の形態について、図面を参照しながら具体的に説明する。
【００２５】
以下の実施の形態で示される数値、構成要素、構成要素の配置位置などは、一例であり、発明の範囲内において種々の変形や変更が可能である。
【００２６】
（実施の形態１）
図１は本発明の実施の形態にかかる通信システムの全体図である。
【００２７】
図１に示されるように、通信システム１００は、中継装置Ａ１と、通信端末Ｔ１と、管理サーバ（通信装置に相当）Ｓ１と、ＬＡＮ１１とを備える。通信システム１００は、通信端末Ｔ１が管理サーバＳ１に格納されたコンテンツデータを取得するために中継装置Ａ１を中継し取得する通信システムである。
【００２８】
中継装置Ａ１と管理サーバＳ１とは、ＬＡＮ１１を通じて、通信可能に接続されている。ＬＡＮ１１は、ＩＥＥＥ８０２．１１ａ、ｂ、ｇ、ｎ規格等に適合する無線ＬＡＮ、あるいはＩＥＥＥ８０２．３規格等に適合する有線ＬＡＮである。
【００２９】
中継装置Ａ１と通信端末Ｔ１とは、通信リンク１２を通じて、通信可能に接続されている。通信リンク１２は、ＩＥＥＥ８０２．１１ａ、ｂ、ｇ、ｎ規格等に適合する無線ＬＡＮで実現される。
【００３０】
中継装置Ａ１は、無線通信可能な通信端末Ｔ１と無線通信するアクセスポイントである。例えば、中継装置Ａ１は、通信端末Ｔ１からＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）パケットを受信した場合に、当該ＩＰパケットに含まれる宛先アドレスを取得し、受

信したＩＰパケットを当該宛先アドレスへＬＡＮ１１を介して転送する。
【００３１】
　また、中継装置Ａ１は、管理サーバＳ１に格納されたコンテンツデータ（例えば、画像、動画、テキストファイルなど）を取得する要求フレームを通信端末Ｔ１から受信した場合、当該要求フレームを管理サーバＳ１に転送し、管理サーバＳ１から要求を受けたコンテンツデータを受信し、一旦格納したうえで、暗号化が必要なコンテンツデータであるか否かを判断する。そして、中継装置Ａ１は、暗号化が必要な場合には、当該コンテンツデータを暗号化し通信端末Ｔ１に送信する。これらの判断プロセスおよび暗号化プロセスは後に詳述する。
【００３２】
　通信端末Ｔ１は、持ち運び可能な通信端末である。例えば、通信端末Ｔ１は、ノートＰＣ、タブレット端末、および携帯端末などである。通信端末Ｔ１は、少なくとも無線通信インタフェース（例えば、ＩＥＥＥ８０２．１１規格に準拠など）を備える。通信端末Ｔ１は、ユーザからの指示をもとに通信リンク１２を通じて中継装置Ａ１と通信を行う。例えば、通信端末Ｔ１は、ユーザが取得したい管理サーバＳ１に格納されたコンテンツデータを取得するために、ユーザの指示をもとに中継装置Ａ１を介して、管理サーバＳ１にコンテンツデータを取得のための要求を送信する。
【００３３】
　管理サーバＳ１は、複数のコンテンツデータを管理しているサーバである。管理サーバＳ１は、セキュリティ機能を備えており、自装置へのアクセス権を付与およびアクセスの制限などを行うこともできるし、認証機能（例えばログイン認証など）も備えている。管理サーバＳ１は、認証が成功した通信端末Ｔ１に対し、通信端末Ｔ１から取得要求があったコンテンツデータを提供する。
【００３４】
　無線通信可能領域１０は、中継装置Ａ１から発信される無線通信のための無線フレーム（例えば、ビーコンフレーム、マネージメントフレームなど）が到達できる領域を示している。通信可能領域１０は、障害物や送信出力などによって、時間経過とともに変化し得る。
【００３５】
　図２は、本発明の実施の形態にかかる通信端末、中継装置のハードウェア構成図である。図２に示すとおり、これらの装置は、ＣＰＵ２０、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）２１、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）２２、記憶装置２３、ＷＮＩＣ（Ｗｉｒｅｌｅｓｓ Ｎｅｔｗｏｒｋ Ｉｎｔｅｒｆａｃｅ Ｃａｒｄ）２４、ＮＩＣ（Ｎｅｔｗｏｒｋ Ｉｎｔｅｒｆａｃｅ Ｃａｒｄ）２５および各構成部品間を接続している内部バス２６などを備えている。
【００３６】
　ＣＰＵ２０は、ＲＯＭ２１に格納された制御プログラムを実行するプロセッサである。
【００３７】
　ＲＯＭ２１は、制御プログラム等を保持する読み出し専用記憶領域である。
【００３８】
　ＲＡＭ２２は、ＣＰＵ２０が制御プログラムを実行するときに使用するワークエリアとして用いられる記憶領域である。
【００３９】
　記憶装置２３は、制御プログラム、制御情報、装置情報、または認証情報などを記憶する記憶領域である。
【００４０】
　ＷＮＩＣ２４は、無線通信を行う無線通信インタフェースを備えている。例えば、ＩＥＥＥ８０２．１１ａ、ｂ、ｇ、ｎ、ａｃ規格等に適合する無線ＬＡＮの通信インタフェースである。
【００４１】

ＮＩＣ２５は、有線通信を行う有線通信インタフェースを備えている。例えば、ＩＥＥＥ８０２．３規格等に適合する有線ＬＡＮの通信インタフェースである。なお、ＮＩＣ２５は必ずしも備えている必要はない。

【００４２】

内部バス２６は、ＣＰＵ２０，ＲＯＭ２１、ＲＡＭ２２、記憶装置２３、ＷＮＩＣ２４、ＮＩＣ２５を電気的に接続し、信号のやりとりを行うバスである。

【００４３】

図３は、本発明の実施の形態にかかる中継装置Ａ１の機能ブロック図である。

【００４４】

図３に示す中継装置Ａ１は、第１通信部３１、記憶部３２、暗号化部３３、制御部３４、復号化用情報生成部３５、第２通信部３６などを備えている。

【００４５】

第１通信部３１は、自装置（中継装置Ａ１）が備える無線インタフェースを介して、通信端末Ｔ１と無線通信に関する種々の処理を行う。第１通信部３１は、管理サーバＳ１から受信して記憶部３２に格納された暗号化したコンテンツデータを通信端末Ｔ１に向けて送信し、送信した旨を制御部３４に通知する。第１通信部３１は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２、ＷＮＩＣ２４などにより実現される。

【００４６】

記憶部３２は、制御部３４の通知にもとづいて、管理サーバＳ１から受信した通信端末Ｔ１から取得要求のあるコンテンツデータを一時格納する。記憶部３２は、復号化用情報生成部３５で生成された、コンテンツデータの復号化用情報を含むビーコンフレームを記憶する。また、記憶部３２は、ユーザにより自装置に備わるツールなどを用いて入力された、自装置が動作するための種々の設定情報を記憶する。記憶部３２は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２、記憶装置２３などにより実現される。

【００４７】

暗号化部３３は、制御部３４の通知をもとに記憶部３２に一時格納したコンテンツデータ（管理サーバＳ１から受信したコンテンツ）内の暗号化するか否かのフラグ情報(暗号化フラグ情報)などを解析し、暗号化が必要か否かを判断する。ここで、暗号化すべきコンテンツか否かの判断は、本発明の実施の形態では管理サーバＳ１が管理しているコンテンツに予め含まれる暗号化フラグ情報などを解析することで判断することにしているが、中継装置Ａ１の記憶部３２に予めコンテンツデータのファイル形式によって判断する設定情報（例えば、ファイルの拡張子がＰＤＦなら暗号化するなど）によって、判断されてもよい。

