(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2010-34651
(P2010-34651A)
(43)公開日　平成22年2月12日(2010.2.12)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 12/08	(2009.01)	H04Q	7/00	184	5B089
G06F 13/00	(2006.01)	G06F	13/00	351Z	5B276
H04W 84/18	(2009.01)	H04Q	7/00	633	5B285
H04W 4/04	(2009.01)	H04Q	7/00	107	5K067
G06F 21/20	(2006.01)	G06F	15/00	330A	

審査請求 未請求　請求項の数 10　ＯＬ　（全 25 頁）　最終頁に続く

(21)出願番号　特願2008-192063 (P2008-192063)
(22)出願日　平成20年7月25日 (2008.7.25)

(71)出願人　591132335
株式会社ザナヴィ・インフォマティクス
神奈川県座間市広野台二丁目６番３５号
(74)代理人　110000198
特許業務法人湘洋内外特許事務所
(72)発明者　青島　弘和
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内
(72)発明者　荒井　正人
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内

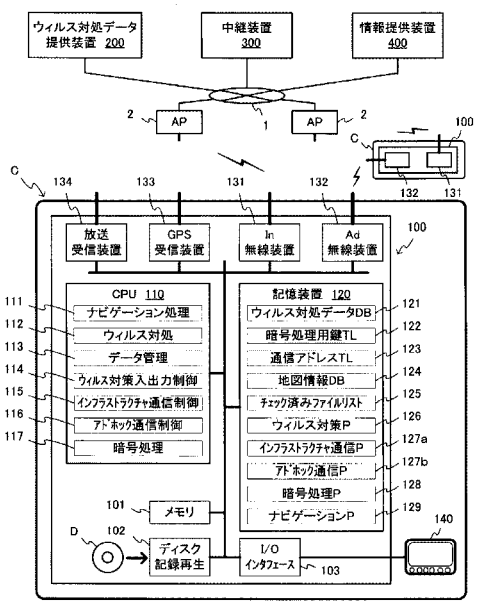
Ｆターム(参考)　5B089 GA11 KA17
5B276 FD08 FD09

最終頁に続く

(54)【発明の名称】情報端末、そのコンピュータウィルス対策プログラム、ナビゲーション装置

(57)【要約】　（修正有）
【課題】コンピュータウィルスに対するセキュリティーを高める。
【解決手段】ナビゲーション装置１００は、ウィルス対処データ提供装置２００から受信したウィルス対処データを格納するウィルス対処データ・データベース１２１と、このウィルス対処データを用いてウィルス対処するウィルス対処部１１２と、データベース１２１に格納されているウィルス対処データが対処十分条件を満たすか否かを判断するデータ管理部１１３と、対処十分条件を満たさない場合に、ウィルス対処が十分な中継装置３００を介して情報提供装置４００との間の通信を実行させるウィルス対策入出力制御部１１４と、を備えている。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
情報提供装置から情報を受け付ける情報端末において、
前記情報提供装置の通信アドレス及びコンピュータウィルス対処処理を実行する中継装置の通信アドレスを記憶する通信アドレス記憶手段と、
前記情報提供装置からの情報を受信する通信手段と、
コンピュータウィルス対処データを受け付ける対処データ受付手段と、
前記対処データ受付手段が受け付けた前記コンピュータウィルス対処データが記憶される対処データ記憶手段と、
前記記憶手段に記憶されている前記コンピュータウィルス対処データを用いて、コンピュータウィルス対処処理を実行するウィルス対処処理手段と、
前記記憶手段に記憶されている前記コンピュータウィルス対処データが予め定められた対処十分条件を満たすか否かを判断するデータ管理手段と、
前記データ管理手段により、前記対処十分条件を満たさないと判断されると、前記通信アドレス記憶手段に記憶されている前記情報提供装置の通信アドレスおよび前記中継装置の通信アドレスを用いて、前記通信手段に、該中継装置を経由した該情報提供装置との間の通信を実行させる情報入出力制御手段と、
を備え、
前記データ管理手段は、前記対処十分条件を満たさないと判断すると、前記通信手段が受信したデータの送信元が前記中継装置でないときには、該データを破棄する
ことを特徴とする情報端末。
【請求項２】
請求項１に記載の情報端末において、
記憶媒体が装着され、該記憶媒体に対してデータの書込み及び読出しを行う記録再生装置を備え、
前記データ管理手段は、前記対処十分条件を満たさないと判断すると、前記記録再生装置に装着された前記記憶媒体からのデータの読出しを制限する、
ことを特徴とする情報端末。
【請求項３】
請求項２に記載の情報端末において、
前記記憶媒体中のデータの特徴値が記憶される特徴値記憶手段を備え、
前記データ管理手段は、前記記録再生装置に記憶媒体が装着されており、該記憶媒体からデータを読出す際に、前記対処十分条件を満たしていると判断すると、該憶媒体中のデータの特徴値を抽出し、該特徴値を前記特徴値記憶手段に記憶し、
前記データ管理手段は、前記記録再生装置に記憶媒体が装着されており、該記憶媒体からデータを読出す際に、前記対処十分条件を満たしていないと判断すると、該記憶媒体中のデータに、前記特徴記憶手段に記憶されている特徴値を持つものが存在するか否かを判断し、該特徴値を持つデータが存在する場合には、該記憶媒体からデータを読み出して、該データに対する以降の処理を実行し、該特徴値を持つデータが存在しない場合には、該データに対する以降の処理を制限する、
ことを特徴とする情報端末。
【請求項４】
請求項１から３のいずれか一項に記載の情報端末において、
データ入出力手段を備え、
前記対処データ受付手段は、前記コンピュータウィルス対処データと共に、該対処データの生成時刻を示す生成タイムスタンプを受け付け、該対処データと共に該生成タイムスタンプを前記対処データ記憶手段に記憶し、
前記データ管理手段は、他の情報端末から前記データ入出力手段が生成タイムスタンプを受け付けると、前記対処データ記憶手段に記憶されている前記タイムスタンプのうちで最新のタイムスタンプと比較し、該他の情報端末からの該生成タイムスタンプが該対処デ

ータ記憶手段に記憶されている該最新のタイムスタンプより古い場合には、該対処データ記憶手段に記憶されている対処データのうち、該他の情報端末の生成タイムスタンプよりも新しいタイムスタンプの対処データを前記データ入出力手段に出力させ、該他の情報端末からの該生成タイムスタンプが該対処データ記憶手段に記憶されている該最新のタイムスタンプより新しい場合には、該最新のタイムスタンプを該データ入出力手段に出力させる、

ことを特徴とする情報端末。

【請求項５】

請求項４に記載の情報端末において、

前記データ入出力手段は、前記他の情報端末との間でアドホック通信を行うアドホック通信手段である、

ことを特徴とする情報端末。

【請求項６】

請求項４に記載の情報端末において、

前記データ入出力手段は、記憶媒体に対する記録再生手段である、

ことを特徴する情報端末。

【請求項７】

請求項１から６のいずれか一項に記載の情報端末と、

前記中継装置と、

を備えていることを特徴とするシステム。

【請求項８】

通信ネットワークに接続されている情報提供装置から情報を取得するナビゲーション装置において、

前記通信ネットワークに対する中継処理を行う無線通信アクセスポイント装置との間で無線通信を行う無線通信手段と、

他のナビゲーション装置と無線通信するアドホック無線通信手段と、

コンピュータウィルス対処データ、及び該コンピュータウィルス対処データの生成時刻を示す生成タイムスタンプを受け付ける対処データ受付手段と、

前記対処データ受付手段が受け付けた前記コンピュータウィルス対処データ及び前記生成タイムスタンプが記憶される対処データ記憶手段と、

前記対処データ記憶手段に記憶されている前記コンピュータウィルス対処データを用いて、外部から受け付けたデータに対してコンピュータウィルス対処処理を実行するウィルス対処処理手段と、

前記アドホック無線通信手段が前記他のナビゲーション装置から生成タイムスタンプを受信すると、前記対処データ記憶手段に記憶されている前記タイムスタンプのうちで最新のタイムスタンプと比較し、該他のナビゲーション装置からの該生成タイムスタンプが該対処データ記憶手段に記憶されている該最新のタイムスタンプより古い場合には、該対処データ記憶手段に記憶されている対処データのうち、該他のナビゲーション装置の生成タイムスタンプよりも新しいタイムスタンプの対処データを前記アドホック無線通信手段により該他のナビゲーション装置へ送信させ、該他のナビゲーション装置からの該生成タイムスタンプが該対処データ記憶手段に記憶されている該最新のタイムスタンプより新しい場合には、該最新のタイムスタンプを該アドホック無線通信手段により該他のナビゲーション装置へ送信させるデータ管理手段と、

を備えていることを特徴とするナビゲーション装置。

【請求項９】

請求項８に記載のナビゲーション装置において、

前記対処データ受付手段は、前記コンピュータウィルス対処データ及び前記生成タイムスタンプを配信するコンピュータウィルス対処データ提供装置が接続されている通信ネットワークにアクセス可能な前記無線通信手段である、

