(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3877167号
(P3877167)
(45)発行日　平成19年2月7日(2007.2.7)　(24)登録日　平成18年11月10日(2006.11.10)

(51)Int.Cl.		F I		
G08B 13/22	(2006.01)	G08B	13/22	
B65G 61/00	(2006.01)	B65G	61/00	522
G08B 25/10	(2006.01)	G08B	25/10	A
H04M 11/00	(2006.01)	H04M	11/00	301

請求項の数 20　(全 36 頁)

(21)出願番号	特願2003-570320 (P2003-570320)
(86)(22)出願日	平成15年2月25日 (2003.2.25)
(86)国際出願番号	PCT/JP2003/002074
(87)国際公開番号	WO2003/071502
(87)国際公開日	平成15年8月28日 (2003.8.28)
審査請求日	平成16年11月16日 (2004.11.16)
(31)優先権主張番号	10/080,927
(32)優先日	平成14年2月25日 (2002.2.25)
(33)優先権主張国	米国(US)
(31)優先権主張番号	10/119,310
(32)優先日	平成14年4月10日 (2002.4.10)
(33)優先権主張国	米国(US)
(31)優先権主張番号	10/200,552
(32)優先日	平成14年7月23日 (2002.7.23)
(33)優先権主張国	米国(US)

(73)特許権者　000002945
オムロン株式会社
京都市下京区塩小路通堀川東入南不動堂町８０１番地
(74)代理人　100083024
弁理士　高橋　昌久
(74)代理人　100103986
弁理士　花田　久丸
(72)発明者　久野　敦司
日本国京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内

最終頁に続く

(54)【発明の名称】対象物および対象物の近傍空間領域の状態監視システムと状態監視方法ならびに、貨物コンテナ監視システム

(57)【特許請求の範囲】

【請求項１】

監視対象物に装着された複数個の無線通信ノード間の無線通信におけるリンク状態を監視することにより得られる前記複数個の無線通信ノード間のリンク状態監視情報を得て、前記監視対象物が正常状態にあった時のリンク状態正常情報と比較し、両情報に差異があるか否かを判断することにより、前記監視対象物の動き又は前記監視対象物近傍の所定領域の状態を検知する状態監視システム。

【請求項２】

監視対象物に装着された複数個の無線通信ノードから構成される通信ネットワークのネットワーク構造情報を、無線通信ノード間の無線通信におけるリンク状態監視情報を総合して生成し、前記監視対象物が正常状態にあった時のリンク状態正常情報と比較し、前記両情報に差異があるか否かを判断することにより、ネットワーク構造情報を用いて前記監視対象物の動き又は前記監視対象物近傍の所定領域の状態を監視する状態監視システム。

【請求項３】

監視対象物に装着された複数個の無線通信ノードから構成される通信ネットワークのネットワーク構造情報を、無線通信ノード間の無線通信におけるリンク状態の情報を総合して生成し、ネットワーク構造情報を用いて監視対象物の動き又は監視対象物近傍の所定領域の状態を監視する状態監視システムであって、前記の無線通信ノードが：

▲１▼他の無線通信ノードとデータ通信を行なうデータ通信手段と；

▲２▼前記データ通信手段により得られた他の無線通信ノードとのリンク状態を検知し、

リンク状態監視情報を記憶するリンク状態検知手段；
とを備えるコンテナの状態監視システムであって、監視時に得られた前記リンク状態監視情報と、前記コンテナが正常状態にあった時のリンク状態正常情報とを比較し、前記両情報に差異があるか否かを判断することにより、前記コンテナの内部状態を監視する状態監視システム。
【請求項４】
監視対象物に装着された複数個の無線通信ノードから構成される通信ネットワークのネットワーク構造情報を、無線通信ノード間の無線通信におけるリンク状態の情報を総合して生成し、ネットワーク構造情報を用いて監視対象物の動き又は監視対象物近傍の所定領域の状態を監視する状態監視システムであって、
所定のタイミングにおけるネットワーク構造情報を監視対象物のＩＤ情報として外部の監視センタに送信する送信手段を備え、前記の無線通信ノードは次の手段を備えるもの
▲１▼他の無線通信ノードとデータ通信を行なうデータ通信手段
▲２▼他の無線通信ノードとのリンク状態を検知し、記憶するリンク状態検知手段。
【請求項５】
前記リンク状態検出手段が、前記無線通信ノード間の距離を検出するものである請求項３又は４に記載の状態監視システム。
【請求項６】
前記リンク状態検出手段が、前記無線通信ノード間のメッセージ転送回数またはそれを元に求まる値を検出するものである請求項３又は４に記載の状態監視システム。
【請求項７】
請求項３又は４記載の状態監視システムにおいて、前記ネットワーク構造情報が、前記ネットワークグラフマトリックスの全部又は特徴ある一部から得られた情報であることを特徴とする状態監視システム。
【請求項８】
請求項３又は４記載の状態監視システムにおいて、前記ネットワーク構造情報が、前記ネットワークグラフマトリックス内の通信不能または脱落ノードの配置情報を除外したネットワークグラフマトリックスの全部又は特徴ある一部から得られた情報であることを特徴とする状態監視システム。
【請求項９】
請求項１から８記載の状態監視システムにおいて、前記監視対象物がコンテナ、家屋、事務所、自動車、倉庫、船舶のように、扉または窓を通じて内部に物体が出入り可能な内部空間を有する物であり、前記無線通信ノードが前記内部空間を構成する内面に装着されて、当該監視対象物を内部から監視することを特徴とする状態監視システム。
【請求項１０】
請求項４記載の状態監視システムにおいてさらに、前記ネットワーク構造情報生成手段により生成された、前記監視対象物の初期ネットワーク構造情報を記録する初期状ネットワーク構造情報記録手段と；
当該ネットワーク構造情報生成手段が所定のインターバル時間で生成する当該監視対象物の監視時ネットワーク構造情報を記録する監視時ネットワーク構造情報記録手段と；
当該初期ネットワーク構造情報記録手段に記録した初期ネットワーク構造情報と監視時ネットワーク構造情報記録手段に記録した監視時ネットワーク構造情報を比較して、比較結果を出力する比較手段；
とで構成されたことを特徴とする状態監視システム。
【請求項１１】
請求項１０記載の状態監視システムにおいて、前記初期ネットワーク構造情報と監視時ネットワーク構造情報との比較で一定以上の差異が検出されるか、比較自体が出来ないか、他のノードとの通信が出来ない場合には、当該監視システムは監視対象物に異常があったと判断し、各通信装置に記録されたネットワーク構造情報を消去することを特徴とする状態監視システム。