【００４８】

また、暗号化部３３は、解析の結果、暗号化が必要であれば、記憶部３２に一時格納したコンテンツデータを暗号化する。そして、暗号化した旨を復号化用情報生成部３５に通知し、暗号化したコンテンツデータを第１通信部３１に渡す。一方、暗号化部３３は、解析の結果、暗号化が必要でなければ、記憶部３２に一時格納されたコンテンツデータをそのままに第１通信部３１に渡す。ここで、コンテンツデータの暗号化方法は、既知の暗号化技術（例えば、共通鍵方式のＲＣ５、公開鍵方式のＲＳＡなど）を用いて暗号化を行えばよく、ここでは暗号化方法について詳細な説明は省略する。なお、上述の暗号化とは、無線通信における秘匿のために行う暗号化処理とは別個に行われる処理である。暗号化部３３は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２などにより実現される。

【００４９】

復号化用情報生成部３５は、暗号化部３３の通知をもとに、暗号化部３３により暗号化されたコンテンツデータを復号化できる情報（復号化用情報）を、ビーコンフレームに格納して、この復号化用情報を含むビーコンフレームを新たに生成し、記憶部３２に渡す。なお、復号化用情報を含むビーコンフレームは、定常的に発信しているビーコンフレーム（以後、従来のビーコンフレーム、または、通常ビーコンフレームとも呼ぶ）と区別するために、以後、特定ビーコンフレームと呼ぶ。復号化用情報生成部３５は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２などにより実現される。

【００５０】
制御部３４は、第１通信部３１を通じて、通信端末Ｔ１から管理サーバＳ１に格納されたコンテンツデータを取得する要求を受信したか否かを判断する。
【００５１】
制御部３４は、第２通信部３６を通じて、通信端末Ｔ１が要求したコンテンツデータを管理サーバＳ１に要求し、受信できたか否かを判断する。制御部３４は、コンテンツデータを受信できた場合には暗号化部３３にその旨を通知し記憶部３２に受信したコンテンツデータを渡す。
【００５２】
また、制御部３４は、自装置（中継装置Ａ１）の通常ビーコンフレーム／特定ビーコンフレームを送信する機会が到来したか否かを判断する。ここで、送信する機会とは、例えば、中継装置Ａ１の存在を周囲の通信端末に周知するために発信する通常ビーコンフレーム／特定ビーコンフレームの発信タイミング（例えば、１００ｍｓ間隔）である。制御部３４は、特定ビーコンフレームを送信する機会が到来した場合は、第１通信部３１を通じて、記憶部３２に格納した特定ビーコンフレームを所定の条件を満たしているあいだ、周囲の通信端末に向けて発信する。
【００５３】
さらに、制御部３４は、所定の条件を満たしているか否かを判断する。制御部３４は、所定の条件を満たしている場合は、第１通信部３１から送信するビーコンフレームを特定ビーコンフレームに変更する。ここで、所定の条件とは、例えばユーザが中継装置Ａ１の設定ツールなどで記憶部３２に予め設定した特定ビーコンフレームを発信し続ける期間（特定ビーコン送信期間。例えば、暗号化コンテンツデータを送信したのちの３０日間、無期限など）である。このように特定ビーコンフレームを発信する期間を設定することで、ユーザは本発明の実施の形態における中継装置を使用する場合に、使用環境によって、従来の中継装置としても本発明の実施の形態における中継装置としても使用でき、ユーザの利便性が向上する。制御部３４は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２などにより実現される。
【００５４】
第２通信部３６は、自装置（中継装置Ａ１）が備える無線インタフェースまたは有線インタフェースを介して、ＬＡＮ１１上の管理サーバＳ１などと通信に関する種々の処理を行う。第２通信部３６は、制御部３４の通知をうけて、通信端末Ｔ１が要求したコンテンツデータを管理サーバＳ１に要求し、その応答を受信する。第２通信部３６は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２、ＷＮＩＣ２４などにより実現される。
【００５５】
図４は、本発明の実施の形態にかかる通信端末Ｔ１の機能ブロック図である。
【００５６】
図４に示す通信端末Ｔ１は、第３通信部４１、記憶部４２、制御部４３、復号化部４４、表示部４５などを備えている。
【００５７】
第３通信部４１は、自装置（通信端末Ｔ１）が備える無線インタフェースを用いて、中継装置Ａ１と無線通信に関する種々の処理を行う。第３通信部４１は、管理サーバＳ１に格納されたコンテンツデータを中継装置Ａ１に要求し、中継装置Ａ１が管理サーバＳ１から受信したコンテンツデータを受信する。第３通信部４１は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２、ＷＮＩＣ２４などにより実現される。
【００５８】
記憶部４２は、制御部４３の通知を受けて、コンテンツデータ（暗号化されたコンテンツデータか、または非暗号化コンテンツデータ）を記憶する。また、記憶部３２は、ユーザにより自装置に備わるツールなどを用いて入力された、自装置が動作するための種々の設定情報を記憶する。記憶部４２は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２、記憶装置２３などにより実現される。

【００５９】
制御部４３は、ユーザが通信端末Ｔ１に備わる入力装置（図示しない）により、第３通信部４１を通じて、管理サーバＳ１に格納されたコンテンツデータを中継装置Ａ１に要求したか否かを判断する。
【００６０】
制御部４３は、第３通信部４１を通じて、中継装置Ａ１から通信端末Ｔ１が要求したコンテンツデータを受信したか否かを判断する。制御部４３は、受信した場合は、受信したコンテンツデータを記憶部４２に渡す。
【００６１】
制御部４３は、ユーザが通信端末Ｔ１に備わる入力装置（図示しない）から記憶部４２に格納しているコンテンツデータを閲覧（利用）する指示をしたか否かを判断する。制御部４３は、ユーザが閲覧する指示をした場合は、その旨を復号化部４４に通知する。
【００６２】
制御部４３は、第３通信部４１を通じて、自装置（通信端末Ｔ１）の周囲に発信されているビーコンフレームを受信できたか否かを判断する。制御部４３は、ビーコンフレームを受信できた場合はその旨を復号化部４４に通知する。ここで、ビーコンフレームを通信端末Ｔ１が受信できなかった場合とは、通信端末Ｔ１が図１の通信可能領域１０で表される範囲外の位置に存在することを意味する。制御部４３は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２などにより実現される。
【００６３】
復号化部４４は、制御部４３の通知をもとにユーザが閲覧しようとしているコンテンツデータを記憶部４２から取得し、コンテンツデータが暗号化されているか否かを解析する。
【００６４】
復号化部４４は、制御部４３の通知をもとに受信したビーコンフレームの解析を行い、ビーコンフレーム内に復号化用情報が格納されているか否かを判断する。復号化部４４は、ビーコンフレーム内に復号化用情報が格納されている（つまり特定ビーコンフレームである）場合は、復号化用情報を抽出し、暗号化されたコンテンツデータを復号化し、表示部４５に通知する。一方、格納されていない（つまり通常ビーコンフレームである）場合は、コンテンツデータをそのままに表示部４５に通知する。復号化部４４は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２などにより実現される。
【００６５】
表示部４５は、自装置（通信端末Ｔ１）を使用するユーザが行う操作や自装置の動作状況を表示する。表示部４５は、ユーザが閲覧（利用）したいコンテンツデータをユーザに向けて表示する。
表示部４５は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２、表示装置（図示しない）などにより実現される。
【００６６】
つぎに、図５を参照しながら、本発明の実施の形態にかかる中継装置の動作フローについて順をおって説明する。
【００６７】
図５は、本発明の実施形態における動作を説明するため、一例として、通信端末Ｔ１が中継装置Ａ１を介して管理サーバＳ１に格納されたコンテンツデータを取得する要求の後、中継装置Ａ１が、必要に応じて管理サーバＳ１から受信したコンテンツを暗号化し、通信端末Ｔ１に送信したうえで、さらに暗号化されたコンテンツデータを復号できる情報（データ復号化用情報）を提供するまでの一連のフロー図である。なお、本発明の実施の形態ではコンテンツデータを暗号化するか否かの判断は、管理サーバＳ１が管理しているコンテンツに予め含まれる暗号化するか否かのフラグ情報（暗号化フラグ情報）などを解析することで判断することを前提に説明を行う。
【００６８】
ステップＳ５１にて、制御部３４は、第１通信部３１を通じて、通信端末Ｔ１から管理