ことを特徴とするナビゲーション装置。

【請求項１０】
通信手段により外部から受信したデータに対してコンピュータウィルス対処処理を実行するコンピュータのウィルス対策プログラムにおいて、
前記コンピュータのデータ受付手段により、コンピュータウィルス対処データを受け付ける対処データ受付ステップと、
前記対処データ受付ステップで受け付けた前記コンピュータウィルス対処データを前記コンピュータの記憶装置に記憶する対処データ記憶ステップと、
前記記憶装置に記憶されている前記コンピュータウィルス対処データを用いて、外部から受け付けたデータに対してコンピュータウィルス対処処理を実行するウィルス対処ステップと、
前記記憶装置に記憶されている前記コンピュータウィルス対処データが予め定められた対処十分条件を満たすか否かを判断するデータ管理ステップと、
前記データ管理ステップで、前記対処十分条件を満たさないと判断されると、前記コンピュータの前記記憶装置に予め記憶されている前記情報提供装置の通信アドレス、およびコンピュータウィルス対処処理を実行する中継装置の通信アドレスを用いて、前記通信手段に、該中継装置を経由した該情報提供装置との間の通信を実行させる情報入出力制御ステップと、
を前記コンピュータに実行させることを特徴とするウィルス対策プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報端末のコンピュータウィルス対策技術に関する。
【背景技術】
【０００２】
車載情報端末として、カーナビゲーション装置がある。このカーナビゲーション装置は、当初、装置内の地図データと、人工衛星からの位置情報とを用いて、自車位置の表示や、目的地までの経路案内を行うものであった。
【０００３】
しかし、近年、カーナビゲーション装置は、携帯電話などの通信手段により、外部とネットワーク接続され、外部からの情報を取得できるようになってきている。また、ＣＤ、ＤＶＤ、メモリ等の可搬型記憶媒体から情報を取得できるようにもなってきている。
【０００４】
情報端末が外部からのデータを取得する場合、情報端末に悪影響を及ぼす不正なデータ、いわゆるコンピュータウィルスによって、情報端末の保持データが被害を受けることがある。このコンピュータウィルス対策として、情報端末に、コンピュータウィルス毎に存在する特徴パターンを予め記憶しておき、情報端末自身に、このような特徴パターンを持つデータが存在するかを監視させることが主流である。
【０００５】
以上のようなコンピュータウィルス対策を行う場合、特徴パターンのデータやコンピュータウィルス対策プログラムの更新が不可欠である。この更新技術としては、例えば、以下の特許文献１に記載されている技術がある。この技術は、地上波ディジタル放送で流されたコンピュータウィルス対策プログラムを受信し、この新たなプログラムをコンピュータウィルス対策に用いる技術である。
【０００６】
【特許文献１】特開２００５－１５１１９３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながら、上記特許文献１に記載の技術では、車両が地上波ディジタル放送を受信できない領域に存在するときには、コンピュータウィルス対策プログラム等を受信できず

、コンピュータウィルス対策が不十分な状態で外部から情報を取得することで、コンピュータウィルスに汚染される虞があるという問題点がある。

【０００８】

本発明は、このような従来技術の問題点に着目し、コンピュータウィルスに対するセキュリティーをより高めることができる技術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】

【０００９】

本発明は、前記目的を達成するために、以下の処理を実行する。

【００１０】

コンピュータのデータ受付手段により、コンピュータウィルス対処データを受け付け、受け付けた該コンピュータウィルス対処データを該コンピュータの記憶装置に記憶し、この記憶装置に記憶されている前記コンピュータウィルス対処データを用いて、外部から受け付けたデータに対してコンピュータウィルス対処処理を実行する。

【００１１】

さらに、前記記憶装置に記憶されている前記コンピュータウィルス対処データが予め定められた対処十分条件を満たすか否かを判断し、該対処十分条件を満たさないと判断されると、前記記憶装置に予め記憶されている情報提供装置の通信アドレス、およびコンピュータウィルス対処処理を実行する中継装置の通信アドレスを用いて、コンピュータの通信手段に、該中継装置を経由した該情報提供装置との間の通信を実行させる。

【００１２】

以上の発明では、記憶装置に記憶されているコンピュータウィルス対処データが予め定められた対処十分条件を満たさない場合には、コンピュータウィルス対処処理を実行する中継装置を経由して、情報提供装置との間の通信を実行させるので、コンピュータウィルス対策が不十分な状態でも、コンピュータウィルスに汚染される虞を最小限に抑えることでき、コンピュータウィルスに対するセキュリティーをより高めることができる。

【００１３】

また、前記目的を達成するためのカーナビゲーション装置に係る発明は、

通信ネットワークに接続されている情報提供装置から情報を取得するカーナビゲーション装置において、

前記通信ネットワークに対する中継処理を行う無線通信アクセスポイント装置との間で無線通信を行う無線通信手段と、

他のカーナビゲーション装置と無線通信するアドホック無線通信手段と、

コンピュータウィルス対処データ、及び該コンピュータウィルス対処データの生成タイムスタンプを受け付ける対処データ受付手段と、

前記対処データ受付手段が受け付けた前記コンピュータウィルス対処データ及び前記生成タイムスタンプが記憶される対処データ記憶手段と、

前記対処データ記憶手段に記憶されている前記コンピュータウィルス対処データを用いて、外部から受け付けたデータに対してコンピュータウィルス対処処理を実行するウィルス対処処理手段と、

前記アドホック無線通信手段が前記他のカーナビゲーション装置から生成タイムスタンプを受信すると、前記対処データ記憶手段に記憶されている前記タイムスタンプのうちで最新のタイムスタンプと比較し、該他のカーナビゲーション装置からの該生成タイムスタンプが該対処データ記憶手段に記憶されている該最新のタイムスタンプより古い場合には、該対処データ記憶手段に記憶されている対処データのうち、該他のカーナビゲーション装置の生成タイムスタンプよりも新しいタイムスタンプの対処データを前記アドホック無線通信手段により該他のカーナビゲーション装置へ送信させ、該他のカーナビゲーション装置からの該生成タイムスタンプが該対処データ記憶手段に記憶されている該最新のタイムスタンプより新しい場合には、該最新のタイムスタンプを該アドホック無線通信手段により該他のカーナビゲーション装置へ送信させるデータ管理手段と、

を備えていることを特徴とするものである。

【００１４】
以上のカーナビゲーション装置に係る発明では、ウィルス対策データ提供装置から最新のウィルス対策データを取得できない場合でも、アドホック通信により、他のカーナビゲーション装置に対して、自ナビゲーション装置が所持するウィルス対処データのタイムスタンプを送信することで、最新のウィルス対処データを取得するための要求を行うことができる。なお、ここでは、当該発明がカーナビゲーション装置に係るものであるが、他のナビゲーション装置、例えば、歩行者の道案内をするためのナビゲーション装置であってもよい。
【発明の効果】
【００１５】
本発明によれば、コンピュータウィルスに対するセキュリティーをより高めることができる。
【発明を実施するための最良の形態】
【００１６】
以下、本発明に係る情報端末の実施形態について、図面を用いて説明する。
【００１７】
本実施形態の情報端末は、図１に示すように、車両Ｃに搭載されるカーナビゲーション装置１００である。
【００１８】
カーナビゲーション装置１００は、各種演算処理を実行するＣＰＵ１１０と、各種プログラムや各種データ等が格納されているハードディスクドライブ装置等の記憶装置１２０と、ＣＰＵ１１０のワークエリアとなるメモリ１０１と、ＤＶＤ等の可搬型ディスク記憶媒体に対するデータの記録再生を行うディスク記録再生装置１０２と、ディスプレイや入力操作部を備えている入出力装置１４０と、この入出力装置１４０のインタフェースであるＩ/Ｏインタフェース１０３と、無線ＬＡＮによりアクセスポイント２を介して通信ネットワーク１にアクセスするインフラストラクチャ無線装置１３１と、アクセスポイント２を介さずに他の情報端末と無線通信するアドホック通信装置１３２と、ＧＰＳ受信装置１３３と、放送受信装置１３４と、を備えている。以上のように、このナビゲーション装置１００は、ナビゲーション機能を実現するために、ＧＰＳ受信装置１３３等を備えていることを除けば、通常のコンピュータと大差はない。
【００１９】
記憶装置１２０には、コンピュータウィルス対処データが格納されるウィルス対処データ・データベース１２１と、データの暗号化及び復号化のための鍵が格納されている暗号処理用鍵テーブル１２２と、通信先の通信アドレスが格納されている通信アドレステーブル１２３と、地図情報が格納されている地図情報データベース１２４と、コンピュータウィルスのチェック後のデータに関する特徴値が格納されるチェック済みファイルリスト１２５と、が設けられている。さらに、この記憶装置１２０には、コンピュータウィルス対策プログラム１２６、インフラストラクチャ通信制御プログラム１２７ａ、アドホック通信プログラム１２７ｂ、暗号処理プログラム１２６、ナビゲーションプログラム１２９等の各種プログラムが格納されている。
【００２０】
ＣＰＵ１１０は、機能的に、ナビゲーション処理を実行するナビゲーション処理部１１１と、コンピュータウィルスに対処するコンピュータウィルス対処部１１２と、記憶装置１２０に対するデータの入出力を管理するデータ管理部１１３と、インフラストラクチャ無線装置１３１やディスク記録再生装置１０２等の入出力装置に対してウィルス対策を施すウィルス対策入出力制御部１１４と、インフラストラクチャ通信制御部１１５と、アドホック通信制御部１１６と、暗号処理部１１７と、を有している。これらの機能部のうち、ナビゲーション処理部１１１は、記憶装置１２０に格納されているナビゲーションプログラム１２９をＣＰＵ１１０が実行することで機能する。また、コンピュータウィルス対処部１１２、データ管理部１１３、ウィルス対策入出力制御部１１４は、記憶装置１２０

に格納されているウィルス対策プログラム１２６をＣＰＵ１１０が実行することで機能する。インフラストラクチャ通信制御部１１５、アドホック通信制御部１１６、暗号処理部１１７は、それぞれ、記憶装置１２０に格納されているインフラストラクチャ通信プログラム１２７ａ、アドホック通信プログラム１２７ｂ、暗号処理プログラム１２８をＣＰＵ１１０が実行することで機能する。

【００２１】

前述の通信ネットワーク１には、各車両Ｃのカーナビゲーション装置１００等へ、コンピュータウィルス対処データを提供するウィルス対処データ提供装置２００と、カーナビゲーション装置１００等へ、地域情報、店情報、交通情報等の各種情報を提供する情報提供装置４００と、ウィルス対策が施されている中継装置３００とが接続されている。

【００２２】

ウィルス対処データ提供装置２００は、図２に示すように、コンピュータであり、各種演算処理を実行するＣＰＵ２１０と、各種プログラムや各種データ等が格納されているハードディスクドライブ装置等の記憶装置２２０と、ＣＰＵ２１０のワークエリアとなるメモリ２０１と、通信ネットワーク１を介して外部と通信する通信装置２３１とを備えている。

【００２３】

記憶装置２２０には、カーナビゲーション装置１００等に提供する最新のコンピュータウィルス対処データが格納されているウィルス対処データ・データベース２２１と、ウィルス対処データの暗号化のための鍵が格納されている暗号処理用鍵テーブル２２２とが設けられている。さらに、記憶装置２２０には、図示されていないが、記憶装置２２０へのデータ入出力制御用のプログラム、暗号処理プログラム、通信制御プログラム等が格納されている。

【００２４】

ＣＰＵ２１０は、機能的に、記憶装置２２０に対するデータの入出力を管理するデータ管理部２１１と、暗号処理部２１２と、通信制御部２１３と、を有している。データ管理部２１１、暗号処理部２１２、通信制御部２１３は、それぞれ、記憶装置２２０に格納されているデータ入出力制御用のプログラム、暗号処理プログラム、通信制御プログラムをＣＰＵ２１０が実行することで機能する。