【請求項１２】
請求項４記載の状態監視システムにおいてさらに、前記ネットワーク構造情報生成手段により生成された監視対象物の初期ネットワーク構造情報と監視時ネットワーク構造情報とを、一定のインターバル時間で監視対象物とは離れた場所にある監視センターへ送信する情報送信手段とを有することを特徴とする状態監視システム。
【請求項１３】
請求項１２記載の状態監視システムにおいて、前記初期ネットワーク構造情報と監視時ネットワーク構造情報との比較で一定以上の差異が検出されるか、比較自体が出来ないか、他のノードとの通信が出来ない場合には、当該監視システムは監視対象物に異常があったと判断し、もし監視センターにその状態情報がすでに記録されていれば、各通信装置に記録されたネットワーク構造情報を消去することを特徴とする状態監視システム。
【請求項１４】
請求項３または４記載の状態監視システムにおいてさらに、各通信ノードにはその周囲のローカルな状態を検知するセンサーを有しており、当該状態監視システムはもし当該センサーがローカルな異常信号を出力したら当該監視対象物に異常が発生したと判断することを特徴とする状態監視システム。
【請求項１５】
請求項１４記載の状態監視システムにおいて、前記センサーが監視対象物の振動を検知する振動センサーか、温度センサーか、又は監視対象物の空間外からの侵入を検知する侵入検知センサーであることを特徴とする状態監視システム。
【請求項１６】
請求項９記載の状態監視システムにおいて、前記無線通信ノードが装着された前記内部空間と外部との通信は、その通信を内部空間を閉鎖した状態で実行するための電磁誘導型の通信装置で行なう事を特徴とする状態監視システム。
【請求項１７】
運送中のコンテナの内部状態を監視する状態監視システムにおいて：
コンテナ内にランダム又は規則的に設置された複数個の通信ノードにより構成され通信ネットワークと；
当該複数個の通信ノードの特徴的配置情報からネットワーク構造情報を得るネットワーク構造情報生成手段と；
前記ネットワーク構造情報生成手段により生成された、前記コンテナの初期ネットワーク構造情報を記録する初期状ネットワーク構造情報記録手段と；
当該ネットワーク構造情報生成手段が所定のインターバル時間で生成する当該コンテナの監視時ネットワーク構造情報を記録する監視時ネットワーク構造情報記録手段と；
当該初期ネットワーク構造情報記録手段に記録した初期状ネットワーク構造情報と監視時ネットワーク構造情報記録手段に記録した監視時ネットワーク構造情報を比較して、比較結果を出力する比較手段と；
当該比較手段から比較結果を受け、もし当該比較手段からの比較結果に一定以上の差異があれば、当該コンテナを下ろすクレーンに対して特別な注意を喚起する警報信号を送る監視センター；
とで構成されたことを特徴とするコンテナの状態監視システム。
【請求項１８】
請求項１７記載の状態監視システムにおいてさらに、前記監視センタは、前記比較手段から比較結果を受け、もし当該比較手段からの比較結果に一定以上の差異が無ければ、コンテナに装備された電子ロックシステムに対して、自動生成された電子ロックソフト又はデータを設定すると共に、別の安全なルートで対応するパスワードを送出することを特徴とするコンテナの状態監視システム。
【請求項１９】
運送中のコンテナの内部状態を監視する状態監視装置において：
コンテナ内にランダム又は規則的に設置された複数個の通信ノードにより構成され通信ネ

ットワークと；
当該複数個の通信ノードの特徴的配置情報からネットワーク構造情報を得るネットワーク構造情報生成手段；
とを備えるコンテナの状態監視装置であって、監視時に得られた前記ネットワーク構造情報である監視情報と、前記コンテナが正常状態にあった時のネットワーク構造情報である正常情報とを比較し、前記両情報に差異があるか否かを判断することにより、前記コンテナの内部状態を監視する状態監視装置。
【請求項２０】
運送中のコンテナの内部状態を監視する状態監視方法において、
複数個の通信ノードにより構成され通信ネットワークをコンテナ内にランダム又は規則的に設置し；
コンテナ出荷時に、当該複数個の通信ノードの特徴的配置情報から初期ネットワーク構造情報を得て、当該初期ネットワーク構造情報を記録し；
コンテナ出荷後に、所定のインターバル時間で当該一定空間または当該一定空間内に載置された監視対象物の監視時ネットワーク構造情報を得て、当該監視時ネットワーク構造情報を記録し；
当該初期状ネットワーク構造情報と監視時ネットワーク構造情報を比較して、比較結果を監視センターへ出力し；
当該比較結果を受け、もし当該比較手段からの比較結果に一定以上の差異があれば、当該監視センターは当該コンテナを下ろすクレーに対して特別な注意を喚起する警報信号を送る；
各ステップで構成されたことを特徴とするコンテナの状態監視方法。
【発明の詳細な説明】
技術分野
本発明は、監視対象物の動き、および監視対象物近傍の所定の空間領域（例えば倉庫内、コンテナ内、車両内、オフィスや個人住宅の室内、倉庫外の倉庫近傍）の状態監視システムと状態監視方法ならびに、それらを応用して、貨物コンテナ内部に不正アクセスする行為を監視したり、貨物コンテナを偽物コンテナに入れ返ることを検知するためのシステムに関する。
背景技術
２００１年９月１１日に米国で発生したテロ事件を代表例として、国際的にテロが頻発するような状況のため、航空機や船舶、貨物列車、トラックで輸送される貨物コンテナのリスク管理が重要となっている。貨物コンテナに、核兵器、爆弾，毒ガス、生物兵器，放射性物質，テロリストを潜ませて、これらが、さまざまな場所に送り込まれる可能性がある。貨物コンテナには、さまざまな分野の製品や原料が積まれる。米国に到着するコンテナは、年間１８００万個と言われている。そして、現在はその中の２％程度しか貨物の検査がなされていない。コンテナの中に危険物などを紛れ込ませられた場合、コンテナに外部からＸ線をあてて、コンテナ内部の透視画像を生成して、この画像を分析して危険物を検知することができる場合もある。また、放射線検知装置や匂いセンサを用いて危険物を検知できる場合もあるが、危険物が多種多様であることと、危険物の梱包形態が多種多様であろうことを考えると、危険物を検知できない場合の方がはるかに多いと判断できる。また、コンテナの内部に危険物を後から積み込むのではなく、最初から危険物を積み込んだ偽物コンテナに、コンテナを入れ替えられる場合もあると考えられる。コンテナ貨物の盗難は昔から発生しているが、このようなコンテナ貨物の盗賊集団がテロリストと結託して、貨物を盗み出して活動資金を稼ぎつつ、危険物をコンテナに積みこんでテロを行おうとするリスクもある。貨物の危険性をセンサを用いてチェックするのは容易ではないので、荷主の信用性をチェックすることで、その荷主の積み込んだ貨物の危険性を評価しようという動きがある。
しかし、荷主のいない空コンテナについては、荷主の信用性を用いてはコンテナの危険性は評価できない。コンテナ貨物の運搬需要の地域別・季節別の不均衡のため、どうしても

空コンテナを船、列車、トラックなどで地域間や多国間で運搬しなければならない場合が多く発生している。コンテナの運送業者にとっては、空コンテナの運送は何ら利益を生まない行為であるし、貨物を積んでいないので盗難の危険性もない。そのため、コンテナの運送業者は、空コンテナに対するセキュリティ対策にコストをかけようとしない傾向が強い。そのため、空コンテナがテロの道具に使われる可能性が大いにある。従って、空コンテナの扉や壁を不正に開けることを監視する事は、コンテナを用いたテロへの対策として非常に重要である。すなわち、▲１▼コンテナが荷物を積んでいても空であっても、コンテナ内部への不正アクセスを監視・通報すること、▲２▼コンテナを偽物に入れ返られてもそれを検知・通報できることが、コンテナを用いたテロへの対策としては必要である。コンテナ用のシールとして使用されている製品および特許を従来技術として、紹介する。

第２５図（Ａ）は、Ｏｍｎｉ　Ｓｅｃｕｒｉｔｙ　Ｃｏｎｓｕｌｔａｎｔｓ，Ｉｎｃ．のＳＥＡＬＯＣＫというメカ式のシールである。第２５図（Ｂ）はＳｈａｗ　Ｃｏｎｔａｉｎｅｒ　Ｓｅｒｖｉｃｅ　Ｉｎｃ．のコンテナドアに用いられる通常のメカ式シールである。このメカ式のシールはドアのハンドルや取付金具に取付けられ、権限のない者はドアが開けられないようになっている。すなわち権限のあるものだけが保有する鍵によってこのシールはあけることが出来る。この種類のメカ式シールでは、材質が硬い金属で出来ているのでそれを切断して内部に入るのは難しい。もし切断して内部に入ったとしても、その痕跡が後で簡単に目視することが容易である。もし侵入したことを隠蔽するために切断部分を修復しても、その部分はやはり容易に目視できる。