サーバＳ１に格納されたコンテンツデータを取得する要求を受信したか否かを判断する。制御部３４は、要求を受けた場合は、ステップＳ５２に遷移する（ステップＳ５１のＹｅｓ）。一方、要求を受けていない場合は、ステップＳ５１を繰り返し待機する（ステップＳ５１のＮｏ）。

【００６９】

ステップＳ５２にて、制御部３４は、第２通信部３６を通じて、通信端末Ｔ１が要求したコンテンツデータを管理サーバＳ１に要求し受信できたか否かを判断する。制御部３４は、コンテンツデータを受信できた場合は、暗号化部３３にその旨を通知し記憶部３２に一時格納する（ステップＳ５２のＹｅｓ）。一方、受信できていない場合は、ステップＳ５２を繰り返し待機する（ステップＳ５２のＮｏ）。

【００７０】

ステップＳ５３にて、暗号化部３３は、制御部３４の通知をもとに記憶部３２に一時格納したコンテンツデータ内の暗号化フラグ情報を解析し、暗号化が必要か否かを判断する。暗号化部３３は、解析の結果、暗号化が必要であれば、ステップＳ５４に遷移する（ステップＳ５３のＹｅｓ）。一方、暗号化が必要でなければ、第１通信部３１に一時格納したコンテンツデータ（非暗号化コンテンツデータ）を通知し、ステップＳ６０に遷移する（ステップＳ５３のＮｏ）。つまり、中継装置Ａ１は、暗号化が必要でなければ、管理サーバＳ１に格納されたコンテンツデータを取得し、通信端末Ｔ１に送信する、従来の中継装置と同様の処理（アクセスポイントとしての処理）を行う。

【００７１】

ステップＳ５４にて、暗号化部３３は、記憶部３２に一時格納したコンテンツデータを暗号化し、その旨を復号化用情報生成部３５に通知する。そして、暗号化部３３は、暗号化したコンテンツデータを第１通信部３１に渡す。

【００７２】

ステップＳ５５にて、復号化用情報生成部３５は、暗号化部３３の通知をもとに、定期的に発信しているビーコンフレームに、暗号化したコンテンツデータを復号できる情報（データ復号化用情報）を格納して、コンテンツの復号化用情報を含む特定ビーコンフレームを生成し記憶部３２に格納する。

【００７３】

ステップＳ５６にて、第１通信部３１は、暗号化したコンテンツデータを通信端末Ｔ１に向けて送信し、送信した旨を制御部３４に通知する。

【００７４】

ステップＳ５７にて、制御部３４は、ステップＳ５６の通知をもとに、特定ビーコンフレームを送信する機会が到来したか否かを判断する。送信する機会とは、例えば、中継装置Ａ１の存在を周囲の通信端末に周知するために発信する特定ビーコンフレームの発信タイミング（例えば、１００ｍｓ間隔）である。制御部３４は、特定ビーコンフレームを送信する機会が到来した場合は、ステップＳ５８に遷移する（ステップＳ５７のＹｅｓ）。一方、特定ビーコンフレームを送信する機会が到来していない場合は、ステップＳ５７を繰り返し待機する（ステップＳ５７のＮｏ）。

【００７５】

ステップＳ５８にて、制御部３４は、第１通信部３１を通じて、記憶部３２に格納した特定ビーコンフレームを周囲の通信端末に周知するために発信する。

【００７６】

ステップＳ５９にて、制御部３４は、特定ビーコン送信期間が終了したか否かを判断する。制御部３４は、期間が終了した場合は、第１通信部３１から送信するビーコンフレームを特定ビーコンフレームから通常ビーコンフレームに変更し、処理を終了する（ステップＳ５９のＹｅｓ）。一方、期間が終了していない場合は、ステップＳ５７からステップＳ５９を繰り返す（ステップＳ５９のＮｏ）。ここで、特定ビーコン送信期間とは、例えばユーザが中継装置Ａ１の設定ツールなどで設定した特定ビーコンフレームを発信し続ける期間（例えば、３０日間、無期限など）である。

【００７７】
ステップＳ６０にて、第１通信部３１は、暗号化が必要でないコンテンツデータをそのままに（特別な処理を施さない）通信端末Ｔ１に向けて送信し、処理を終了する。
【００７８】
つぎに、図６を参照しながら、本発明の実施の形態にかかる通信端末の動作フローについて順を追って説明する。
【００７９】
図６は、本発明の実施形態における動作を説明するため、一例として、通信端末Ｔ１が中継装置Ａ１を介して管理サーバＳ１に格納されたコンテンツを取得する要求後、中継装置Ａ１が必要に応じて管理サーバから受信したコンテンツを暗号化し、通信端末Ｔ１に送信し、さらに暗号化されたコンテンツを通信端末Ｔ１上で閲覧（利用）できるまでの一連のフロー図である。
【００８０】
ステップＳ６１にて、制御部４３は、ユーザが通信端末Ｔ１に備わる入力装置（図示しない）により、第３通信部４１を通じて、管理サーバＳ１に格納されたコンテンツデータを中継装置Ａ１に要求したか否かを判断する。制御部４３は、要求した場合は、ステップＳ６２に遷移する（ステップＳ６１のＹｅｓ）。一方、要求をしていない場合は、ステップＳ６１を繰り返し待機する（ステップＳ６１のＮｏ）。
【００８１】
ステップＳ６２にて、制御部４３は、第３通信部４１を通じて、中継装置Ａ１から通信端末Ｔ１が要求したコンテンツデータを受信したか否かを判断する。制御部４３は、受信した場合は、ステップＳ６３に遷移する（ステップＳ６２のＹｅｓ）。一方、受信していない場合は、ステップＳ６２を繰り返し待機する（ステップＳ６２のＮｏ）。
【００８２】
ステップＳ６３にて、制御部４３は、ステップＳ６２で受信したコンテンツデータを、暗号化されている／いないに関わらず、そのまま記憶部４２に格納する。
【００８３】
ステップＳ６４にて、制御部４３は、ユーザが通信端末Ｔ１に備わる入力装置（図示しない）から記憶部４２に格納しているコンテンツデータを閲覧（利用）する指示をしたか否かを判断する。制御部４３は、ユーザが閲覧する指示をした場合は、その旨を復号化部４４に通知し、ステップＳ６５に遷移する（ステップＳ６４のＹｅｓ）。一方、ユーザが閲覧する指示をしていない場合は、ステップＳ６４を繰り返し待機する（ステップＳ６４のＮｏ）
【００８４】
ステップＳ６５にて、復号化部４４は、制御部４３の通知（ステップＳ６４のＹｅｓ）をもとに
ユーザが閲覧しようとしているコンテンツデータを記憶部４２から取得し、コンテンツデータが暗号化されているか否かを解析する。復号化部４４は、暗号化されていれている場合はステップＳ６６に遷移する（ステップＳ６５のＹｅｓ）。一方、暗号化されていれていない場合は、ステップＳ６９に遷移する（ステップＳ６５のＮｏ）。
【００８５】
ステップＳ６６にて、制御部４３は、第３通信部を通じて、周囲に発信されているビーコンフレームを受信できたか否かを判断する。制御部４３は、ビーコンフレームを受信できた場合はその旨を復号化部４４に通知し、ステップＳ６７に遷移する（ステップＳ６６のＹｅｓ）。一方、受信できなかった場合はステップＳ６６を繰り返し待機する（ステップＳ６６のＮｏ）。ここで、ビーコンフレームを通信端末Ｔ１が受信できなかった場合とは、通信端末Ｔ１が図１の通信可能領域１０で表される範囲外の位置に存在することを意味する。
【００８６】
ステップＳ６７にて、復号化部４４は、制御部４３の通知をもとに受信したビーコンフ