【００２５】

中継装置３００は、コンピュータであり、各種演算処理を実行するＣＰＵ３１０と、各種プログラムや各種データ等が格納されているハードディスクドライブ装置等の記憶装置３２０と、ＣＰＵ３１０のワークエリアとなるメモリ３０１と、通信ネットワーク１を介して外部と通信する通信装置３３１とを備えている。

【００２６】

記憶装置３２０には、最新のコンピュータウィルス対処データが格納されているウィルス対処データ・データベース３２１と、カーナビゲーション装置１００等からのメッセージを情報提供装置４００等に中継する際に必要な通信アドレス等が格納される中継用テーブル３２２とが設けられている。さらに、記憶装置３２０には、コンピュータウィルス対策プログラム３２３と、通信プログラム３２４と、記憶装置３２０に対するデータ入出力制御用のプログラム（図示されていない）等が格納されている。

【００２７】

ＣＰＵ３１０は、機能的に、コンピュータウィルスに対処するコンピュータウィルス対処部３１１と、通信制御部３１２と、図示されていないデータ管理部と有している。コンピュータウィルス対処部３１１、通信制御部３１２、データ管理部は、それぞれ、記憶装置３２０に格納されているコンピュータウィルス対策プログラム３２３、通信プログラム３２４、記憶装置３２０に対するデータ入出力制御用のプログラムを、ＣＰＵ３１０が実行することで機能する。

【００２８】

情報提供装置４００は、コンピュータであり、各種演算処理を実行するＣＰＵ４１０と

、各種プログラムや各種データ等が格納されているハードディスクドライブ装置等の記憶装置４２０と、ＣＰＵ４１０のワークエリアとなるメモリ４０１と、通信ネットワーク１を介して外部と通信する通信装置４３１とを備えている。

【００２９】

記憶装置４２０には、カーナビゲーション装置１００等へ提供する地域情報、店情報、交通情報等が格納されている情報データベース４２１が設けられている。記憶装置４２０には、さらに、図示されていない、通信プログラムや記憶装置３２０に対するデータ入出力制御用のプログラム等が格納されている。

【００３０】

ＣＰＵ４１０は、機能的に、記憶装置４２０に対するデータの入出力を管理するデータ管理部４１１と、通信制御部４１２とを有している。データ管理部４１１、通信制御部４１２は、それぞれ、記憶装置４２０に対するデータ入出力用のプログラム、通信プログラムをＣＰＵ４１０が実行することで機能する。

【００３１】

次に、本実施形態の各装置の動作について説明する。

【００３２】

まず、図５に示すフローチャートに従って、情報要求の受付時におけるカーナビゲーション装置１００の動作について説明する。

【００３３】

データ管理部１１３は、情報要求を受け付けると（Ｓ１１１）、ウィルス対処データ・データベース１２１に格納されているデータがコンピュータウィルスに対する対処十分条件を満たしているか否かを判断する（Ｓ１１２）。この情報要求は、例えば、運転者が入出力装置１４０の操作により、ある店の情報を情報提供装置４００に要求する場合や、データ管理部１１３自身がウィルス対処データの予め定められた更新期間（例えば、１週間）を経過したと判断して、ウィルス対処データをウィルス対処データ提供装置２００に要求する場合に発生する。また、ここでの対処十分条件は、ウィルス対処データ・データベース１２１に格納されているデータの更新タイムスタンプが現時点から予め定められた期間（例えば、１週間）未満であることである。

【００３４】

ここで、図３を用いて、記憶装置１２０に設けられているウィルス対処データ・データベース１２１について説明する。

【００３５】

ウィルス対処データ・データベース１２１は、図３に示すように、各種コンピュータウィルス毎の特徴パターンを示す特徴パターンデータが格納される特徴パターンデータ欄１２１ｄと、特徴パターンデータの更新処理を行った日時が格納される更新タイムスタンプ欄１２１ａと、特徴パターンデータの作成日時が格納される作成タイムスタンプ欄１２１ｂと、特徴パターンデータの作成元の電子署名が格納される電子署名欄１２１ｃとがある。

【００３６】

前述のステップＳ１１２において、データ管理部１１３は、ウィルス対処データベース１２１の更新タイムスタンプ欄１２１ａを参照し、最新の更新日時と現日時とを比較し、両者の日時差が予め定められた期間（例えば、１週間）未満であるか否かを判断し、この期間未満である場合には、対処十分条件を満たすとする。

【００３７】

データ管理部１１３は、ステップＳ１１２で対処十分条件を満たすと判断すると、インフラストラクチャ通信制御部１１５に、要求先への情報要求パケットを作成させる（Ｓ１１３）。続いて、インフラストラクチャ通信制御部１１５が通信可能なアクセスポイント２が存在するか否かを判断する（Ｓ１１５）。無線ＬＡＮでは、アクセスポイント２がビーコンを発信している。インフラストラクチャ通信制御部１１５は、インフラストラクチャ無線装置１３１が受信したアクセスポイント２からのビーコンが予め定められた電波強

度以上であるか否かで、このアクセスポイント２と通信可能か否かを判断する。

【００３８】

インフラストラクチャ通信制御部１１５は、通信可能なアクセスポイント２が存在すると判断すると、ステップＳ１１３で作成されたパケット又は後述のステップＳ１１４で作成されたパケットをインフラストラクチャ無線装置１３１に送信させて（Ｓ１１７）、一連の情報要求処理を終了する。一方、インフラストラクチャ通信制御部１１５は、通信可能なアクセスポイント２が存在しないと判断すると、パケット送信準備が完了（パケットの作成が完了）した時点から予め定められた時間以内であるか否かを判断し（Ｓ１１６）、予め定められた時間以内である場合にはステップＳ１１５に戻り、予め定められた期間を超えた場合には、パケット送信をせずに、一連の情報要求処理を終了する。すなわち、本実施形態のカーナビゲーション装置１００を搭載している車両Ｃの現在地に対して、通信可能な位置にアクセスポイント２が存在しない場合には、情報要求を受け付けたとしても、この要求を要求先に送信できない場合がある。なお、情報要求を要求先へ送信できない場合には、入出力装置１４０のディスプレイに、要求パケット送信ができなかった旨を表示することが好ましい。

【００３９】

また、ステップＳ１１２で、データ管理部１１３が対処十分条件を満たさないと判断すると、ウィルス対策入出力制御部１１４にその旨を伝える。ウィルス対策入出力制御部１１４は、通信アドレステーブル１２３を参照して、対処十分条件を満たさないときの宛先アドレスとして、中継装置３００の通信アドレスを取得すると共に、情報要求先を最終的な送信先アドレスとし、宛先アドレス及び最終的な送信先アドレスをインフラストラクチャ通信制御部１１５に渡す。さらに、ウィルス対策入出力制御部１１４は、情報要求のメッセージ番号を定め、これもインフラストラクチャ制御部１１５に渡す。そして、インフラストラクチャ通信制御部１１５は、中継装置３００経由での要求先への情報要求パケットを作成する（Ｓ１１４）。

【００４０】

ここで、中継装置３００経由での要求先への情報要求パケットについて、図１２を用いて説明する。

【００４１】

この情報要求パケット１０は、ヘッダ部１１とペイロード部１５とを有している。ヘッダ部１１は、送信元アドレスが格納される送信元アドレス領域１２と宛先アドレスが格納される宛先アドレス領域１３とを有している。送信元アドレス領域１２には、カーナビゲーション装置１００自身の通信アドレスが格納され、宛先アドレス領域１３には、ウィルス対策入出力制御部１１４が指定した中継装置３００の通信アドレスが格納される。また、ペイロード部１５は、情報要求メッセージが格納されるメッセージ領域１６と、このメッセージのメッセージ番号が格納されるメッセージ番号領域１７と、送信先アドレスが格納される送信先アドレス領域１８とを有している。メッセージ番号領域１７には、ウィルス対策入出力制御部１１４が指定したメッセージ番号が格納される。このメッセージ番号は、メッセージ領域１６に格納される情報要求メッセージを一意に特定する番号である。また、送信先アドレス領域１８には、ウィルス対策入出力制御部１１４が指定した、最終的な送信先、つまり情報要求先の通信アドレスが格納される。

【００４２】

インフラストラクチャ通信制御部１１５は、中継装置３００経由での要求先への情報要求パケットを作成すると（Ｓ１１４）、前述したように、通信可能なアクセスポイント２が存在するか否かを判断し（Ｓ１１５）、通信可能なアクセスポイント２が存在すれば、ステップＳ１１４で作成したパケットをインフラストラクチャ無線装置１３１に送信させて（Ｓ１１７）、一連の情報要求処理を終了する。

【００４３】

以上のように、本実施形態では、通信ネットワーク１経由で情報要求をする際に、コンピュータウィルスに対する対処が不十分な場合には、コンピュータウィルス対処が十分な

中継装置３００経由で、情報要求先と通信するようにして、カーナビゲーション装置１００がコンピュータウィルスに侵される可能性を小さく抑えている。

【００４４】

次に、前述したステップＳ１１３で作成された情報要求パケットが、ウィルス対処データ提供装置２００に対するウィルス対処データの要求パケットであるとし、その場合のウィルス対処データ提供装置２００の動作について説明する。

【００４５】

ウィルス対処データ提供装置２００のウィルス対処データ・データベース２２１には、各種コンピュータウィルス毎の特徴パターンを示す特徴パターンデータとして、過去のものから最新のものまで格納されている。このウィルス対処データ・データベース２２１には、特徴パターンデータの他、該当特徴パターンデータの作成日時が格納される作成タイムスタンプと、該当特徴パターンデータの作成元の電子署名とが組になって格納されている。

【００４６】

ウィルス対処データ提供装置２００の通信制御部２１３が、カーナビゲーション装置１００からウィルス対処データ要求パケットを受信すると、データ管理部２１１に、ウィルス対処データ・データベース２１１から、最新の特徴パターンデータ、この作成タイムスタンプ、この作成元の電子署名の組（以下、特徴パターンデータ、作成タイムスタンプ、電子署名の組を特徴パターンデータ組とする）を抽出する。暗号処理部２１２は、この特徴パターンデータ組を、暗号処理用鍵テーブル２２２に格納されている秘密鍵を用いて暗号化する。通信制御部２１３は、これをパケット化し、ウィルス対処データ要求パケットの送信元のカーナビゲーション装置１００へ送信する。