しかしながら鍵は比較的複製するのが容易であり、このためにセキュリティレベルが低くなる。この点が特にテロリスト等により、危険物を内部に持ち込まれるという重大な問題となる。また、シールがコンテナの外に取り付けられているために、同型のものを用意しておきコンテナの扉を不正開閉した後に、用意したシールと入れかえる準備も容易である。

第２６図（Ａ）はＥ．Ｊ．Ｂｒｏｏｋｓ　Ｃｏｍｐａｎｙの、いわゆるＥ・シールと呼ばれる電子式のコンテナシールで、コンテナの出荷人はこのＥ－シール付きのコンテナと通信が可能になる。本装置は陸上輸送、鉄道輸送、そして海上輸送等の大容量輸送に使用することが出来る。このＥ－シールが装備されたドアを権限の無い者が開けようとすれば、金属ロッドかケーブルを切断しなければ出来ない。もしその金属ロッドかケーブルが切断されると、電子回路がそれを検知して、そのデータを記憶装置に記録する。そのデータは通信が可能なときに監視センタに送られる。このシステムではコンテナのドアを目視で確認する必要は無く、コンテナのドア開閉を遠隔監視することが出来る。従ってより多くのコンテナをチェックすることが可能となる。

しかし、これもコンテナの外に取り付けられているものなので、扉の不正開閉を計画する者が事前にシールの無効化の準備をすることが容易である。例えば、電子回路を急速冷却して扉の開閉の監視機能を眠らせることもできる。

第２６図（Ｂ）は、イスラエルのＨｉ－Ｇ－Ｔｅｋ社の電子式シールであり、これはいわゆるＨｉ・シールと呼ばれている。このＡｃｔｉｖｅ　Ｈｉ－Ｇ－シールはデータを記録するセキュリティー装置で、記録されたデータを遠隔地から読み出すことが出来る。またこの装置は詳細確認機能を有している。すなわち全ての開閉を記録し、ハンドヘルドの装置へその記録をダウンロードすることが可能である。装置内に記録されダウンロードされる詳細な記録内容は、開閉の時刻と時間が含まれており、シールされた監視対象の責任者に、常に管理責任を明確にさせることが出来る。ハンドヘルド装置に集めら得たデータは、データ管理のために、標準的なスプレッドシートとデータベースに使用するためにテキストファイル形式でダウンロードされる。繰り返し使用可能な本装置は１０００台のシールに使用可能であり、その電池の使用期限は一日の読み出し回数にもよるが数年である。本装置は迂回ないしは複製できない。本装置とハンドヘルド装置間の通信は３ＤＥＳで暗号化されており、データの複製は出来ないようになっている。しかし、これもコンテナの外に取り付けられているものなので、扉の不正開閉を計画する者が事前にシールの無効化の準備をすることが容易である。例えば、電子回路を急速冷却して扉の開閉の監視機能を

眠らせることもできる。
コンテナのシールとして、さらに米国特許４，７５０，１９７に開示されたコンテナ装置がある。第２７図に示すように、コンテナの内部にドア開閉センサ（３８、４０、４２、４４）を設けている。コンテナの内部でセンサ情報を処理してドアの開閉監視および開閉検知の際の外部への無線通報、警告音発生などの対応を制御するコントローラが装備されている。コンテナの天井には穴があいていて、そこから携帯電話のアンテナや無線測位装置のアンテナが外部に突き出している。
この技術の問題点は次のとおりである。
▲１▼センサの設置位置が一定であるので、センサに感知されないコンテナの壁や天井や扉の部分を切断されて、侵入されてもそれが検知できない。これは、コンテナ外部にｅ－Ｓｅａｌが設置されているのと同様に、セキュリティシステムの手の内をさらしてしまい、侵入を企てる者が、センサの裏をかくやりかたを編み出し易くしてしまう。
▲２▼電波によりセンターに通報ができない状態で、扉を不正に開けられた後で、コンテナ内部に危険物を積みこまれた後で、コントローラやセンサをとりかえられて、扉の不正開閉の記録のない状態にされると、まったく扉の不正開閉があったことがわからなくなる。そうすると、コンテナ内部に危険物が容易に送りこまれるようになる。
さらに米国特許５，６１５，２４７にはコンテナのシールとして第２８図に示すものが開示されている。コンテナ２０の内部にコントローラ３４を設け、コンテナの扉の継ぎ目３３から外部にケーブル２４と２５を出す。このケーブルは、コンテナの扉の外側に設けられたドアハンドル２６と２７をつなぐように懸架されている。ケーブル２４と２５はコンテナ外部にあるシール３０で相互に接続されて、コントローラ３４に接続されたループを描いている。したがって、扉をあけるためには、この継ぎ目３３をはずすか、ケーブル２４またはケーブル２５を切断するしかない。コントローラ３４がコンテナの内部にあるので、コンテナの外部にｅ－Ｓｅａｌを設ける方法よりもコントローラ３４が不正者から攻撃を受ける危険は小さい。コントローラ３４は、ケーブル２４、ケーブル２５、シール３０のどれかの切断を検知すると、扉の不正開放と判断して、無線通信機能で、センターにその旨を通報する。この技術の問題点は、次のとおりである。
▲１▼ドアハンドル２６、２７を切断して、ケーブル２４とケーブル２５をドアハンドルから取り外せば、扉を開放してもコントローラ３４はそれを検知できない。コントローラがわからない間に、扉を開けてコンテナ内に危険物を積みこみ、その後、ケーブル２４とケーブル２５を懸架した状態で、新しいドアハンドルを付ければ、扉の不正開閉をコントローラに検知されないで、しかもコンテナ外観も変わらないということになる。これも結局は、扉の不正開閉を試みようとする者が、不正開閉の前から扉の不正開閉の検知システムの状況を把握できることに原因がある。
▲２▼電波によりセンターに通報ができない状態で、扉を不正に開けられた後で、コンテナ内部に危険物を積みこまれた後で、コントローラやセンサをとりかえられて、扉の不正開閉の記録のない状態にされると、まったく扉の不正開閉があったことがわからなくなる。そうすると、内部に危険物のあるコンテナが容易に送りこまれるようになる。
日本国の公開特許公報である特開平０９－２７４０７７号に記載の電子式シールがある。この電子式シールにおいては、送信手段は、所定の拡散符号で拡散変調したスペクトル拡散波をスペクトル拡散波が反射可能な検出空間内（コンテナ内など）に出力し、受信手段は、送信手段で用いた拡散符号と一致するスペクトル拡散波を受信する毎にその受信強度に応じた相関ピーク信号を出力する。検出空間内において人間などの物体が移動すると、検出空間内を伝播するスペクトル拡散波の伝播経路が変化し、その変化に応じて受信手段から出力される相関ピーク信号の出力状態が変化するので、この相関ピーク信号の出力状態の変化を検出することにより、検出空間内における人間などの物体の移動を感知することができる。
この技術の問題点は、次のとおりである。
▲１▼コンテナに適用する場合、コンテナの内壁や扉の表面の材質や状態が種々雑多であるので、扉の開閉を検知できるように、受信手段の感度や判定基準値を設定するのに専門