レームの解析を行い、ビーコンフレーム内に復号化用情報が格納されているか否かを判断する。復号化部４４は、ビーコンフレーム内に復号化用情報が格納されている場合（つまり特定ビーコンフレーム）はステップＳ６８に遷移する（ステップＳ６７のＹｅｓ）。一方、格納されていない場合（つまり通常ビーコンフレーム）はステップＳ６６に戻って、ステップＳ６６からステップＳ６７を繰り返す（ステップＳ６７のＮｏ）。

【００８７】

ステップＳ６８にて、復号化部４４は、特定ビーコンフレーム（ステップＳ６７のＹｅｓ）から復号化用情報を抽出し、暗号化されたコンテンツデータを復号化し、表示部４５に通知する。そして、表示部４５は、コンテンツデータをユーザに向けて表示する。このとき、複合化され、ユーザの閲覧に供された一時ファイルが通信端末に存在することになるが、このファイルは表示が終わるたびに削除するのが望ましい。複合化されたファイルを通信端末に残存させることは、特定ビーコンフレームの到達範囲外でもファイルを閲覧できる利便性を得られるものの、端末の盗難・紛失やファイルの漏洩などの点で好ましくない。

【００８８】

ステップＳ６９にて、復号化部４４は、ステップＳ６５の判断（ステップＳ６５のＮｏ）をもとに、コンテンツデータをそのままに、表示部４５に通知する。そして、表示部４５は、通信端末Ｔ１に備わるアプリケーション（図示しない）により、コンテンツデータをユーザに向けて表示する。このように、ユーザが閲覧しようとしたコンテンツデータは暗号化されていないため、復号化部４４は特別な処理を施さない。

【００８９】

なお、図６では、ステップＳ６６およびステップＳ６７を繰り返し待機することで説明したが、これらステップを所定の回数だけ繰り返すと、処理を終了するようにしてもよい。このようにすれば、暗号化されたコンテンツデータを閲覧したい通信端末のユーザは、中継装置から特定ビーコンフレームを所定の回数以内に受信できなければ、閲覧できなくなるため、セキュリティの向上に寄与する。

【００９０】

図７は、本発明の実施の形態にかかる特定ビーコンフレーム７００の一例である。

【００９１】

図７は、中継装置Ａ１の暗号化部３３で暗号化されたコンテンツデータを復号するために必要となる復号化用情報を含むビーコンフレームである。

【００９２】

図７に示す特定ビーコンフレーム７００は、ＭＡＣヘッダ、データ７１、ＦＣＳ（Frame Check Sequence）などで構成される。ＭＡＣヘッダは、無線通信のために必要となる情報（例えば、送信元アドレス、送信先アドレスなど）が格納されている。ＦＣＳは、エラーチェック用に付加されるデータである。

【００９３】

ここで、特定ビーコンフレーム７００は、ＩＥＥＥ８０２．１１規格に準拠した無線通信で利用されるマネージメントフレームであるビーコンフレーム（従来のビーコンフレーム）のフォーマットに準拠しており、異なる点はベンダーが自由に使用できる領域（例えば、図７におけるデータ７１の一部）に復号化用情報が含まれている点である。

【００９４】

特定ビーコンフレーム７００は、従来のビーコンフレームと構造および機能（マネージメントフレームとして）が変わらない。

【００９５】

特定ビーコンフレーム７００は、データ７１の領域の一部に復号化用情報を格納できる。

【００９６】

また、特定ビーコンフレーム７００のデータ７１には、図７で示すように複数のコンテンツデータ個々に対応した復号化用情報を格納できるようにしてもよい。このようにすれば、管理サーバＳ１から複数の暗号化されたコンテンツデータを取得した通信端末Ｔ１は

、それぞれの暗号化されたコンテンツに対応した復号化用情報を取得できる。よって、通信端末Ｔ１は、１度の特定ビーコンフレームの取得によって、複数の暗号化されたコンテンツを閲覧（利用）可能となる。

【００９７】

（実施の形態１の変形例）

上述のように実施の形態では、管理サーバからコンテンツデータを取得する構成の通信システムを例に説明したが、管理サーバではコンテンツデータを取得するために認証機能などを含んでいた。しかしながら、本発明のポイントである中継装置が、ネットワークを介して中継するコンテンツデータを解析し、中継装置自身に備える暗号化すべきコンテンツデータであるか否かを判断するための判断情報（例えば、画像ファイル、映像ファイルなどであれば暗号化するなど）を備えていればよいので、管理サーバが必須の構成要件ではない。すなわち、複数の通信端末間で無線通信を行い、コンテンツデータを送信する場合にも、本発明の通信制御方法は適用できる。例えば、通信装置Ａ内の画像データを中継装置を介して通信端末Ｂが取得した場合に通信端末Ｂのユーザは、中継装置の特定ビーコンが届く範囲内にいるときのみ取得した画像データを閲覧できるようになる。

【００９８】

また、特定ビーコンフレームを送信させるための特定の条件は、データを暗号化して送信したのちの記憶部に予め設定された所定の期間として説明したが、かかる条件に限る必要はない。例えば、管理サーバもしくは中継装置の管理者からの停止入力、または通信端末のユーザによる停止入力に基づく中継装置への停止信号の受信などでもよい。

【００９９】

（実施の形態２）

本発明の実施の形態２では、通信端末が中継装置と無線接続処理を行うときに、通信端末が記憶部に格納している暗号化されたコンテンツデータを復号するために用いる復号化用情報（データ復号化用情報）を中継装置から取得する場合に、ＩＥＥＥ８０２．１１ａｉ規格の一部機能に準拠した無線通信を用いる形態を説明する。なお、本実施の形態では、前提として、ＩＥＥＥ８０２．１１ａｉ通信規格に準拠した無線通信が可能な中継装置および通信端末で構成される。また、本発明の実施の形態２では、具体的には、ＩＥＥＥ８０２．１１ａｉ通信規格で規定されているＨＬＰ（Ｈｉｇｈｅｒ　Ｌａｙｅｒ　Ｐｒｏｔｏｃｏｌ）機能を利用する。また、ＨＬＰとは、中継装置と通信端末との無線接続時に、上位プロトコルの情報を受け渡し可能とする機能であり、ＨＬＰフレームの特定箇所（例えばＨＬＰ　Ｃｏｎｔａｉｎｅｒ　ｅｌｅｍｅｎｔなど）にはベンダー固有のデータを格納できる。これらの技術は既知であり、詳細な説明を省く。