【００４７】

なお、ウィルス対処データ提供装置２００は、中継装置３００を介して、カーナビゲーション装置１００からのウィルス対処データ要求パケットを受信した場合には、ウィルス対処データである特徴パターンデータの組を暗号化せずに、中継装置３００を介して、このカーナビゲーション装置１００に送信する。これは、後述するように、中継装置３００では、コンピュータウィルスチェックをするため、暗号化されていると、ウィルスチェックを行えないからである。中継装置３００経由での通信で、特徴パターンデータ組を暗号化させない方法としては、ウィルス対処データ提供装置２００に対して、中継装置３００経由での通信では暗号化しない旨を予め定めておくか、要求元のカーナビゲーション装置１００からのデータ要求パケットに、データ提供にあってはデータを暗号化しない旨のメッセージを組み込んでおく方法等がある。

【００４８】

次に、前述したステップＳ１１４で作成された情報要求パケットを受信した中継装置３００の動作について説明する。

【００４９】

中継装置３００の通信制御部３１２が、情報要求元のカーナビゲーション装置１００から情報要求パケットを受信すると、ウィルス対処部３１１が、この情報要求パケット内のデータ中に、ウィルス対処データ・データベース３２１に格納されている特徴パターンデータのうちのいずれかに対応するものがあるか否かをチェックする。いずれかの特徴パターンデータに対応するものがある場合には、この情報要求パケットを破棄する。いずれの特徴パターンデータにも対応するものがなければ、通信制御部３１２が、この情報要求パケットを解析して、解析で得られたデータを中継用テーブル３２２に格納する。

【００５０】

この中継用テーブル３２２は、情報要求に対する応答を情報要求先から受けた際に、この応答を情報要求元のカーナビゲーション装置１００へ送るためのデータを格納するテーブルである。この中継用テーブル３２２は、図４に示すように、受信した情報要求パケットの送信元のアドレスが格納される送信元アドレス領域３２２ａと、この情報要求パケットの最終的な送信先のアドレスが格納される送信先アドレス領域３２２ｂと、この情報要

求パケットに含まれているメッセージ番号が格納されるメッセージ番号領域３２２ｃとを有する。

【００５１】

通信制御部３１２は、受信した情報要求パケット１０（図１２）の送信元アドレス領域１２に格納されている送信元アドレス、送信先アドレス領域１８に格納されている送信先アドレス、メッセージ番号領域１７に格納されているメッセージ番号を、それぞれ、中継用テーブル３２２の送信元アドレス領域３２２ａ、送信先アドレス領域３２２ｂ、メッセージ番号領域３２２ｃに格納する。

【００５２】

次に、通信制御部３１２は、図１２に示すように、情報要求転送パケット１０ａの宛先アドレス領域１３aに、カーナビゲーション装置１００からの情報要求パケット１０の送信先アドレス領域１８に格納されている通信アドレスを格納し、情報要求転送パケット１０ａの送信元アドレス領域１２ａに、カーナビゲーション装置１００からの情報要求パケット１０の宛先アドレス領域１３に格納されている通信アドレス、つまり、中継装置３００の通信アドレスを格納する。さらに、この情報要求転送パケット１０ａのペイロード部１５ａの情報要求メッセージ領域１６、メッセージ番号領域１７に、それぞれ、カーナビゲーション装置１００からの情報要求パケット１０の情報要求メッセージ領域１６に格納されている情報要求メッセージ、メッセージ番号領域１７に格納されているメッセージ番号を格納する。そして、この情報要求転送パケット１０ａを通信ネットワーク１へ送出する。すなわち、情報要求パケット１０に含まれている情報要求メッセージを要求先へ転送する。

【００５３】

ここで、情報要求転送パケット１０ａの宛先アドレス領域１３ａに格納されている通信アドレス、つまり、カーナビゲーション装置１００からの情報要求パケット１０の送信先アドレス領域１８に格納されている通信アドレスが、情報提供装置４００の通信アドレスであるとする。

【００５４】

この場合、情報要求転送パケット１０ａを情報提供装置４００の通信装置４３１が受信する。情報提供装置４００の通信制御部４１２は、この情報要求転送パケット１０ａを解析して、このパケット１０ａに含まれている情報要求メッセージをデータ管理部４１１に渡す。データ管理部４１１は、情報データベース４２１に格納されている各種情報のうちから、この情報要求メッセージが要求している情報を抽出して、通信制御部４３１に渡す。

【００５５】

通信制御部４３１は、データ管理部４１１からの情報を、図１２に示す応答パケット２０の応答メッセージ領域１６ｂに格納する。さらに、この応答パケット２０の送信元アドレス領域１２ｂ、宛先アドレス領域１３ｂ、メッセージ番号領域１７に、それぞれ、中継装置３００からの情報要求転送パケット１０ａの宛先アドレス領域１３ａに格納されている通信アドレス、この情報要求転送パケット１０ａの送信元アドレス領域１２ａに格納されている通信アドレス、この情報要求パケット１０ａのメッセージ番号領域１７に格納されているメッセージ番号を格納する。そして、この応答パケット２０を通信ネットワーク１へ送出する。

【００５６】

中継装置３００の通信制御部３１２は、通信装置３３１を介して、この応答パケット２０を受け取ると、ウィルス対処部３１１が、この応答パケット内のデータ中に、ウィルス対処データ・データベース３２１に格納されている特徴パターンデータのうちのいずれかに対応するものがあるか否かをチェックする。いずれかの特徴パターンデータに対応するものがある場合には、この応答パケットを破棄する。いずれの特徴パターンデータに対応するものがなければ、通信制御部３１２が、この応答パケットに基づき、後述の応答転送パケットを作成する。

【００５７】
通信制御部３１２は、応答転送パケットの作成にあたり、まず、応答パケット２０のメッセージ番号領域１７に格納されているメッセージ番号、この応答パケット２０の送信元アドレス領域１２ｂに格納されている通信アドレスが、それぞれ、中継用テーブル２２２のメッセージ番号領域３２２ｃ、送信先アドレス領域３２２ｂに格納されているレコードが存在するか否かを判断する。該当するレコードが存在する場合には、このレコードの送信元アドレス領域３２２ａに格納されている通信アドレス、つまり、情報要求元のカーナビゲーション装置１００の通信アドレスを取得する。次に、図１２に示すように、応答転送パケット２０ａの宛先アドレス領域１３ｃに、中継用テーブル２２２の送信元アドレス領域３２２ａから取得した情報要求元のカーナビゲーション装置１００の通信アドレスを格納し、応答転送パケット２０ａの送信元アドレス領域１２ｃに、応答パケット２０の宛先アドレス領域１３ｂに格納されている中継装置３００の通信アドレスを格納する。さらに、応答パケット２０のペイロード部１５ｂの応答メッセージ領域１６ｂに格納されている応答メッセージ、メッセージ番号領域１７に格納されているメッセージ番号を、それぞれ、応答転送パケット２０ａのペイロード部１５ｂの応答メッセージ領域１６ｂ、メッセージ番号領域１７に格納する。そして、通信制御部３１２は、この応答転送パケット２０ａを通信ネットワーク１へ送出する。

【００５８】
この応答転送パケット２０ａは、通信ネットワーク1に接続されている複数のアクセスポイント２のうちのいずれかのアクセスポイント２と通信可能な位置に、情報要求元のカーナビゲーション装置１００が存在する場合、このカーナビゲーション装置１００に受信される。

【００５９】
次に、カーナビゲーション装置１００のインフラストラクチャ無線装置１３１が通信ネットワーク１から通信パケットを受信した際の動作について、図６に示すフローチャートに従って説明する。

【００６０】
インフラストラクチャ通信制御部１１５は、インフラストラクチャ無線装置１３１が通信ネットワーク１から通信パケットを受信したか否かを常に監視しており（Ｓ１２１）、インフラストラクチャ無線装置１３１が通信ネットワーク１からデータを受信したことを検知すると、その旨をデータ管理部１１３に通知する。

【００６１】
データ管理部１１３は、この通知を受けると、ウィルス対処データ・データベース１２１に格納されているデータがコンピュータウィルスに対する対処十分条件を満たしているか否かを判断する（Ｓ１２２）。このデータ管理部１１３の判断は、図５におけるステップＳ１１２におけるデータ管理部１１３の判断と同様である。

【００６２】
データ管理部１１３は、対処十分条件を満たしていないと判断すると、受信した通信パケットのヘッダ部の情報から送信元がどこであるかを調べる（Ｓ１２３）。そして、送信元が中継装置３００である場合には、ステップＳ１２７に進み、送信元が中継装置３００を除く装置である場合には、受信した通信パケットを破棄して（Ｓ１５９）、一連の処理を終了する。

【００６３】
また、データ管理部１１３は、ステップＳ１２２で対処十分条件を満たしていると判断した場合も、受信した通信パケットのヘッダ部の情報から送信元がどこであるかを調べる（Ｓ１２４）。データ管理部１１３は、送信元がウィルス対処データ提供装置２００である場合には、暗号処理部１１７に、通信パケット内のデータに復号化処理を施させる（Ｓ１２５）。

【００６４】
ウィルス対処データ提供装置２００からの特徴パターンデータ組は、前述したように、

ウィルス対処データ提供装置２００において、秘密鍵で暗号化されている。そこで、カーナビゲーション装置１００の暗号化処理部１１７は、この秘密鍵に対する公開鍵を暗号処理用鍵テーブル１２２から抽出して、この公開鍵で特徴パターンデータ組を復号化する。

【００６５】

次に、データ管理部１１３は、暗号化処理部１１７による通信パケット内のデータの復号化が成功したか否かを判断する（Ｓ１２６）。復号化に失敗していれば、受信した通信パケットを破棄して（Ｓ１５９）、一連の処理を終了する。

【００６６】

前述したステップＳ１２３で、通信パケットの送信元が中継装置３００であると判断された場合に加え、ステップＳ１２４で、通信パケットの送信元がウィルス対処データ提供装置２００ではないと判断された場合、さらに、ステップＳ１２６で、復号化に成功したと判断された場合には、いずれも、ステップＳ１２７に進む。

【００６７】

ステップＳ１２７では、ウィルス対処部１１２が、通信パケット内のデータ中に、ウィルス対処データ・データベース１２１中の特徴パターンデータに対応するものがあるか否かをチェックする。なお、本実施形態では、前述したように、最新の特徴パターンデータで、コンピュータウィルスチェックを行う中継装置３００から送信されてきた通信パケット内のデータに関しても、ウィルスチェックを行うようにしているが、中継装置３００から送信されてきた通信パケット内のデータに関しては、これを行わず、直ちに、後述のステップＳ１２９に進むようにしてもよい。