家の技術やノウハウが必要になる
▲２▼送信手段と受信手段がそれぞれ１個しかないので、コンテナに貨物を積む際や、コンテナを運搬中に送信手段または受信手段が破損された場合、システムが全く動作しなくなる。
▲３▼送信手段、受信手段の設置位置を一定にするものであると思われるが、その場合には、コンテナの外部から、送信手段や受信手段に対する攻撃が行なわれる可能性が高くなり、セキュリティレベルが低下する。
上述のように従来のメカ式、電子式のシールには数々の問題点が存在する。その問題をまとめてみれば特に以下のようなＰ１、Ｐ２、Ｐ３の問題がある。
Ｐ１：　シールがコンテナの外側に装着されていると、どのようなシールが装着されているかが、コンテナの外側から丸見えであり、事前にわかるので、擬装用のシールや扉の不正開閉の事前準備が容易である。すなわちメカ式のシールに対しては、破壊して扉を開閉した後で、事前に準備した同型のシールに交換するのは比較的容易である。また電子式のシールに対しても、事前に同型のシールを用いて電子回路の急速冷却の予行演習を充分にすることで、見つけた方法を用いて、現場で急速に、極低温まで電子回路（特にＣＰＵ）を冷却して電子回路の動作を停止させ、扉の開閉を検知できないようにして扉を開閉し、その後、放置して電子回路の動作が再開するようにされる可能性がある。
また、メカ式のシールや電子式のシールを装着する金属の棒（第２５図（ａ）および第２５図（ｂ）においてコンテナの左右の扉に存在する縦方向の金属の棒）をコンテナの扉に固着するためのネジやリベットを取り外されると、メカ式のシールや電子式のシールに何ら手を加えなくても、これらのシールをかいくぐって、コンテナの扉の開閉ができるという欠点もある。
Ｐ２：　メカ式シールにおいては、メカ式のキーによって正当な者がシールを開けるし、電子式シールにおいては、パスワードによって電子ロックを解除する。どちらも、コンテナの運用をする企業にテロリストの仲間がいた場合には、キーやパスワードが漏れて、正当な扉の開閉を偽装され得る。正当な扉の開閉であると偽装されると、いくらシールがあっても、役にはたたない。
Ｐ３：メカ式でも電子式シールでも、コンテナの扉の開閉のみを監視している場合には扉以外からの侵入を検知できない。コンテナの材質はスチールやアルミであり、コンテナの壁板の厚みは２ｍｍ程度であるので、壁板にドリルで穴を開けたり、バーナーやレーザーで穴を開けることも可能である。このように扉以外を攻撃されると、扉だけをシールする方式では対応できない。
コンテナを用いたテロ対策としてのシールには、従来技術の問題点である上記のＰ１，Ｐ２，Ｐ３を解決する必要があるのみでなく、コンテナ輸送の実態と、シールのセキュリティレベルの向上の必要性からみた次のような課題も解決することが求められる。
Ｐ４：　コンテナはすでに全世界に大量に存在している。１年間に米国に入ってくるコンテナの個数は１８００万にも達する。したがって、コンテナを監視するシールは既存のコンテナにも、専門家でなくても簡単に取り付けられるものでなければならない。
Ｐ５：　Ｐ１に記載の問題があるので、コンテナの内部でコンテナの扉や内壁を監視する必要がある。しかし、コンテナは様々な環境で使用されているので、コンテナの扉や内壁の表面の状態は塗装やサビや汚れなどのために様々な状態である。したがって、そのような様々な表面状態の扉や壁などでも監視できるようなものでなければならない。
Ｐ６：　Ｐ５に記載の課題である「様々な表面状態の扉や壁などでも監視できる」ものを解決するセンサであっても、そのようなセンサを個別のコンテナの扉や壁の表面状態に合わせて調整する必要のあるものであってはならない。コンテナを運用する荷物の運搬や積み下ろしの現場に、そのような事ができる人材を確保することは困難であるし、そのような調整作業をする場面は実現しにくい。
Ｐ７：　コンテナへの貨物の積載とコンテナからの貨物の運び出しはフォークリフトを用いて行なわれる場合もあれば、人間が手作業で行なう場合もある。コンテナ内の貨物がコンテナの輸送中にコンテナの壁や扉にぶつかることもあるし、貨物の積み下ろしの時に、

コンテナの壁や扉に貨物やフォークリフトがぶつかることもある。したがって、コンテナ内部に取り付けられて、コンテナ内部を監視するセンサが衝撃で破損することも充分にあるので、単一のセンサに頼っていたのでは、そのセンサが破損したら全く監視ができなくなる。したがって、複数個のセンサをコンテナ内に分散配置し、破損していないセンサからの情報を総合的に利用する仕組みを持たなければならない。

Ｐ８：　コンテナを、危険物を積載した偽物に入れかえられることを検知できるように、再生が不能のＩＤ情報をコンテナごとに保持させるとともに、コンテナからは独立した遠隔地にもそのＩＤ情報を登録しておかねばならない。

Ｐ９：　シール自身への攻撃がやりにくいものであるとともに、もしシールへの攻撃があった場合に、その攻撃を検知でき、検知できた場合には攻撃があったことの痕跡をわかりやすく確実に残せるものでなければならない。

本発明の概要を説明する前に、課題の構造の分析と、解決策としての本発明の位置付けを説明する。Ｐ１～Ｐ９の問題点や課題の中では、Ｐ１がコンテナを用いたテロ対策を考える上で、非常に重要である。Ｐ１はコンテナの外部に設けたシールでは、手間とコストをかけてでもコンテナの内部に不正アクセスしようとするテロリストへの対応策としては、全く不充分であることを示している。すなわち、テロ対策として行なうコンテナのシールのためには、コンテナを内側からシールするｉｎｓｉｄｅ　ｓｅａｌ（インサイド・シール）が必須である事を示している。Ｐ２は、正当な権限を持った者がシールを解除する手段に関するセキュリティ確保手段における問題点を示している。Ｐ８は、コンテナを偽物コンテナかどうか判断するためのコンテナＩＤ情報の実現手段が必要であることを示している。したがって、インサイド・シールとしてコンテナを内部から監視するという前提で、監視機能の実現手段としてはＰ３，Ｐ４，Ｐ５，Ｐ６，Ｐ７のそれぞれの問題点や課題を解決する必要がある。コンテナへの攻撃を監視するためのシール自身を攻撃することは、インサイド・シールにすることで、コンテナ外部にシールを設けるよりも格段に困難になるが不可能ではない。したがって、シールを攻撃して無力化した上でコンテナに不正アクセスしようとすることへの対応策は必要であるので、課題Ｐ９の解決も必要である。想定される解決手段として想定される表１に示す各方式を、コンテナを用いたテロへの対策としてのシールでの課題と比較したものを、表２に示す。コンテナを用いたテロ対策の観点では、本発明を用いた方式４が最も課題を解決できるものであることがわかる。

表１

方式名称　　方式の内容

方式１　コンテナの扉の内側表面の一定箇所や、コンテナの内壁の一定箇所に光・音波などの何らかのエネルギーをコンテナ内部から照射し、その反射を受信するセンサを設置し、そのセンサの出力を分析することで、コンテナの扉の動きや内壁への穴あけなどを監視する方式。

方式２　コンテナの扉内側表面にメカニカルスイッチを装着して、扉の開閉でスイッチがＯＮ／ＯＦＦする方式。

方式３　コンテナの内側に、電波を発射する発信機を１つ設け、コンテナ内部で反射して帰ってきた電波を受信する。受信した電波信号を分析して、コンテナ内部の変化を検出する方式。（特開平０９－２７４０７７号に記載の電子式シール）