【０１００】

以下、実施の形態２に関する各図面の説明において、実施の形態１と同じ符号を付された図については、詳細な説明を省略する。

【０１０１】

図８は本発明の実施の形態２にかかる通信システムの全体図である。

【０１０２】

図８に示されるように、通信システム２００は、中継装置Ａ１０と、通信端末Ｔ１０と、通信端末Ｔ１１と、通信端末Ｔ１２と、管理サーバ（通信装置に相当）Ｓ１と、ＬＡＮ１１とを備える。通信システム２００は、通信端末Ｔ１０が管理サーバＳ１に格納されたコンテンツデータを取得するために中継装置Ａ１０を中継し取得する通信システムである。なお、以後、通信端末Ｔ１０、通信端末Ｔ１１、および通信端末Ｔ１２は、総称して通信端末Ｔとも呼ぶ。

【０１０３】

中継装置Ａ１０と管理サーバＳ１とは、ＬＡＮ１１を通じて、通信可能に接続されている。ＬＡＮ１１は、ＩＥＥＥ８０２．１１ａ、ｂ、ｇ、ｎ、ａｃ規格等に適合する無線ＬＡＮ、あるいはＩＥＥＥ８０２．３規格等に適合する有線ＬＡＮである。

【０１０４】

中継装置Ａ１０と通信端末Ｔ１とは、通信リンク１５を通じて、通信可能に接続されている。通信リンク１５は、ＩＥＥＥ８０２．１１ａ、ｂ、ｇ、ｎ、ａｃ規格等に適合する無線ＬＡＮで実現される。

【０１０５】

中継装置Ａ１０は、無線通信可能な通信端末Ｔと無線通信するアクセスポイントである。例えば、中継装置Ａ１０は、通信端末ＴからＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）パケットを受信した場合に、当該ＩＰパケットに含まれる宛先アドレスを取得し、受信したＩＰパケットを当該宛先アドレスへＬＡＮ１１を介して転送する。

【０１０６】

また、中継装置Ａ１０は、実施の形態１で説明した機能に加え、ＩＥＥＥ８０２．１１ａｉ通信規格に準拠した無線通信も可能である。

【０１０７】

通信端末Ｔ（Ｔ１０、Ｔ１１，およびＴ１２）は、実施の形態１で説明した機能に加え、ＩＥＥＥ８０２．１１ａｉ通信規格に準拠した無線通信も可能である。

【０１０８】

図９は、本発明の実施の形態２にかかる中継装置Ａ１０の機能ブロック図である。

【０１０９】

図９に示す中継装置Ａ１０は、第１通信部３１、記憶部３２、暗号化部３３、制御部３０１、復号化用情報生成部３０２、第２通信部３６などを備えている。なお、実施の形態１で説明した中継装置Ａ１と同符号の機能および構成については詳細な説明を省く。

【０１１０】

制御部３０１は、実施の形態１の制御部３４の機能に加え、第１通信部３１を介して通信端末１０から受信したＰｒｏｂｅＲｅｑｕｅｓｔから公開鍵を取得し、復号化用情報生成部３０２に当該公開鍵を通知する。

【０１１１】

また、制御部３０１は、復号化用情報生成部３０２により通知された、暗号化済みのデータ復号化用情報をＰｒｏｂｅＲｅｓｐｏｎｓｅに格納する。具体的には、ＰｒｏｂｅＲｅｓｐｏｎｓｅに組み込む（挿入する）ＨＬＰの特定箇所に暗号化済みのデータ復号化用情報を格納する。

【０１１２】

復号化用情報生成部３０２は、実施の形態１の復号化用情報生成部３５の機能に加え、元々暗号化部３３により暗号化された、通信端末Ｔ１０のコンテンツデータを復号化できる情報（データ復号化用情報）を暗号化する。この暗号化は公開鍵を用いて行う。ここで、公開鍵を用いてデータ復号化用情報を暗号化する目的は、無線接続処理において、第三者によりデータ復号化用情報を奪取されることを防ぐためである。また、復号化用情報生成部３０２は、暗号化済みのデータ復号化用情報を制御部３０１に通知する。

【０１１３】

図１０は、本発明の実施の形態にかかる通信端末Ｔの機能ブロック図である。

【０１１４】

図１０に示す通信端末Ｔは、第３通信部４１、記憶部４２、制御部４０１、鍵生成部４０２、復号化部４０３、表示部４５などを備えている。なお、実施の形態１で説明した通信端末Ｔ１と同符号の機能および構成については詳細な説明を省く。

【０１１５】

制御部４０１は、実施の形態１の制御部４３の機能に加え、ユーザから表示部４５を介して、記憶部４２に格納された暗号化済みコンテンツデータを閲覧するための要求（閲覧要求とも呼ぶ）の通知を受けると、鍵生成部４０２に閲覧要求があった旨を通知する。

【０１１６】

また、制御部４０１は、鍵生成部４０２から取得した公開鍵を、中継装置Ａ１０との無線接続処理を開始するために送信するＰｒｏｂｅＲｅｑｕｅｓｔに格納する。具体的には、当該公開鍵をＰｒｏｂｅＲｅｑｕｅｓｔに組み込む（挿入する）ＨＬＰの特定箇所に当

該公開鍵を格納する。

【０１１７】

鍵生成部４０２は、制御部４０１の通知をもとに、中継装置Ａ１０との間で無線通信を行うための無線接続処理に必要となる秘密鍵および公開鍵を生成する。そして、鍵生成部４０２は、制御部４０１に公開鍵を通知し、復号化部４０３に秘密鍵を通知する。なお、秘密鍵および公開鍵の生成については、既知の技術であり、詳細説明は省く。

【０１１８】

復号化部４０３は、実施の形態１の復号化部４４の機能に加え、第３通信部４１を介して、中継装置Ａ１０が送信したＰｒｏｂｅＲｅｓｐｏｎｓｅから暗号化されたデータ復号化用情報を抽出する。具体的には、ＰｒｏｂｅＲｅｓｐｏｎｓｅに組み込まれた（挿入された）ＨＬＰの特定箇所から暗号化されたデータ復号化用情報を抽出する。

【０１１９】

また、復号化部４０３は、鍵生成部４０２より通知を受けた秘密鍵を用いて、暗号化されたデータ復号化用情報を復号し、当該データ復号化用情報を用いて、暗号化されたコンテンツデータを復号し、表示部４５に通知する。

【０１２０】

つぎに、図１１を参照しながら、本発明の実施の形態２にかかる中継装置と通信端末との間で行われる一連の通信処理について順をおって説明する。

【０１２１】

図１１は、本発明の実施形態２における動作を説明するため、一例として、通信端末Ｔ１０が中継装置Ａ１０を介して管理サーバＳ１に格納されたコンテンツデータを取得する要求の後、中継装置Ａ１０が必要に応じて管理サーバＳ１から受信したコンテンツデータを暗号化し、通信端末Ｔ１０に送信、その後、通信端末Ｔ１０が、当該コンテンツデータを記憶部４２に格納している前提とする。図１１は、ユーザの指示により、通信端末Ｔ１０が暗号化されたコンテンツデータを表示するために復号化情報を中継装置Ａ１０から取得し、暗号化されたコンテンツデータを表示するまでの一連のデータ処理の図である。