【００６８】

ウィルス対処部１１２によるウィルスチェックの結果、この通信パケット内のデータにコンピュータウィルスが在った場合には、この通信パケットは、データ管理部１１３により破棄される（Ｓ１５９）。コンピュータウィルスが見つからなければ、データ管理部１１３が、この通信パケット内のデータに対して、どのような処理をすべきか判断する（Ｓ１２９）。

【００６９】

登録処理が必要であると判断して場合には、このデータ管理部１１３により、記憶装置１２０内の所定領域への登録処理が実行され（Ｓ１６０）、一連の処理を終了する。また、返信処理等の他の処理が必要であると判断した場合、ＣＰＵ１１０の諸機能によりこの他の処理が実行され（Ｓ１５８）、一連の処理を終了する。

【００７０】

以上のように、本実施形態では、通信ネットワーク１から通信パケットを受信した際に、コンピュータウィルスに対する対処が不十分な場合には、コンピュータウィルス対処が十分な中継装置３００経由での通信パケットのみを受信し、他の通信パケットを破棄して、カーナビゲーション装置１００がコンピュータウィルスに侵されるのを防いでいる。

【００７１】

次に、カーナビゲーション装置１００のアドホック無線装置１３２が通信パケットを受信した際、及び通信パケットを送信する際の動作について、図７に示すフローチャートに従って説明する。

【００７２】

アドホック通信制御部１１６は、常に、アドホック通信可能な相手が存在するか否かを監視している（Ｓ１３１）。アドホック通信制御部１１６は、アドホック通信可能な相手が存在する場合、この相手から所定時間内に通信パケットを受信したか否かを判断する（Ｓ１３２）。所定時間内にアドホック通信パケットを受信しなければ、データ管理部１１３が、ウィルス対処データ・データベース１２１の作成タイムスタンプ領域１２１ｂ（図３）に格納されているタイムスタンプのうちから最新のタイムスタンプを取得し（Ｓ１４１）、これを暗号処理部１１７に渡し、暗号化させる（Ｓ１４２）。暗号処理部１１７は、この際、カーナビゲーション装置相互間でウィルス対処データの共有化サービスを受けるカーナビゲーション装置群が共有する対称鍵を暗号処理用鍵テーブル１２２から取得し

、この対称鍵で、前述の最新のタイムスタンプを暗号化する。最新の作成タイムスタンプが暗号化すると、アドホック通信制御部１１６は、これをパケット化し、アドホック通信可能な相手に、これを送信する（Ｓ１４３）。

【００７３】

このように、作成タイムスタンプを暗号化することにより、外部の第三者が、当該カーナビゲーション装置１００で扱われていないウィルス対処データを知る手掛かりを隠蔽することができる。また、あるタイムスタンプが、暗号化のたびに、同じ暗号文にならないように、対称鍵と乱数データとを用いて、タイムスタンプを暗号化するようにしてもよい。

【００７４】

なお、ここでは、送信相手が、カーナビゲーション装置相互間でウィルス対処データの共有化サービスを受けるとしたカーナビゲーション装置群のうちの一のカーナビゲーション装置であるか否かに関わらず、最新のタイムスタンプを送信しているが、これは暗号化されているため、仮に、送信相手が共有化サービスを受けるカーナビゲーション装置でなくても、基本的に問題ない。但し、好ましくは、通信相手の存在を確認した時点で（Ｓ１３１）、この通信相手が共有化サービスを受けるカーナビゲーション装置であるか否かを調べ、このカーナビゲーション装置である場合にのみ、最新のタイムスタンプを送信することが好ましい。

【００７５】

また、ここでは、アドホック通信可能な相手から所定時間内に通信パケットを受信しなければ（ステップＳ１３２でNOの場合）、ステップＳ１４１及びステップＳ１４２の処理を経て、最新の生成タイムスタンプを相手先に送信（Ｓ１４３）するようにしているが、アドホック通信可能な相手から所定時間内に通信パケットを受信しないとき（ステップＳ１３２でNOの場合）、所定の条件を満たしたときのみ、ステップＳ１４１及びステップＳ１４２の処理を経て、最新のタイムスタンプを相手先に送信（Ｓ１４３）するようにしてもよい。この場合、当該カーナビゲーション装置１００を搭載している車両Cの運転手が、入出力装置１４０から最新のタイムスタンプの送信指示をすること、以前に最新のタイムスタンプを送信してから所定期間経過していること、ＣＰＵ１１０の負荷が所定値以下になっていること等、を所定の条件にするとよい。

【００７６】

また、アドホック通信可能な相手が複数存在する場合には、これら相手に、タイムスタンプをブロードキャストで送信するようにしてもよいし、これら相手のうち、所定の基準を満たした相手のみにユニキャストでタイムスタンプを送信するようにしてもよい。

【００７７】

また、以上では、タイムスタンプを暗号化するにあたって、対称鍵を用いているが、同一のタイムスタンプを暗号化のたびに、同じ暗号文にならないように、対称鍵と乱数データとを用いて、タイムスタンプを暗号化するようにしてもよい。

【００７８】

ステップＳ１３２で、アドホック通信制御部１１６が、所定時間以内にアドホック通信可能な相手からアドホック通信パケットを受信したと判断した場合には、データ管理部１１３が、ウィルス対処データ・データベース１２１に格納されているデータがコンピュータウィルスに対する対処十分条件を満たしているか否かを判断する（Ｓ１３３）。このデータ管理部１１３の判断は、図５におけるステップＳ１１２におけるデータ管理部１１３の判断と同様である。

【００７９】

データ管理部１１３は、対処十分条件を満たしていないと判断すると、受信したアドホック通信パケットのヘッダ部の情報から送信元がどこであるかを調べる（Ｓ１４５）。そして、送信元が前述の共有化サービスを受けるカーナビゲーション装置でない場合には、受信した通信パケットを破棄して（Ｓ１４９）、一連の処理を終了する。なお、送信元が共有化サービスを受けるカーナビゲーション装置であるか否かは、アドホック通信パケッ

トのヘッダ部に格納されている送信元アドレスを調べ、この送信元アドレス中に、共有化サービスを受けるカーナビゲーション装置に共通する部分が存在するか否かで判断する。

【００８０】

また、データ管理部１１３は、ステップＳ１３３で対処十分条件を満たしていると判断した場合も、受信した通信パケットのヘッダ部の情報から送信元がどこであるかを調べる（Ｓ１３４）。そして、送信元が共有化サービスを受けるカーナビゲーション装置でない場合には、ステップＳ１３７に進む。また、ステップＳ１４５及びステップＳ１３４で、送信元が共有化サービスを受けるカーナビゲーション装置であると判断した場合には、データ管理部１１３は、暗号処理部１１７に、アドホック通信パケット内のデータに復号化処理を施させる（Ｓ１３５）。

【００８１】

なお、ステップＳ１４５、ステップＳ１３４で送信元がカーナビゲーション装置であるか否かの判定を行っているが、特にこれを行わず、ステップＳ１３６で復号化が成功したと判断した場合には、この復号化に成功した通信パケットの送信元がカーナビゲーション装置であるとみなして処理してもよい。

【００８２】

共有化サービスを受けるカーナビゲーション装置からのアドホック通信パケット内のデータは、共有化サービスを受けるカーナビゲーション装置群が共有する対称鍵により暗号化されている。そこで、ステップＳ１４５及びステップＳ１３４で、送信元が共有化サービスを受けるカーナビゲーション装置であると判断した場合には、ステップＳ１３５において、暗号処理部１１７が、暗号処理用テーブル１２２に格納されている対称鍵を用いて、アドホック通信パケット内のデータを復号化する。

【００８３】

次に、データ管理部１１３は、暗号化処理部１１７によるアドホック通信パケット内のデータの復号化が成功したか否かを判断する（Ｓ１３６）。復号化に失敗していれば、受信したアドホック通信パケットを破棄して（Ｓ１４９）、一連の処理を終了する。この復号化に失敗する原因としては、伝送途中でのデータ改変、伝送途中でのウィルス等による攻撃等が考えられる。また、復号化に成功した場合、及びステップＳ１３４でアドホック通信パケットの送信元が共有サービスを受けるカーナビゲーション装置でないと判断された場合には、ウィルス対処部１１２が、アドホック通信パケット内のデータ中に、ウィルス対処データ・データベース１２１中の特徴パターンデータに対応するものがあるか否かをチェックする（Ｓ１３７）。

【００８４】

ウィルス対処部１１２によるウィルスチェックの結果、アドホック通信パケット内のデータにコンピュータウィルスが在った場合には、このアドホック通信パケットは、データ管理部１１３により破棄される（Ｓ１４９）。コンピュータウィルスが見つからなければ、データ管理部１１３が、このアドホック通信パケット内のデータに対して、どのような処理をすべきか判断する（Ｓ１３９）。

【００８５】

アドホック通信パケット内のデータに作成タイムスタンプが格納されている場合には、後述のタイムタイムスタンプ処理が必要であると判断され、この場合には、タイムスタンプ処理が実行され（Ｓ１５０）、一連の処理を終了する。また、登録処理が必要であると判断された場合には、このデータ管理部１１３により、記憶装置１２０内の所定領域への登録処理が実行され（Ｓ１６０）、一連の処理を終了する。この登録処理で、登録対処がウィルス対処データである場合には、このウィルス対処データがウィルス対処データ・データベース１２１に登録される。さらに、返信処理等の他の処理が必要であると判断された場合、ＣＰＵ１１０の諸機能によりこの他の処理が実行され（Ｓ１４８）、一連の処理を終了する。

【００８６】

次に、図８に示すフローチャートに従って、ステップＳ１５０におけるタイムスタンプ

処理の詳細について説明する。

【００８７】

まず、データ管理部１１３が、ウィルス対処データ・データベース１２１の作成タイムスタンプ領域１２１ｂ（図３）に格納されているタイムスタンプのうちから最新のタイムスタンプを取得する(Ｓ１５１)。次に、データ管理部１１３は、アドホック通信で受信したアドホック通信パケット中に含まれている生成タイムスタンプと、ステップＳ１５１で取得したタイムスタンプとの新旧を比較する（Ｓ１５２）。ステップＳ１５１で取得したタイムスタンプの方が古ければ、図７中のステップＳ１４２に進み、このタイムスタンプが暗号化され、これが通信相手に送信される(Ｓ１４３)。