方式４（本発明をコンテナ監視に応用した方式）コンテナの内側の扉や壁の表面に装着された複数個の無線通信ノード間のリンク状態を監視することで、コンテナの扉や壁の動きや、扉や壁の近傍の所定領域の状態を検知する事、前記リンクの状態が対象物固有のＦｉｎｇｅｒｐｒｉｎｔとしても利用可能である事を特徴とするセンシング方式（本発明の方式）

表２ ○：課題解決に適切　×：課題解決に不適切　？：不明

解決されるべき課題		方式１	方式２	方式３	方式４
監視手段としての課題	P3:扉だけでなく内壁も監視すること	○	×	○	○
	P4:コンテナ内部に簡単に取り付けられるシールであること	×	○	○	○
	P5:様々な状態の表面を持ったコンテナであっても監視できること	○	○	○	○
	P6:監視性能の調整に専門家を必要としないこと	×	○	×	○
	P7:部分的な故障などにも耐えるロバスト性があること	×	×	×	○
攻撃対応	P2:シール解除用のキーが盗みにくいこと	？	？	？	○
	P9:シール自身への攻撃対策をしていること	×	×	×	○
コンテナの偽造対策	P8:再現不能なＩＤ情報をコンテナに付与すること	？	？	×	○
総合評価		不適切	不適切	不適切	適切

発明の開示

本発明の第１の目的は、監視対象物の“動き”、および対象物近傍の所定の空間領域の状態を汎用的な方法で、セキュリティーを保ちながら監視できるようにすることである。例えば監視対象物がコンテナであり、コンテナ内からコンテナを監視する場合には、１）コンテナの扉の開閉や壁などへの穴あけ等の監視、２）コンテナ内での物体の移動、コンテナ内への物体の侵入、コンテナ外への物体の移動の監視３）シール自身への攻撃の監視と攻撃があった場合、攻撃があったことを示すことである。

第２の目的は対象物が偽物と入れ替えられることを検知することである。例えば、監視対象物がコンテナである場合には、すなわち爆発物等の不審物を予め積み込んだ偽のコンテナと真正なコンテナを入れ替えられたことを検知することである。上述の目的を達成するために、本発明では”Ｈａｇｏｒｏｍｏ”という方式をコンテナの内側に用いて、コンテナを内側から封印するｉｎｓｉｄｅ　ｓｅａｌ（インサイド・シール）とする。ここで、”Ｈａｇｏｒｏｍｏ”方式とは、２００２年２月２５日の米国特許出願（出願番号：１０／０８０，９２７）、および２００２年４月１０日の米国特許出願（出願番号：１０／１１９，３１０）で開示した「対象物に装着された複数個の無線通信ノード間のリンク状態を監視することで、対象物の動きや対象物近傍の所定領域の状態を検知する事、前記のリンク状態が対象物固有のＦｉｎｇｅｒｐｒｉｎｔとしても利用可能である事を特徴とするセンシング方式」である。

コンテナの内壁の広範囲を検知エリアとしてカバーするように、内側からの封印であるｉ

ｎｓｉｄｅ　ｓｅａｌを、Ｈａｇｏｒｏｍｏ方式で実現するとともに、Ｆｉｎｇｅｒｐｒｉｎｔからコンテナ開閉のパスワードを自動生成すること、シール自身が攻撃を受けた場合には、再生不能なＦｉｎｇｅｒｐｒｉｎｔをシール内の記憶から消去することで、前記の各課題が解決される。

第１図には、従来のセンシング方式を示し、第２図には、本発明のＨａｇｏｒｏｍｏ方式の概念が図示されている。例えばコンテナ１１０が監視対象物であり、コンテナ１１０内に貨物１２０が存在する場合、従来のセンシング方式では、壁面等に各種のセンサ、例えばレーザ変位センサー１３０を多数設置し、対象物であるコンテナの扉、内壁の開閉や貨物の移動変化を監視する。しかしながらこの方式ではその監視対象物の特性（材質、表面特性、大きさ等）に合わせてセンサの感度設定、判定しきい値設定、センサの取り付け位置調整、さらに取付け角度調整等を、正確に行なう必要がある。このように監視対象物の属性ごとに監視条件を変更しなければならないとすれば、多種多様な監視対象物を監視する上で、普遍性のある方式とは云い難い。また、このような従来の方式では、センサの取り付け位置は一定にしなければ、センサの取り付けを素人でもできるような取り付けマニュアルを作ることも困難である。しかし、センサの取り付け位置を一定にしていると、センサ自身を攻撃され得るというセキュリティ上の脆弱性が発生する。

そこで本発明によるＨａｇｏｒｏｍｏ方式では、監視対象物であるコンテナの扉や内壁の特性（材質、表面特性、大きさ等）とは無関係に監視が出来るようにする。すなわちコンテナ１１０内の壁面に複数の無線通信装置（通信ノード）１４０を設置する。この無線通信装置は、電波による無線送受信機能を有し、それらは相互に通信可能であり、通信ネットワーク１５０を形成する。そしてこの通信ネットワーク内での任意の２つの通信ノード（以下、ノードと略記することもある）の間における通信特性を求め、その任意の２つのノード間の通信特性のデータをマトリックスの要素とするネットワークグラフマトリックスを作成する。このマトリックスは、コンテナ内におけるノードの配置、コンテナの扉の開閉などの状態、コンテナ内に置かれた積み荷の移動、コンテナ内の空間状態を表現できるものである。本発明では、上述ノード間の通信特性を求めるために、第１実施例では各ノードは、近隣ノードのみと通信可能な微弱電波を出し、他の離れたノードとは近隣ノードを中継ノードとして、メッセージを中継によって転送することで、初めて通信可能な状態におく。そして、任意の２つのノード間で通信を行なうために必要とされるメッセージ中継回数を求め、この中継回数（これをＨＯＰ数という）を、マトリックス要素の値としたネットワークグラフマトリックスを作成する。このネットワークグラフマトリックスの（ｓ，ｐ）要素の値は、ノードｓとノードｐとの間の通信特性を示す。なお、この通信特性を示す情報をノードｓとノードｐの間のリンク情報と言うこともある。ノードを装着したコンテナの扉や壁が変位することで、ネットワークグラフマトリックスが変化するので、ネットワークグラフマトリックスの変化を監視することで、コンテナの状態監視ができる。

また第２実施例では、Ｕｌｔｒａ　Ｗｉｄｅ　Ｂａｎｄ電波（以下、ＵＷＢ電波という）を各ノードから出して、それを受信した他のノードが返信してくる電波を受信し、送信した電波と受信した電波の間の時間差を求め、この時間差を用いて、当該他のノードとの間の距離を求める。この場合、ノード間の距離を求めるための電波が、何らかの物体によって遮蔽されて、距離が求まらない場合もある。また、ノード間に侵入した物体までの、ノードからの距離が求まり、それを侵入物の情報とできる場合もある。ノード間距離を表現するネットワークグラフマトリックスおよびノード近傍での侵入物の有無の情報を監視することで、コンテナの状態監視ができる。

第１実施例では、各ノード間で通信を行なうための各ノードにおける中継回数（ＨＯＰ数）で、または第２実施例では、各ノード間の距離で、ネットワークグラフマトリックスのマトリックス要素の値が表現される。このネットワークグラフマトリックスは、コンテナの扉が閉じられて、鍵がかけられたコンテナでは、ノードの動作停止や脱落またはコンテナ内の荷崩れなどが生じない限り、Ｆｉｎｇｅｒｐｒｉｎｔのように不変であり、コンテナ全体としてのＩＤ情報となり得る。また、人間の指紋において、指紋表面の汚れや傷が