【０１２２】

なお、通信端末Ｔ１０が、管理サーバＳ１に格納されたコンテンツデータを取得し、暗号化されたコンテンツデータを記憶部４２に格納するまでの処理については、実施の形態１における動作で記載しているため、説明を省く。

【０１２３】

ステップＳ８０１にて、ユーザは、通信端末Ｔ１０の表示部４５を介して、制御部４０１に暗号化されたコンテンツデータを閲覧するための閲覧要求を通知する。そして、制御部４０１は、鍵生成部４０２に閲覧要求があった旨を通知する。

【０１２４】

ステップＳ８０２にて、通信端末Ｔ１０の鍵生成部４０２は、制御部４０１の通知（ステップＳ８０１）をもとに、無線通信における無線接続処理に必要となる秘密鍵および公開鍵を生成する。そして、鍵生成部４０２は、制御部４０１に公開鍵を通知し、復号化部４０３に秘密鍵を通知する。

【０１２５】

ステップＳ８０３にて、通信端末Ｔ１０の制御部４０１は、鍵生成部４０２から取得した公開鍵を、中継装置Ａ１０との無線接続処理を開始するためのＰｒｏｂｅＲｅｑｕｅｓｔに格納する。

【０１２６】

ステップＳ８０４にて、通信端末Ｔ１０の制御部４０１は、第３通信部４１を介して、無線接続処理のためにＰｒｏｂｅＲｅｑｕｅｓｔを中継装置Ａ１０にユニキャスト送信する。

【０１２７】

ステップＳ８０５にて、中継装置Ａ１０の制御部３０１は、ステップＳ８０４の処理により、第１通信部３１を介して受信したＰｒｏｂｅＲｅｑｕｅｓｔから、公開鍵を取得す

る。そして、制御部３０１は、復号化用情報生成部３０２に当該公開鍵を通知する。また、復号化用情報生成部３０２は、暗号化部３３により暗号化されたコンテンツデータを復号化できる情報を、当該公開鍵を用いて、データ復号化用情報を暗号化する。

【０１２８】

ステップＳ８０６にて、制御部３０１は、復号化用情報生成部３０２により通知された、暗号化済みのデータ復号化用情報をＰｒｏｂｅＲｅｓｐｏｎｓｅに格納する。

【０１２９】

ステップＳ８０７にて、制御部３０１は、第１通信部３１を介して、ＰｒｏｂｅＲｅｑｕｅｓｔに対する応答として、暗号化済みのデータ復号化用情報が格納されたＰｒｏｂｅＲｅｓｐｏｎｓｅを通信端末Ｔ１０にユニキャスト送信する。

【０１３０】

ステップＳ８０８にて、通信端末Ｔ１０の復号化部４０３は、第３通信部４１を介して、ステップＳ８０７において送信されたＰｒｏｂｅＲｅｓｐｏｎｓｅから暗号化済みのデータ復号化用情報を抽出する。具体的には、ＩＥＥＥ８０２．１１ａｉ通信規格におけるＨＬＰから抽出する。そして、復号化部４０３は、鍵生成部４０２より通知を受けた秘密鍵（ステップＳ８０２）を用いて、暗号化されたデータ復号化用情報を復号する。その後、復号化部４０３は、データ復号化用情報を用いて、暗号化されたコンテンツデータを復号し、表示部４５に通知する。

【０１３１】

ステップＳ８０９にて、表示部４５は、復号化部４０３の通知を受けて、復号されたコンテンツデータをユーザに向けて表示する。

【０１３２】

以上のように、本発明の実施の形態２にかかる通信システムは、中継装置と通信端末との無線接続処理において、暗号化されたコンテンツデータを閲覧するために必要となるデータ復号化用情報を通信端末が取得できる。ここで、例えば、中継装置と接続する通信端末が多数存在する場合には、実施の形態１におけるビーコン（特定ビーコン）にデータ復号化用情報を通信端末ごとに格納すると、ビーコン長が長くなり得ることが懸念される。また、実施の形態１では、一定間隔でビーコンが中継装置から周囲に送信されるため、セキュリティ面でリスクがないとは言えない。一方、実施の形態２にかかる通信システムは、無線接続処理（ＩＥＥＥ８０２．１１ａｉ通信規格に一部準拠した通信）において、ＨＬＰに格納したデータ復号化用情報をユニキャストにより送信できるため、セキュリティの向上が見込める。

【０１３３】

（まとめ）

上述のように、本発明の実施の形態１にかかる通信システムは、通信端末のユーザが取得したい管理サーバに格納されたコンテンツデータをネットワーク上で中継する中継装置内で暗号化し、暗号化したコンテンツデータを復号するために用いる復号化用情報を作成し、ビーコンフレーム（特定ビーコンフレーム）に格納して、通信端末に提供する。

【０１３４】

このようにすれば、本発明の実施の形態１にかかる通信端末において、暗号化されたコンテンツデータを閲覧（利用）する場合には、中継装置と通信端末との間で無線通信のための無線接続が確立していなくても、中継装置から周囲に向けて発信される特定ビーコンフレームを通信端末が受信さえできればよい。このように、通信端末は、復号化用情報を特定ビーコンフレームから取得できることで、中継装置との間で不必要な無線通信により周囲の無線環境を悪化させることを抑制できる。

【０１３５】

また、暗号化されたコンテンツデータは、通信端末の記憶部に記憶されているため、従来技術である中継装置と通信端末との間で無線通信ができなくなるとコンテンツそのものを削除してしまうために、管理サーバから削除されたコンテンツデータを再取得する必要があった。しかしながら、本発明の実施の形態１にかかる通信システムでは、通信端末に

保存されるコンテンツデータは暗号化されたコンテンツデータ（つまり、復号化用情報がなければ閲覧できない状態のデータ）、あるいは、暗号化する必要のない（閲覧の制限を施す必要がない）コンテンツデータのみである。よって、コンテンツデータの管理者はコンテンツデータの保護ができ、ユーザは通信端末内のコンテンツデータを中継装置の電波受信可能範囲から一旦遠ざかってもコンテンツデータが削除されることがない。

【０１３６】

さらに、本発明の実施の形態１にかかる通信システムは、所定の条件（例えば、特定ビーコンフレームの発信に期限を設定できるなど）を設けることで、管理サーバＳ１から取得したコンテンツデータを通信端末で閲覧（利用）する場合には、閲覧（利用）期限を設定できることなる。つまり、特定ビーコンフレームは所定の条件下でしか中継装置から発信されず、通信端末は復号化用情報をビーコンフレームから取得できないため、自装置（通信端末）に記憶しているコンテンツデータを中継装置あるいは管理サーバの管理者から意図的に閲覧（利用）制限を加えられることになる。よって、本発明の実施の形態にかかる通信システムは、セキュリティの向上にも寄与する。

【０１３７】

また、本発明の実施の形態２にかかる通信システムは、ユニキャスト通信を行い、無線接続処理が短時間で完了するＩＥＥＥ８０２．１１ａｉ通信規格に一部準拠した通信と同時に、中継装置から通信端末にデータ復号化用情報を送信できるため、無線通信におけるセキュリティを担保しつつ、暗号化されたコンテンツデータを復号することができ、ユーザの利便性がさらに向上する。