【００８８】

また、ステップＳ１５１で取得したタイムスタンプと、アドホック通信パケット中に含まれる生成タイムスタンプと、が同じであれば、このタイムスタンプ処理（Ｓ１５０）を終了する。これは、自身が所有している最新の特徴パターンデータ群と同じものを相手方も所有しているからである。

【００８９】

また、ステップＳ１５１で取得したタイムスタンプが、アドホック通信パケット中に含まれる生成タイムスタンプより新しければ、ウィルス対処データ・データベース１２１から、アドホック通信パケット中に含まれている生成タイムスタンプより新しい全ての生成タイムスタンプに対応する特徴パターンデータ群を抽出し、これを暗号処理部１１７に渡す（Ｓ１５３）。暗号処理部１１７は、この特徴パターンデータ群を対称鍵により暗号化して（Ｓ１５４）、アドホック通信制御部１１６に渡す。アドホック通信制御部１１６は、この暗号化された特徴パターンデータ群をパケット化し、アドホック無線装置１３２から無線送信し（Ｓ１５５）、このタイムスタンプ処理（Ｓ１５０）を終了する。すなわち、自身の生成タイムスタンプが相手方の生成タイムスタンプより新しければ、自身の方が新しい特徴パターンデータ群を保持していることになるので、この特徴パターンデータ群を相手方に送信する。

【００９０】

なお、ステップＳ１５４で、特徴パターンデータ群を暗号化するのは、当該カーナビゲーション装置１００が保持している特徴パターンデータを外部の第三者に隠蔽するためである。

【００９１】

次に、図９に示すフローチャートに従って、図６及び図７中のステップＳ１６０における登録処理の詳細について説明する。

【００９２】

登録処理では、まず、データ管理部１１３が、受信パケット中のデータが記憶装置１２０に既に登録済みのデータであるか否かを判断する（Ｓ１６１）。登録済みのデータである場合には、このデータを廃棄して（Ｓ１６４）、処理を終了する。また、未登録のデータである場合には、このデータがウィルス対処データ（特徴パターンデータ群）であるか否かを判断する（Ｓ１６２）。このデータがウィルス対処データである場合には、このデータに含まれている電子署名が正規のものであるか否かを検証する(Ｓ１６３)。この場合、ウィルス対処データの作成元の公開鍵証明書を記憶装置１２０に予め登録しておき、データ管理部１１３がこの証明書を利用して検証する。

【００９３】

ウィルス対処データに含まれている電子署名が正規のものでなければ、このデータを廃棄して（Ｓ１６４）、処理を終了する。また、電子署名が正規のものであると判断された場合、及び、ステップＳ１６２の判断でこのデータがウィルス対処データでないと判断された場合に、このデータを記憶装置１２０に登録して、処理を終了する。なお、受信パケット中のデータがウィルス対処データである場合には、これを記憶装置１２０中のウィルス対処データ・データベース１２１に登録する。なお、ウィルス対処データを登録する際には、復号化（Ｓ１３５）したものをそのまま登録してもよいが、ウィルス対処部１１２

が利用する形態に整理し直した後、登録してもよい。

【００９４】

以上のように、本実施形態では、共有化サービスを受ける他のカーナビゲーション装置との間でのアドホック通信により、特徴パターンデータの生成タイムスタンプを受信し、自生成タイムスタンプの方が新しければ、最新の特徴パターンデータ群をこの他のカーナビゲーション装置へ送信し、自生成タイムスタンプの方が古ければ、自生成タイムスタンプを他のカーナビゲーション装置へ送信して、この他のカーナビゲーション装置から最新の特徴パターンデータ群を受信している。また、すなわち、本実施形態では、共有化サービスを受けるカーナビゲーション装置相互間で、アドホック通信により、最新の特徴パターンデータ群の共有化を図っている。

【００９５】

次に、ディスク記録再生装置１０２に装着された可搬型ディスク記憶媒体Ｄに対する書込／読出処理について、図１０のフローチャートに従って説明する。

【００９６】

データ管理部１１３は、常時、ディスク記録再生装置１０２にディスクが装着されたか否かを監視している（Ｓ１７１）。ディスクが装着されている場合、データ管理部１１３は、入出力装置１４０から指示等に従って、このディスクに対してデータ書込処理を行うかデータ読出処理を行うかを判断する（Ｓ１７２）。データ書込処理を行うと判断した場合には、入出力装置１４０から指示等に従って、記憶装置１２０に格納されているデータの一部や入出力装置１４０から入力されたデータ等を、ディスク記録再生装置１０２により、ディスクに書き込ませて（Ｓ１８１）、処理を終了する。

【００９７】

データ管理部１１３は、読込処理を行うと判断した場合には、ウィルス対処部１１２に、ディスク中のデータにコンピュータウィルスが存在するか否かをチェックさせる。この際、ウィルス対処部１１２は、ディスク中のデータに、ウィルス対処データ・データベース１２１中の特徴パターンデータに対応するものがあるか否かをチェックする（Ｓ１７３）。

【００９８】

ウィルス対処部１１２によるウィルスチェックの結果、コンピュータウィルスが在った場合には、ウィルス対策入出力制御部１１４により、このディスクのデータには、コンピュータウィルスが存在する旨が、入出力装置１４０に表示される(Ｓ１８３)。当該カーナビゲーション装置１００が搭載されている車両Ｃの運転者等は、この表示を見て、ディスク記録再生装置１０２からディスクを取り出す等の処理を行う。また、この際、運転者が入出力装置１４０を操作して、ディスク中のデータを記憶装置１２０に登録しようとしても、ウィルス対策入出力制御部１１４により、この登録が拒否される。すなわち、このデータの利用が拒否される。

【００９９】

ウィルス対処部１１２がディスク中のデータにコンピュータウィルスが存在しないと判断すると、データ管理部１１３が、ウィルス対処データ・データベース１２１に格納されているデータがコンピュータウィルスに対する対処十分条件を満たしているか否かを判断する（Ｓ１７５）。このデータ管理部１１３の判断は、図５におけるステップＳ１１２におけるデータ管理部１１３の判断と同様である。

【０１００】

データ管理部１１３は、対処十分条件を満たしていると判断すると、ディスク中のデータから特徴値を抽出し（Ｓ１７６）、これを記憶装置１２０のチェック済みファイルリスト１２５に記録し（Ｓ１７７）、ステップＳ１７９に進む。なお、データの特徴値は、このデータのハッシュ値であってもよい。また、データ管理部１１３は、ステップＳ１７５で、対処十分条件を満たしていないと判断すると、ディスク中のデータに、チェック済みファイルリスト１２５に記録されている特徴値を持つものが存在するか否かを調べる（Ｓ１７８）。ディスク中のデータに、チェック済みファイルリスト１２５に記録されている

特徴値が存在する場合、ディスク中のデータと対応するデータが過去に不正なデータでなかったことが確認されているので、このディスク中のデータも安全であるとみなし、ステップＳ１７９に進む。また、ディスク中のデータに、チェック済みファイルリスト１２５に記録されている特徴値が存在しない場合、このディスク中のデータは、コンピュータウィルスが存在する可能性があるので、ウィルス対策入出力制御部１１４により、このディスクのデータには、コンピュータウィルスが存在する可能性がある旨が、入出力装置１４０に表示される(Ｓ１８３)。また、この際も、運転者が入出力装置１４０を操作して、ディスク中のデータを記憶装置１２０に登録しようとしても、ウィルス対策入出力制御部１１４により、この登録が拒否される。

【０１０１】

ステップＳ１７９では、データ管理部１１３が、このディスク中のデータに対して、どのような処理をすべきか判断する（Ｓ１７９）。ディスク中のデータに作成タイムスタンプが格納されている場合には、タイムスタンプ処理が必要であると判断され、この場合には、タイムスタンプ処理が実行され（Ｓ１９０）、一連の処理を終了する。また、登録処理が必要であると判断された場合には、このデータ管理部１１３により、記憶装置１２０内の所定領域への登録処理が実行され（Ｓ１６０（図９））、一連の処理を終了する。この登録処理で、登録対処がウィルス対処データである場合には、このウィルス対処データがウィルス対処データ・データベース１２１に登録される。さらに、表示処理等の他の処理が必要であると判断された場合、ＣＰＵ１１０の諸機能によりこの他の処理が実行され（Ｓ１８２）、一連の処理を終了する。

【０１０２】

次に、図１１に示すフローチャートに従って、ステップＳ１９０におけるタイムスタンプ処理の詳細について説明する。

【０１０３】

まず、データ管理部１１３が、図８を用いて説明したタイムスタンプ処理（Ｓ１５０）と同様に、ウィルス対処データ・データベース１２１の作成タイムスタンプ領域１２１ｂ（図３）に格納されているタイムスタンプのうちから自端末が持つ最新のタイムスタンプを取得する(Ｓ１９１)。次に、データ管理部１１３は、ディスクのデータ中に含まれている生成タイムスタンプと、ステップＳ１９１で取得したタイムスタンプとの新旧を比較する（Ｓ１９２）。ステップＳ１９１で取得した自端末の最新のタイムスタンプの方が古ければ、ディスク記録再生装置１０２により、ステップＳ１９１で取得した自端末の最新のタイムスタンプをディスクに書き込ませて（Ｓ１９５）、このタイムスタンプ処理（Ｓ１９０）を終了する。このように、ステップＳ１９１で取得したタイムスタンプ、つまり自タイムスタンプをディスクに書き込ませるのは、先にこのディスクにタイムスタンプを書き込んだ装置へ、自タイムスタンプを知らせることで、自タイムスタンプよりも新しい特徴パターンデータを必要としていることを伝えるためである。

【０１０４】

また、ステップＳ１９１で取得した自端末の最新のタイムスタンプと、ディスクのデータ中に含まれる生成タイムスタンプと、が同じであれば、このタイムスタンプ処理（Ｓ１５０）を終了する。これは、自身が所有している最新の特徴パターンデータ群と同じものを相手方も所有しているからである。

【０１０５】

また、ステップＳ１９１で取得した自端末の最新のタイムスタンプが、ディスクのデータ中に含まれる生成タイムスタンプより新しければ、ウィルス対処データ・データベース１２１から、ディスクのデータ中に含まれている生成タイムスタンプより新しい全ての生成タイムスタンプに対応する特徴パターンデータ群を抽出し（Ｓ１９３）、ディスク記録再生装置１０２により、この特徴パターンデータ群をディスクに書き込ませて（Ｓ１９４）、このタイムスタンプ処理（Ｓ１５０）を終了する。すなわち、自身の生成タイムスタンプが相手方の生成タイムスタンプより新しければ、自身の方が新しい特徴パターンデータ群を保持していることになるので、先にこのディスクにタイムスタンプを書き込んだ装