あっても、それらの影響を除去して、指紋による本人照合が可能であるように、上記のネットワークグラフマトリックスは、処理の工夫によって一部のノードの動作停止や脱落があっても、コンテナを照合するためと、コンテナ内の変化の検出に利用可能である。
本発明では、コンテナに貨物が積まれていても空であっても、コンテナの扉が閉鎖された時点のネットワークグラフマトリックス（Ｆｉｎｇｅｒｐｒｉｎｔ）と、その後の輸送途中のネットワークグラフマトリックスを一定の時間間隔または常時、あるいは目的地に到着した時点で比較することにより、少なくともそのコンテナ内に何らかの変化があったか否かを検出する。もしそのような変化を検知したコンテナは、内部で異常な動きがあったと判断して、該コンテナが目的地に到着する前のコンテナ船上、または到着直後のコンテナヤードで、個別の検査を行う等の対応を取ることで、コンテナのセキュリティを確保することが出来る。換言すると本発明は、下記の特性を有する。
１．　コンテナの内部に設けた異常検知のための従来技術によるセンサでは、コンテナ内部でのその取り付け位置などが一定であれば、テロリスト等によって何らかの対策をとられる可能性があるので、本発明によるインサイド・シールではコンテナの内部での通信ノードの取り付け位置は一定位置ではないことを原則とする。一定位置ではないようにするためには、ランダムな位置に設置することや、外部からはわからない規則性にしたがった位置に設置することで実現できる。
２．　本発明ではさらに、扉の開閉用のパスワードをコンテナ運用会社とは別個のセンタで自動生成する。コンテナの運用会社の内部にテロリストの協力者がいて、扉に装着された電子錠の開放用のパスワードをこっそりと入手して、正当な扉の開閉であるかのように偽装されることを防止する。
３．　コンテナ内部に設けたインサイド・シールが攻撃を受けるか、扉の不正開閉を検知した場合には、センターに登録したコンテナのＦｉｎｇｅｒｐｒｉｎｔに対応してコンテナ内に照合用に記録しているＦｉｎｇｅｒｐｒｉｎｔデータを消去する。このＦｉｎｇｅｒｐｒｉｎｔはランダムに発生しているデータを含んでいるので、二度と再生できない。したがって、コンテナを不正開閉したり、偽物のコンテナを用意した場合、正当なコンテナが保持しているべきＦｉｎｇｅｒｐｒｉｎｔが無くなるので、不正コンテナであることがわかる。これにより、不正開閉の検知を、センターに無線通報ができない場合でも、コンテナにＦｉｎｇｅｒｐｒｉｎｔを示させることで不正開閉を受けたコンテナや偽物コンテナがわかる。
４．　さらに本発明では、コンテナの側板、床板、天井板、扉など６つの面のどれであっても、不正開閉だけでなく、ドリルやバーナー、レーザで穴を開けて危険物を投入したり、不審者が侵入することを検知して、その記録を残すセンサーを設置して、局所的な攻撃を検知する。
５．　そしてそのような不正な侵入があったと思われるコンテナが例えば米国内に侵入するのを防止するために、コンテナ輸送途中で本発明に係る監視システムでは、そのコンテナがコンテナ船上に載置されている時にすでに、監視センタに警報信号を送ることが出来る。これにより監視センタはそのコンテナが目的港に到着する前に例えば沿岸警備隊にそのような危険情報を送ることが可能となる。本発明でいう監視対象物は、自動車、コンテナ、家屋、オフィス、工場、病院、倉庫、工作機械などさまざまである。監視対象物の外面や内側面に複数個の無線通信ノードを配置し、無線通信ノード間の通信状態を監視することで、監視対象物の変形（例：ドアの開閉）や、監視対象物の近傍への侵入物の発生や物体の出入りなどを検知できる。言わば、対象物について汎用的なセキュリティ機能を提供するシステムとなる。その中で、以下、特に貨物コンテナに着目して説明する。

発明を実施するための最良の形態

以下、図面を参照して本発明の好適な実施の形態を例示的に詳しく説明する。但しこの実施の形態に記載されている構成部品の寸法、材質、形状、その相対的配置等は特に特定的な記載がないかぎりは、この発明の範囲をそれに限定する趣旨ではなく、単なる説明例にすぎない。
以下この明細書中で用いられる用語を、下記のように定義づける。

１）通信ノード
通信ノードとは通信ネットワークを形成するノードである。
第１実施例に用いられる自己組織型通信ネットワークでは、近隣のノードにのみ通信可能な微弱電波で相互にデータ通信が可能であり、それ以外の遠くの通信ノードとは、微弱電波を受け取ったノードが受信したデータを中継することでデータを送信することが出来る。なおこの中継回数をＨＯＰ数という。
また第２実施例の通信ノードは、ＵＷＢ（Ｕｌｔｒａ　Ｗｉｄｅ　Ｂａｎｄ）電波を用いたデータ通信や距離測定によって、他のノードとの間の距離を求める。
２）制御装置
制御装置とは通信ネットワーク内の通信ノードのうち、いわば親ノードとして機能し、メモリー機能や外部の通信設備とのデータの授受を行なう機能を有する特定のノードをいう。
３）ノード配置情報
ノード配置情報とはネットワーク内の任意の１つのノードが、空間内で他のノードとの関係でどのような配置関係にあるかを示す情報である。その任意の１つのノードから他のノードへのデータ中継回数、その任意の１つのノードから他のノードまでの距離で表すことが出来る。その任意の１つのノードから他のノードに無線通信キャリア（電波、光、音波）が届いているか否かによっても表現することも出来る。本発明の第１実施例では、自己組織通信ネットワークを応用して、任意のノードから他のノードへデータを送るためのデータ中継回数（いわゆるＨＯＰ数）により、このノード配置情報が定義される。これは、任意のノードから他のノードへ至るメッセージ中継回数を表すいわゆるＨＯＰ数テーブルと同義でもある。また本発明の第２実施例ではこのノード配置情報は、任意のノードから他のノードへの距離で定義づけられる。ノード間の距離が測定できているノード間では直接に通信ができるし、他の通信ノードからのキャリアが届いているかどうかを示すノード配置情報において、キャリアが届いていれば、その通信ノードとの間で直接に通信ができる。なおこのノード配置情報から、次に述べる全ノードの他ノードとの配置関係を、ネットワークグラフマトリックスとして求められる。換言すれば、ネットワークグラフマトリックスの、一行または一列がノード配置情報として表現される。
４）監視対象物の状態情報
監視対象物の状態情報とは、▲１▼監視対象物の変形、▲２▼監視対象物の位置、▲３▼監視対象物近傍の物体の分布、▲４▼監視対象物近傍での物体の移動の状態の少なくと１つを示す情報である。
５）ネットワーク構造情報
監視対象物に装着された複数個のノードから構成された無線通信ネットワーク全体の構造を示す情報である。このネットワーク構造情報は、各ノードのノード配置情報を合成することで、ネットワークグラフマトリックスとしても、求められる。
６）ネットワークグラフマトリックス
監視対象物に装着された複数個のノードから構成される無線通信ネットワークの全体構造を、任意の２つのノード間のリンク状態を要素とするマトリックスとして表現したものである。ここで、ノード間のリンク状態とは、ノード間の距離、ノード間でのメッセージ転送が直接できるか否かのフラグ、ノード間での通信速度、ノード間で送受する電波が受信ノードに形成する電界強度など、ノード間の通信の状態を示すものである。
このネットワークグラフマトリックスの（ｓ，ｐ）要素は、第１実施例では、任意の２つのノードｓ，ｐ間で中継無しで直接通信できる場合（ＨＯＰ数がゼロ）を１、ノードｓ，ｐ間で直接通信できず他のノードでの中継を要する場合（ＨＯＰ数が１以上）を０として表現される。また第２実施例では、任意の２つのノードｓ，ｐ間の距離を測定した値でネットワークグラフマトリックスの（ｓ，ｐ）要素が表現される。本発明の監視システムでは、基準となるネットワークグラフマトリックスと、監視時のネットワークグラフマトリックスとを適時比較することで、監視対象物に変化があるか否かがチェックされる。すなわちこの基準となるネットワークグラフマトリックスは、例えばコンテナの出荷時に検知