【産業上の利用可能性】

【０１３８】

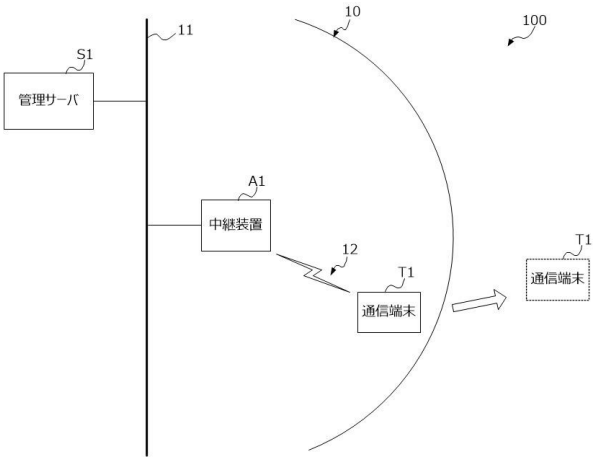
通信システムにおいて、提供されるコンテンツデータのうち、ユーザが取得したコンテンツデータを特定エリアでのみ閲覧できるようにしたいときに有用である。

【符号の説明】

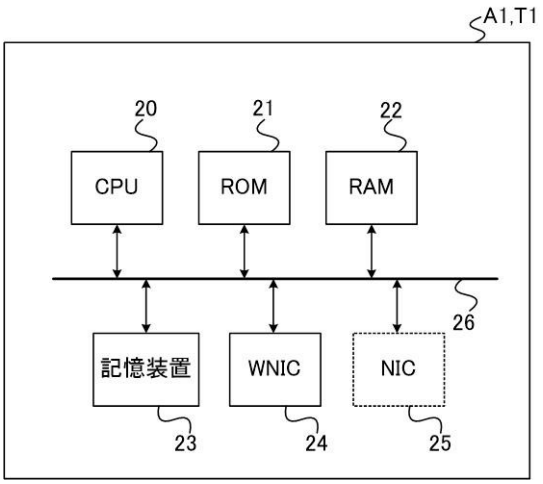
【０１３９】

Ａ１、Ａ１０　中継装置（無線アクセスポイント）
Ｓ１　管理サーバ
Ｔ１、Ｔ１０、Ｔ１１、Ｔ１２　通信端末
１００　通信システム
１０　無線通信可能領域
１１　ＬＡＮ
１２、１５　通信リンク
２０　ＣＰＵ
２１　ＲＯＭ
２２　ＲＡＭ
２３　記憶装置
２４　ＷＮＩＣ
２５　ＮＩＣ
２６　内部バス
３１　第１通信部
３２、４２　記憶部
３３　暗号化部
３４、４３、３０１、４０１　制御部
３５、３０２　復号化用情報生成部
３６　第２通信部
４１　第３通信部
４４、４０３　復号化部
４５　表示部
４０２　鍵生成部