置へ、この特徴パターンデータ群を知らせる。

【０１０６】

以上のように、本実施形態では、共有化サービスを受ける他のカーナビゲーション装置との間での記憶媒体のやり取りで、特徴パターンデータの生成タイムスタンプを受け取り、自生成タイムスタンプの方が新しければ、最新の特徴パターンデータ群をこの他のカーナビゲーション装置へ記憶媒体を介して渡し、自生成タイムスタンプの方が古ければ、自生成タイムスタンプを他のカーナビゲーション装置へ記憶媒体を介して渡して、この他のカーナビゲーション装置から、記憶媒体を介して最新の特徴パターンデータ群を受け取っている。すなわち、本実施形態では、共有化サービスを受けるカーナビゲーション装置相互間で、記憶媒体のやり取りにより、最新の特徴パターンデータ群の共有化を図っている。

【０１０７】

なお、以上の実施形態では、ディスク型記憶媒体を利用する場合を例示しているが、本発明は、これに限定されるものではなく、他の可搬型記憶媒体、例えば、メモリデバイス等を利用してもよいことは言うまでもない。

【０１０８】

以上、本実施形態によれば、定期的に、最新のウィルス対処データ（特徴パターンデータ群）をウィルス対処データ提供装置２００から取得するようにしているが、このウィルス対処データ提供装置２００から最新のウィルス対処データを取得できず、最新のウィルス対処データを保持していないときに通信ネットワーク１を利用して通信を行う際には、ウィルス対処が十分な中継装置３００を介して、通信を行うようにしているので、カーナビゲーション装置１００がコンピュータウィルスに侵される可能性を低下させることができる。この場合、本実施形態では、最新のウィルス対処データを保持していないときにでも、中継装置３００を介した通信を許容しているので、通信ネットワーク１との接続を完全に遮断する場合と比べて、運転者等の不都合を小さく抑えることができる。

【０１０９】

また、本実施形態では、このウィルス対処データ提供装置２００から最新のウィルス対処データを取得できず、最新のウィルス対処データを保持していないときには、ディスク記録再生装置１０２からのデータの取り込みも制限しているので、この点からも、カーナビゲーション装置１００がコンピュータウィルスに侵される可能性を低下させることができる。この場合、ディスク記録再生装置１００からのデータ取込を一律に制限するのではなく、過去実績に基づいて、一部のデータ取込を制限しているので、記憶媒体を利用できない等による運転者等の不都合を小さく抑えることができる。

【０１１０】

また、本実施形態では、アクセスポイント２を介して、ウィルス対処データ提供装置２００から最新のウィルス対処データを取得できない場合でも、共有化サービスを受ける他のカーナビゲーション装置から、アドホック通信又は記憶媒体のやり取りにより、最新のウィルス対処データを取得することができるので、最新のウィルス対処データを保持していない期間を短くすることができる。このため、通信ネットワーク１の利用制限やディスク記録再生装置１００からのデータ取込制限の期間を短くすることができる。

【０１１１】

なお、本実施形態では、当該カーナビゲーション装置１００と通信ネットワークとの接続に、無線ＬＡＮを利用しているが、この代わりに、例えば、携帯電話によるデータ通信を利用してもよい。

【０１１２】

また、本実施形態では、生成タイムスタンプを他のカーナビゲーション装置と交換し合うことで、自カーナビゲーション装置１００が自生成タイムスタンプの新旧を判断するようにしているが、例えば、ウィルス対処データ提供装置２００を管理している施設から、放送波で最新の生成タイムスタンプを配信するようにしてもよい。この場合、自カーナビゲーション装置１００が最新の生成タイムスタンプより自生成タイムスタンプの方が古い

と判断すると、ウィルス対処データ２００に対して、中継装置３００を介して、ウィルス対処データを要求するか、生成タイムスタンプを他のカーナビゲーション装置と交換せずに、他のカーナビゲーション装置に対してウィルス対処データを要求して、これらから最新のウィルス対処データを取得することになる。

【０１１３】

また、本実施形態では、ウィルス対処データ提供装置２００からのウィルス対処データの配信は、通信ネットワーク１を媒体にするものであるが、放送波を媒体にしてもよい。この場合、ウィルス対処データを頻繁に配信するように配信スケジュールを組むことがこのましい。また、放送によりウィルス対処データを配信する場合、カーナビゲーション装置１００から、ウィルス対処データ提供装置２００に対して、ウィルス対処データの配信要求すること必要はない。

【０１１４】

放送波は、アナログ放送にデータを重畳したものであってよいし、ディジタル放送であって、送信するデジタルデータに上記情報あるいはデータを含むものであってよい。特徴パターンデータの対象となる機種などごとに、データ放送のチャンネルを割り当ててもよい。同一のチャンネル内に、異なる機種などの複数の対象に対するデータを混在させてもよい。その場合、データごとに対象となる機種などを判別する識別子を付与し，受信する情報端末において選択可能にしてもよい。

【０１１５】

データをいくつかのブロックに分割して、送信することにしてもよい。電波の受信状態などの影響で受信できないブロックが生じた場合に、該当ブロックの再放送時に当該ブロックを受信し，受信済みのブロックと統合することでデータの受信を完了するようにしてもよい。

【０１１６】

さらに、以上では、カーナビゲーション装置を対象にしているが、カーナビゲーション装置以外のナビゲーション装置、例えば、歩行者の道案内用のナビゲーション装置に本発明を適用してもよい。

【図面の簡単な説明】

【０１１７】

【図１】本発明に係る一実施形態におけるカーナビゲーション装置の構成図である。

【図２】本発明に係る一実施形態におけるシステムを構成する各装置の構成図である。

【図３】本発明に係る一実施形態におけるウィルス対処データ・データベースのデータ構成を示す説明図である。

【図４】本発明に係る一実施形態における中継用テーブルのデータ構成を示す説明図である。

【図５】本発明に係る一実施形態における通信ネットワークに対する情報要求時の処理を示すフローチャートである。

【図６】本発明に係る一実施形態における通信ネットワークからのパケット受信時の処理を示すフローチャートである。

【図７】本発明に係る一実施形態におけるアドホック通信時の処理を示すフローチャートである。

【図８】図７のフローチャート中のタイムスタンプ処理（Ｓ１５０）の詳細を示すフローチャートである。

【図９】図７のフローチャート中の登録処理（Ｓ１６０）の詳細を示すフローチャートである。

【図１０】本発明に係る一実施形態におけるディスクに対するデータの書込及び読出時の処理を示すフローチャートである。

【図１１】図１０のフローチャート中のタイムスタンプ処理（Ｓ１９０）の詳細を示すフローチャートである。

【図１２】本発明に係る一実施形態における各種通信パケットのデータ構成を示す説明図

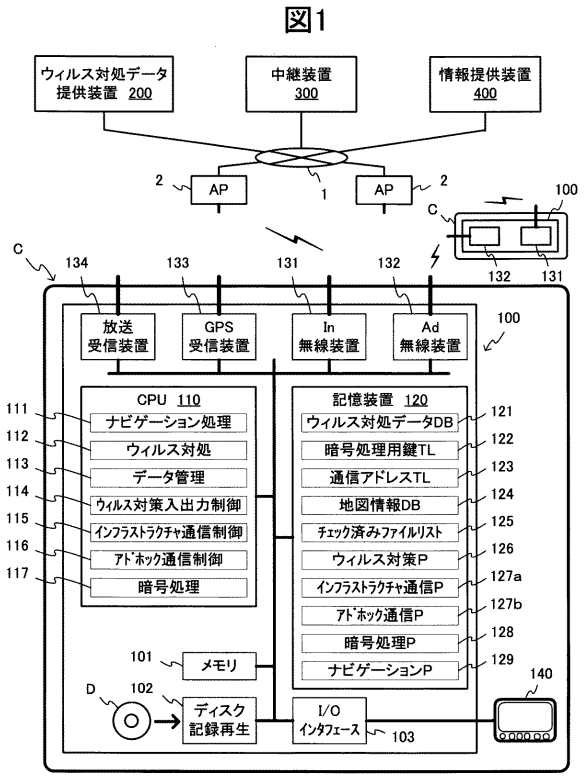
である。

【符号の説明】

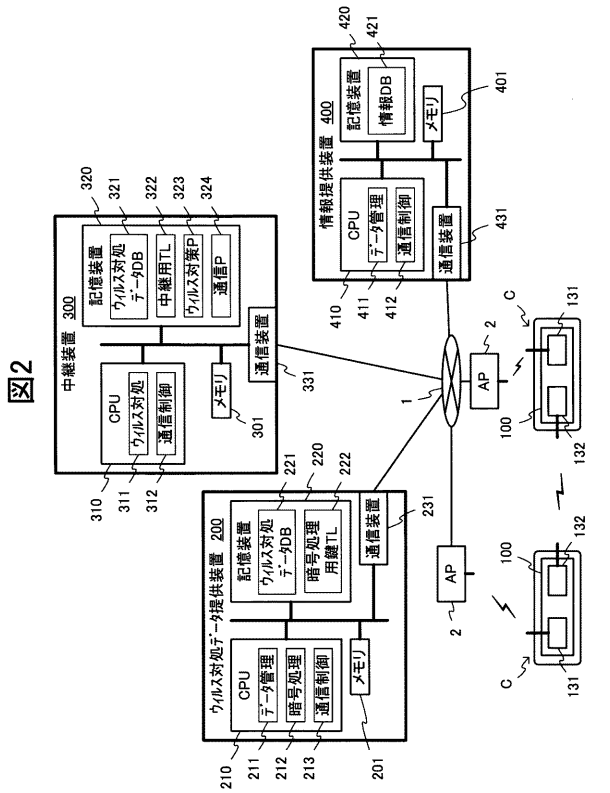
【０１１８】

１：通信ネットワーク、２：アクセスポイント、１０：情報要求パケット、１０ａ：情報要求転送パケット、２０：応答パケット、２０ａ：応答転送パケット、１００：カーナビゲーション装置、１０１：メモリ、１０２：ディスク記録再生装置、１１０，２１０，３１０，４１０：ＣＰＵ、１１１：ナビゲーション処理部、１１２，３１１：ウィルス対処部、１１３，２１１，４１１：データ管理部、１１４：ウィルス対策入出力制御部、１１５：インフラストラクチャ通信制御部、１１６：アドホック通信制御部、１１７：安藤処理部、１２０，２２０，３２０，４２０：記憶装置、１２１，２２１，３２１：ウィルス対処データ・データベース、１２２：暗号処理用鍵テーブル、１２３：通信アドレステーブル、１２４：地図情報データベース、１２５：チェック済みファイルリスト、１２６，３２３：ウィルス対策プログラム、１２７ａ：インフラストラクチャ通信プログラム、１２７ｂ：アドホック通信プログラム、１２８：暗号処理プログラム、１２９：ナビゲーションプログラム、１３１：インフラストラクチャ無線装置、１３２：アドホック無線装置、１３３：ＧＰＳ受信装置、１４０：入出力装置、２００：ウィルス対処データ提供装置、３００：中継装置、４００：情報提供装置