されたもので、コンテナ内にその後も異常が無ければ不変であるが、何らかの変化があればネットワークグラフマトリックスにも変化が生ずる。

７）Ｆｉｎｇｅｒｐｒｉｎｔ（指紋）

ネットワークグラフマトリックスが表現するネットワークを構成するノードの配置がネットワークごと異なるようにするので、ネットワーク構造を示すマトリックスがネットワークごとの特有のＦｉｎｇｅｒｐｒｉｎｔとなる。そのため、ネットワークグラフマトリックスのことを、Ｆｉｎｇｅｒｐｒｉｎｔと称する場合がある。また、ネットワークグラフマトリックスを構成する各ノードの番号が、ノードごとにランダムに生成され、ネットワークグラフマトリックスの各行と各列に、対応するノードの番号のデータも含ませておけば、ネットワークを構成するノードの配置が全く同じネットワークが他にあったとしても、ネットワークグラフマトリックスは、ネットワークごとに全く異なった特有のものであるＦｉｎｇｅｒｐｒｉｎｔとなる。

本発明に係る監視システムにおける異常検知の原理を以下に説明する。

本発明は、対象物およびその近傍、例えば、貨物コンテナ、事務所、倉庫、工場、家屋等を監視対象とし、監視対象とその近傍領域（監視対象の内側の空間または外側の近傍の空間）を監視する監視システムに関する。便宜上以下は海上輸送用の貨物コンテナ（以下、コンテナと略記することもある）を例として説明を行なうがこれに限定されない。一般にコンテナは、貨物列車、トラック、貨物船、飛行機などの間の積み替えが簡単になるように、積み替え作業車で持ち上げたり降ろすための係合部材が備えられている。また、積み重ねても強度が維持されるとともに、コンテナがずれないようにするための部材もある。さらに、コンテナ内の荷物を降ろしたり、コンテナ内に荷物を積むための出入り口となる扉や蓋もある。本発明はこのコンテナ内で発生する異常状態を”Ｈａｇｏｒｏｍｏ”方式を用いて検知する。”Ｈａｇｏｒｏｍｏ”方式とは、「対象物に装着された複数個の無線通信ノード間のリンク状態を監視することで、対象物の動きや対象物近傍の所定領域の状態を検知する事、前記のリンク状態が対象物固有のＦｉｎｇｅｒｐｒｉｎｔとしても利用可能である事を特徴とするセンシング方式」である。危険物の検知は貨物の積み方や危険物の材質やその梱包の仕方の影響を受けやすい。危険物の特性に適合させて設計されたセンサを用いて、危険物を検知しようとするよりも、危険物を入れられる対象であるコンテナに危険物を搭載する行為に伴って発生するコンテナの“動き”を検出する方が、危険物の特性の影響を受けないで汎用的に異常を検知できる。このコンテナの“動き”の検出もさまざまな材質や構造のコンテナが存在することを考えれば、コンテナ自身の動きを検出するよりも、コンテナに装着した複数個の通信ノードが相互に通信することで、コンテナの“動き”によって生じる“通信ノードの配置の動き”を検出する方がコンテナの材質や構造の影響を受けにくいので、汎用性が高い。

また、コンテナの内部に危険物を後から積み込むのではなく、最初から危険物を積み込んだ偽物コンテナに、コンテナを入れ替えられる場合もある。そのような入れ替えに対応するには、人間の指紋や声紋に該当するような個別コンテナに固有の情報が、コンテナに付随するとともにセンターに登録されていて、センターに登録されている情報とコンテナに付随している情報を照合することで、偽物かどうかを判定できるようにしなければならない。そのためには、コンテナを同定するための固有情報の発生とセンターへの登録が、人間の介在なしに自動的に行われることが重要である。パスワードなどの固有情報の漏洩は、人間から行われることが多いからである。

上記の分析から、課題を解決するための手段は、次のようなものであることが望ましいということがわかる。

対象物に装着した複数個の通信ノードが相互に通信することで、対象物の動きによって生じる“通信ノードの配置の動き”を検出できるとともに、“通信ノードの配置”から対象物を同定できる固有の状態情報が生成できる。

ここで、対象物の動きと、通信ノードの配置の動きについて、説明する。対象物が変形したり、対象物の部分が移動することで、対象物に配置した通信ノードの配置の動きを、次のようにして検出する。すなわち、対象物の各部分に通信機能を持ったノード（通信ノー

ド）を複数個、分散して配置する。この各通信ノードが通信をして、通信ノードのノード配置情報を通信ノードごとに生成し、各通信ノードごとのノード配置情報を総合して、対象物上の全通信ノードで構成されるネットワークの構造を示すネットワーク構造情報を生成する。たとえば、特定の通信ノードを中心ノードに設定して、その中心ノードからの距離を各通信ノードが、中心ノードからその通信ノードまでの電波の到達時間によって計測して中心ノードに報告することで、中心ノードから各通信ノードまでの距離として表現されたノード配置情報を得ることもできる。また、座標が既知の通信ノードを複数個、基準ノードとして、各基準ノードと各通信ノードまでの距離を計測し、各基準ノードを中心として計測した距離を半径とした円または球の交点として、各通信ノードの座標を求める。そして各通信ノードの座標データとしてネットワーク構造情報を生成することもできる。

さらに、中心ノードや基準ノードというものを設けずに、各通信ノードが、それぞれ他の通信ノードとのリンク情報（直接に通信できるかどうかという符号でも良いし、他の通信ノードと通信する場合に必要な中継ノード数でも良いし、直接通信するのに必要な電波の送信電力でも良いし、電波の到達時間でも良いし、電波の到達時間から換算した距離でも良い）を検出し、自通信ノードから他の通信ノードまでのリンク情報をまとめたものをノード配置情報とし、ノード配置情報を総合して得たネットワーク構造情報を、対象物の固有の状態情報としても良い。ネットワーク構造情報は、対象物への通信ノードの配置が対象物に固有のものであったり、通信ノードに付与したノード番号の組み合わせが対象物に固有であれば、対象物を同定できる固有の状態情報にもなる。

上述の通信ノード間のリンク情報は、本発明の第１実施例ではノード間の微弱電波により直接通信できるか、それとも他のノードを中継して初めて通信できるか、により検知できるし、また第２実施例ではＵＷＢ電波によって測定したノード間距離として検知することができる。