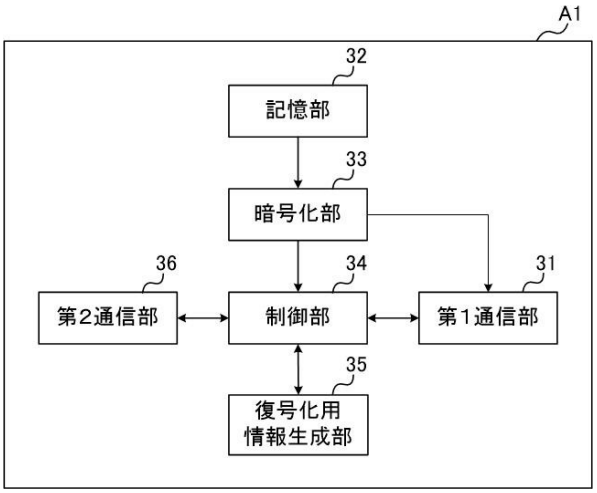
７００　特定ビーコンフレーム
７１　データ部
【図面】
【図１】



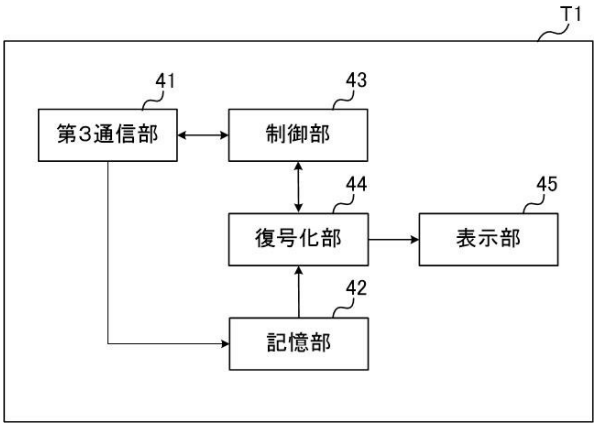

【図２】



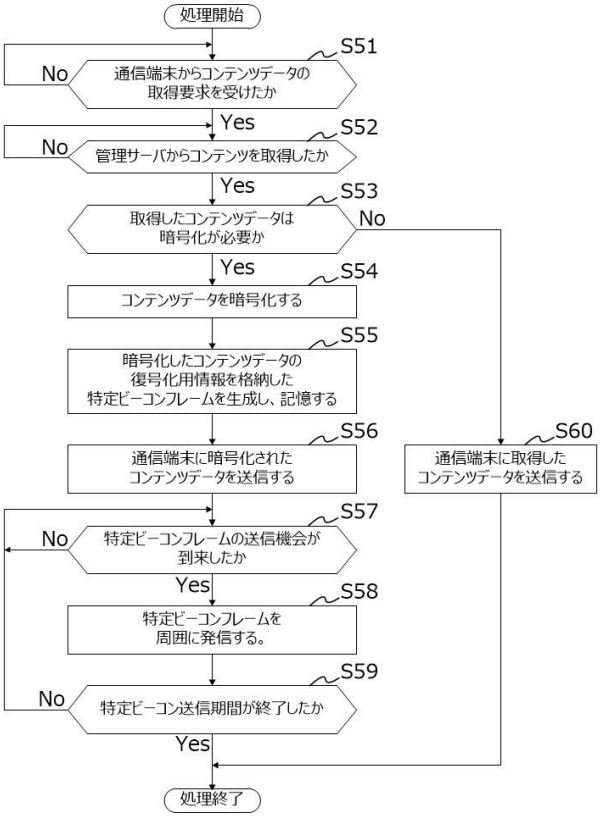

【図３】



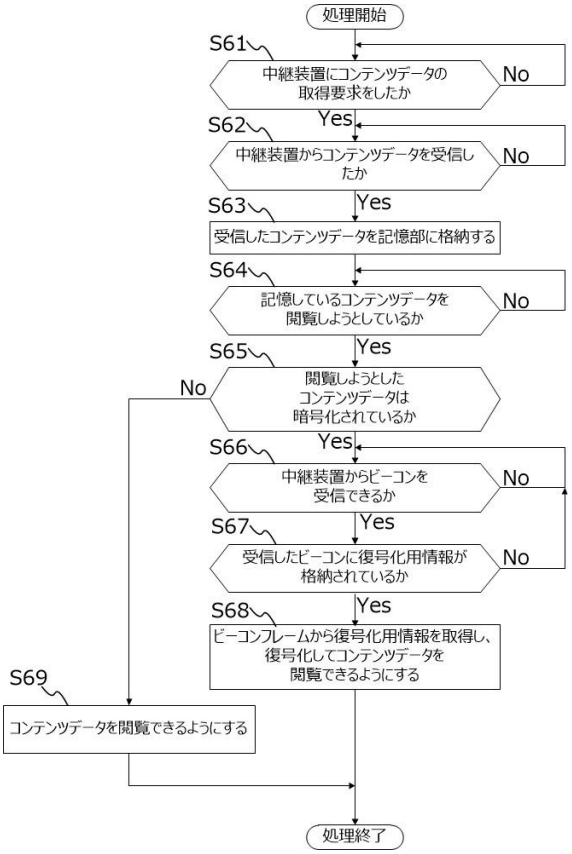

【図４】



【図５】


処理開始
S51
No
通信端末からコンテンツデータの
取得要求を受けたか
Yes
S52
No
管理サーバからコンテンツを取得したか
Yes
S53
取得したコンテンツデータは
暗号化が必要か
No
Yes
S54
コンテンツデータを暗号化する
S55
暗号化したコンテンツデータの
復号化用情報を格納した
特定ビーコンフレームを生成し、記憶する
S56
通信端末に暗号化された
コンテンツデータを送信する
S60
通信端末に取得した
コンテンツデータを送信する
S57
No
特定ビーコンフレームの送信機会が
到来したか
Yes
S58
特定ビーコンフレームを
周囲に発信する。
S59
No
特定ビーコン送信期間が終了したか
Yes
処理終了

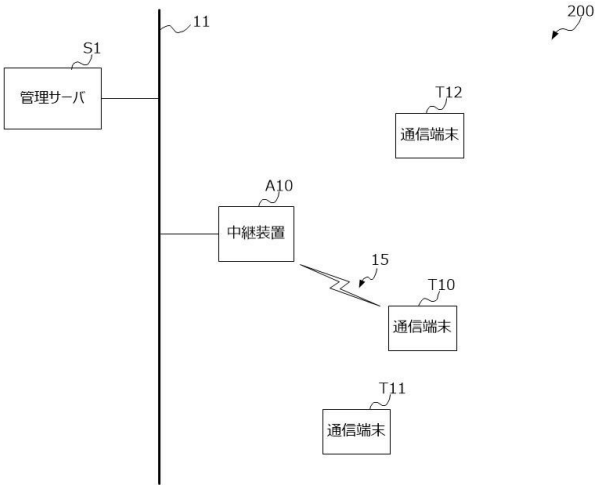
【図６】


処理開始
S61
中継装置にコンテンツデータの
取得要求をしたか
No
Yes
S62
中継装置からコンテンツデータを受信し
たか
No
Yes
S63
受信したコンテンツデータを記憶部に格納する
S64
記憶しているコンテンツデータを
閲覧しようとしているか
No
Yes
S65
No
閲覧しようとした
コンテンツデータは
暗号化されているか
Yes
S66
中継装置からビーコンを
受信できるか
No
Yes
S67
受信したビーコンに復号化用情報が
格納されているか
No
Yes
S68
ビーコンフレームから復号化用情報を取得し、
復号化してコンテンツデータを
閲覧できるようにする
S69
コンテンツデータを閲覧できるようにする
処理終了

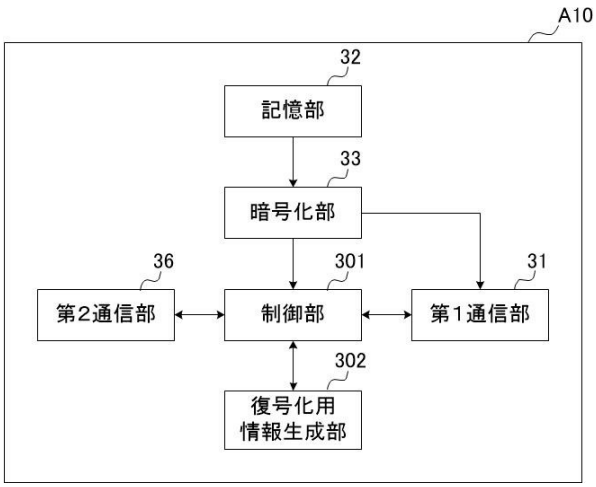
【図７】


700
71
MACヘッダ
…
コンテンツA
復号化用
情報
コンテンツB
復号化用
情報
…
コンテンツF
復号化用
情報
…
FCS

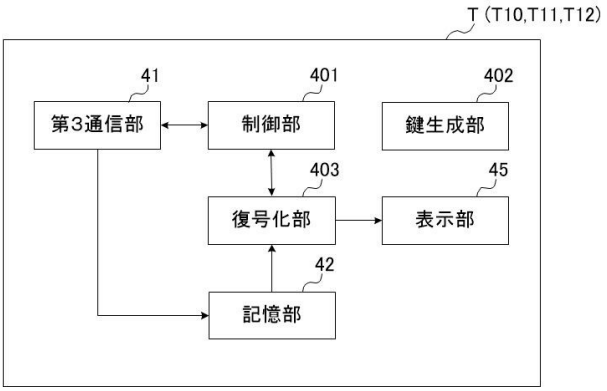
【図８】


200
11
S1
管理サーバ
T12
通信端末
A10
中継装置
15
T10
通信端末
T11
通信端末

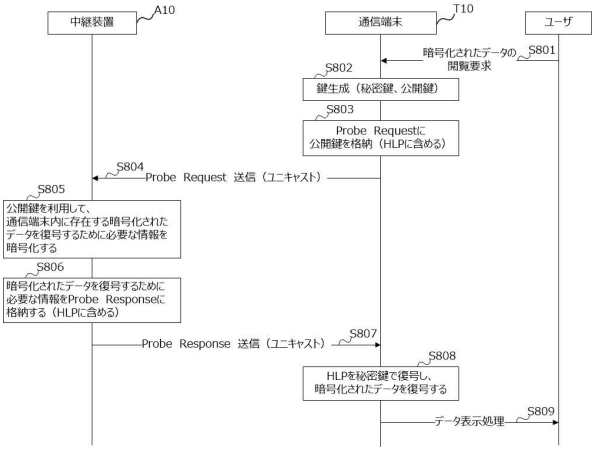
【図９】


A10
32
記憶部
33
暗号化部
36
301
31
第2通信部
制御部
第1通信部
302
復号化用
情報生成部

【図１０】


T (T10,T11,T12)
41
401
402
第3通信部
制御部
鍵生成部
403
45
復号化部
表示部
42
記憶部

【図１１】


中継装置
A10
通信端末
T10
ユーザ
暗号化されたデータの開錠要求
S801
S802
鍵生成（秘密鍵、公開鍵）
S803
Probe Requestに公開鍵を格納（HLPに含める）
S804
Probe Request 送信（ユニキャスト）
S805
公開鍵を利用して、通信端末内に存在する暗号化されたデータを復号するために必要な情報を暗号化する
S806
暗号化されたデータを復号するために必要な情報をProbe Responseに格納する（HLPに含める）
S807
Probe Response 送信（ユニキャスト）
S808
HLPを秘密鍵で復号し、暗号化されたデータを復号する
S809
データ表示処理

フロントページの続き

(51)国際特許分類　　ＦＩ
*Ｈ０４Ｗ　84/10　(2009.01)*　　Ｈ０４Ｗ　84/10　１１０

(56)参考文献　特開２０１５－０３２９５４（ＪＰ，Ａ）
特開２００７－２４１９０７（ＪＰ，Ａ）
特開２００３－２５８７９０（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／００－８８
Ｈ０４Ｗ　４／００－９９／００