【図１】



【図２】



【図３】

図3

ウィルス対処データDB 121

更新ﾀｲﾑｽﾀﾝﾌﾟ	作成ﾀｲﾑｽﾀﾝﾌﾟ	電子署名	特定パターンデータ
⋮	⋮	⋮	⋮
2008/4/30	2008/4/26	BB	…
2008/5/7	2008/5/3	AA	…
2008/5/14	2008/5/10	AA	…
121a	121b	121c	121d

【図４】

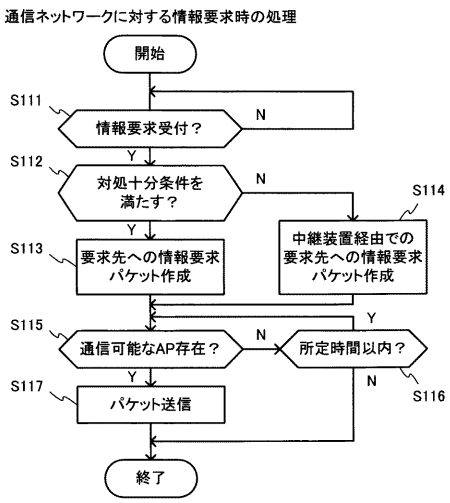
図4

中継用TL 322

送信元アドレス	送信先アドレス	メッセージ番号
212.112.168	248.329.455	AB002
143.521.342	248.329.455	AC014
⋮	⋮	⋮
322a	322b	322c

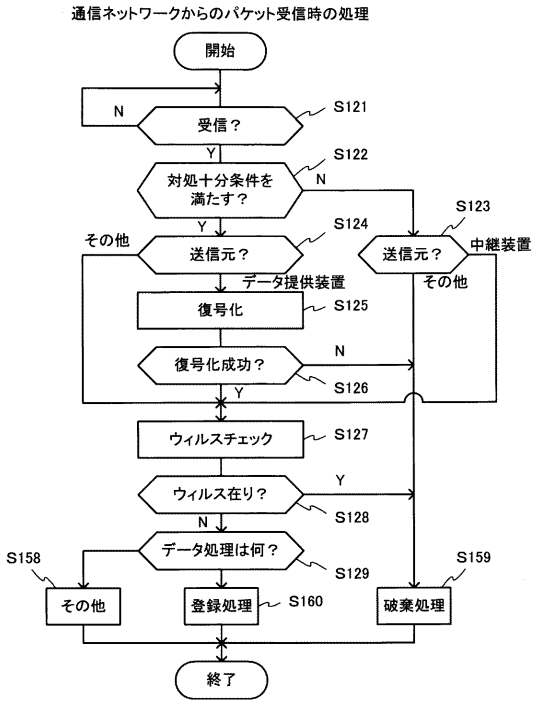
【図５】

図5



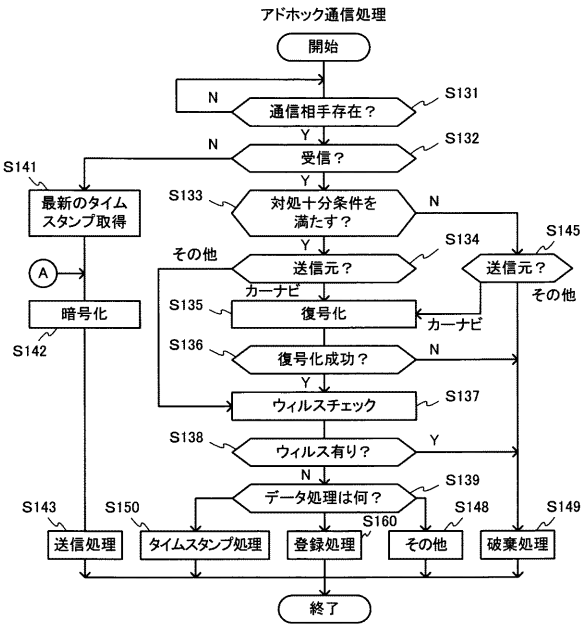
【図６】

図6



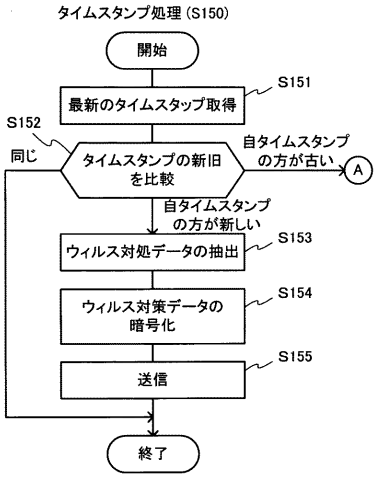
【図７】

図7



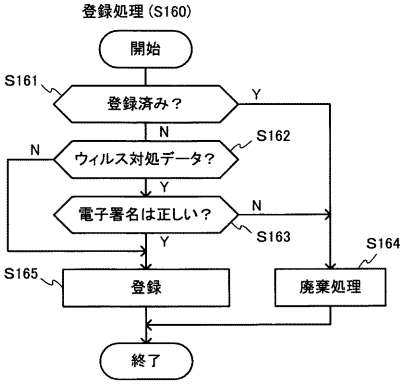
【図８】

図8



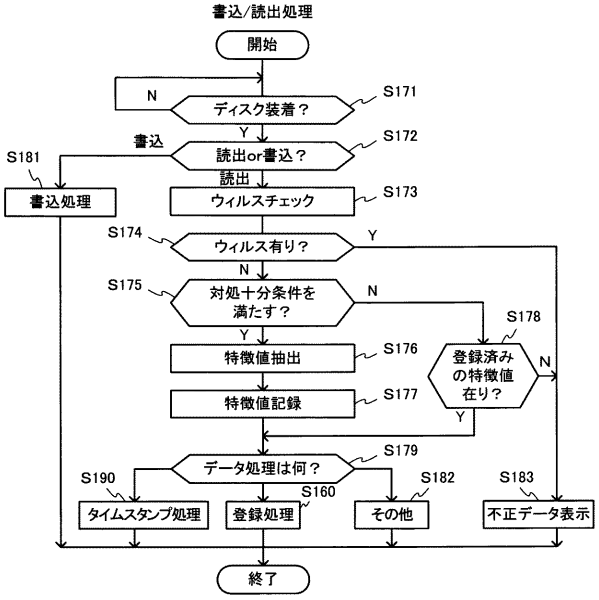
【図９】

図9



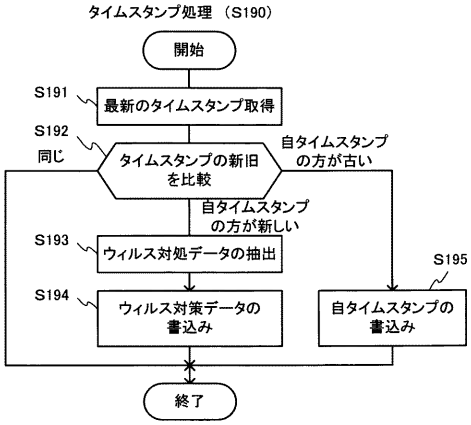
【図１０】

図10



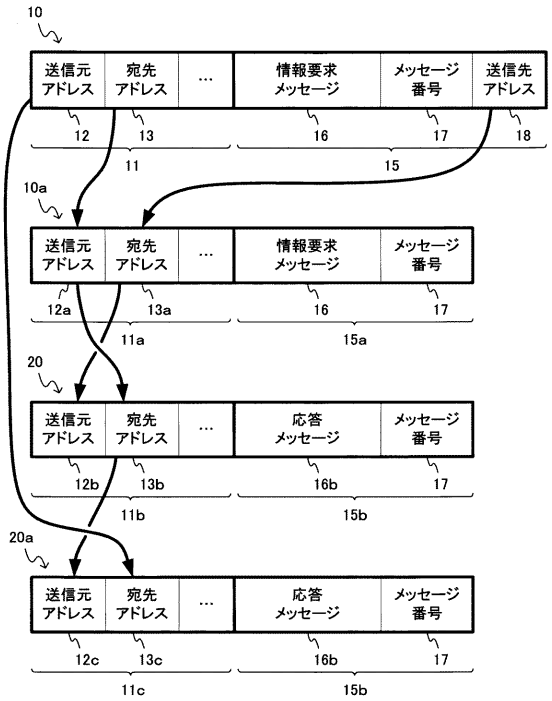
【図１１】

図11



【図１２】

図12


10
送信元アドレス
宛先アドレス
…
情報要求メッセージ
メッセージ番号
送信先アドレス
12
13
16
17
18
11
15
10a
送信元アドレス
宛先アドレス
…
情報要求メッセージ
メッセージ番号
12a
13a
16
17
11a
15a
20
送信元アドレス
宛先アドレス
…
応答メッセージ
メッセージ番号
12b
13b
16b
17
11b
15b
20a
送信元アドレス
宛先アドレス
…
応答メッセージ
メッセージ番号
12c
13c
16b
17
11c
15b

フロントページの続き

(51)Int.Cl.												テーマコード（参考）
Ｇ０６Ｆ 21/22 (2006.01)							Ｇ０６Ｆ 9/06 ６６０Ｎ					
Ｆターム(参考)	5B285	AA01	BA01	CA06	CA12	CA16	CA34	CA36	CB62	CB72	CB84	
		DA05										
	5K067	AA30	BB36	CC08	DD17	EE02	EE10	FF23	HH22	HH23	HH36	
		KK15										