すなわちノード配置情報を得る方法の一例として、本発明の第１実施例に示す自己組織型ネットワークに関する米国特許６，０２８，８５７がある。この自己組織型ネットワークとは複数のノード間における通信リレーシステムで、各通信ノードは、微弱な電波で通信するように設定されているので、各通信ノードは近傍の通信ノードとのみ直接の通信ができる。各通信ノードは自己組織により、自ノードから他の任意のノードにメッセージを伝送するために必要とされるメッセージ中継回数を示すテーブル（Ｈｏｐ数テーブル）を作成する。このＨｏｐ数テーブルは、ノード配置情報である。

ノード配置情報を得る他の方法は、本発明の第２実施例に示すＵｌｔｒａ　Ｗｉｄｅｂａｎｄ（ＵＷＢ）を使用し、ノード間の具体的距離（例えば何センチメートルの距離）を測定する方法である。このＵＷＢ技術によると、例えばコンテナ等の閉空間内に設置された複数のノード間の距離を次のようにして測定する。送信ノードからＵＷＢ電波で距離測定用の信号を送信する。受信ノードで、この距離測定用の信号を受信後、受信ノードは送信ノードに信号を送り返す。そして、送信ノードでは送り返された信号を受信して、距離測定用の信号の送信時刻と、受信ノードから送り返された信号を送信ノードが受信した時刻の時間差を計測することにより、ノード間の距離を算出することが出来る。この算出された各々のノード間の距離をベースとしたそのコンテナ独自のネットワークグラフマトリックスを作ることが出来る。このネットワークグラフマトリックスでのマトリックス要素は、ノード間の距離を値に持つ。そして、このネットワークグラフマトリックスは、上述の”Ｆｉｎｇｅｒｐｒｉｎｔ”となり得る。この場合、そのコンテナ内に不正に侵入した人間、不正に搬入または搬出された物体があると、コンテナ内での電波の伝播状況が変化する。その結果、ノード間の距離の計測ができなくなったりする。また、コンテナの扉が開閉されると、ノード間の距離が変化して、ネットワークグラフマトリックスも変化する。

第３図には本発明に係る対象物の状態監視システム２００のシステム構成が示されている。コンテナ２０１内部にはその壁面に複数のノード２１１で形成された通信ネットワーク２１０が設けられ、これを用いて前述の”Ｈａｇｏｒｏｍｏ”方式でコンテナ内を監視している。該コンテナ２０１は、通常のコンテナに各種の電子機器を装備したものである。この通信ネットワーク２１０については、さらに詳細に述べるが、この通信ネットワーク

のネットワーク構造情報として検知されたコンテナの状態情報は制御装置２２０、そして外部アンテナ２４０を経由して監視センター２３０へ送られる。監視センター２３０では、コンテナ２０１から送られた状態情報に基づき異常状態と判断した場合には例えばクレーンのオペレータ２８０に対して、その異常状態と判断されたコンテナ２０１をコンテナヤード内の特別な場所へ移動し、さらに詳細な検査を行なうべく指示が出される。一方、異常がないと判断された際には、監視センタ２３０から無線で電子ロック解除用ソフトが電子ロック装置２５０へ送られ、そのソフトがインストールされる。そして監視センターからは別途コンテナのオペレータ２８０に対して例えば電話や電子メールで電子ロック装置２５０の電子ロック解除のためのパスワードが送られ、オペレータ２８０によりマニュアルでパスワードを入力後、コンテナ２０１のドア２６０が開放される。

一般にコンテナ２０１の内部は、第２９図（Ａ），第２９図（Ｂ）に示すようにコンテナの内壁は溝が繰り返す蛇腹のような構造をしているので、配線を壁にしっかりと密着させて固定するには工夫がいる。もし、配線が壁に密着していなければ、コンテナ内で荷物の積み下ろし作業をしている際に、配線をひっかけて傷つけることも頻発する。したがって、通信ネットワーク２０１の複数の通信端末（通信ノード）を壁などに接着剤またはボルトで固定し、通信端末からの通信情報は無線でコンテナ内の制御装置２２０に収集するという方式が考えられる。その場合、各通信ノードは内蔵の電池で駆動されることになる。しかし、通信ノードにそれぞれ小さな電池を内蔵させていると、必要な期間だけ通信ノードを動作させるのには電池の容量が不足するという問題や、電池の取り替えのときに全ての通信ノードの電池交換の手間がかかるという問題も発生する。したがって、各通信ノードに内蔵する電池として、充分な容量のものがあれば各通信ノードが電池を保持するという方式を採用するし、そうでなければ、制御装置２２０に大容量の電池を内蔵させ、各通信ノードを制御装置２２０からの電源ケーブルに接続して電源供給するという方式を採用する。制御装置２２０から通信ノードに電源ケーブルで電源供給をする場合、電源ケーブルはコンテナの内壁の凹凸の凹の部分に配線するようにして、コンテナ内に荷物を積み込む時に、ケーブルが損傷する確率が小さくなるようにする。コンテナ内という作業環境が悪い場所で、通信ノードを設置する場合を考えると、設置位置を厳密に規定するような方法であると、設置コストが高くなりすぎる。また、設置はランダムである方がセキュリティ対策としても優れているので、通信端末（通信ノード）の設置位置はほぼ自由に選べるものである必要が生じる。このように自由な位置に設置した通信ノードからの情報を制御装置に無線で収集するための通信ネットワークをコンテナ内に構築するためには、無線通信ネットワークの自己組織化機能が必要となる。

またコンテナ２０１の壁（側板、天井、扉、床板）は、厚さが約２ｍｍのアルミまたはスチールでできているが、ドリルやバーナーで穴を開けることは可能である。特に、最近はコンテナの軽量化が行なわれているので、穴はさらに開け易くなっていると思われる。そこで、コンテナの扉の開閉検知以外にも、コンテナの壁に穴を開けようとする行為を検知しなければならない。コンテナの外部から側板、天井、扉、床板などにドリル、バーナー、レーザーで穴を開けようとする行為を検出するのに、振動センサ，温度センサを用いることもできる。振動センサとしては、オムロンの形Ｄ７Ｆ－Ｃ０１がある。これを改造して、動作温度範囲を広げるとともに、コンテナの側板などの蛇腹構造の溝部分にボルトや接着剤で装着することができるように薄い構造で底面で装着するタイプにすれば良い。例えば、特開平６－１６２３５３（オムロン株式会社）にはこのような振動センサが開示されている。

さらにコンテナの内部は、輸送中や保管中に周囲の気温や日射によって、－３０度Ｃから＋８０度Ｃまで変化する。したがって、コンテナの内部で動作するこれらのセンサおよび後述の通信ノードは広い温度範囲で長時間、動作可能な電池やマイコンおよび周辺回路を必要とする。例えば、電池としては松下電工のＢＲ２４７７Ａ（耐高温フッ化黒鉛リチューム電池）が使用可能である。この動作温度範囲は、－４０度Ｃから１２５度Ｃであり、出力電圧３Ｖである。さらに通信ノードや制御装置２２０のマイコンとしては、三菱電機のＭ３２Ｒ／ＥＣＵシリーズが使用可能である。これは、動作温度範囲が－４０度Ｃから

＋８０度Ｃであり、電源電圧が３．３Ｖである。
また連続でこのマイコンをＢＲ２４７７Ａ（耐高温フッ化黒鉛リチューム電池）を電源として動作させた場合、短時間で全エネルギーを消費してしまうので、超低消費電力のタイマー回路を用いて、定期的にマイコンを内蔵する通信ノード、制御装置２２０およびそれらに接続されたセンサに通電して起動する必要がある。コンテナ内に設置する通信ノード、センサおよび制御装置は動作温度範囲を広く設定するとともに、各々が動作温度範囲の広い電池を内蔵したものとする。そして、通信ノードのうちのいくつかにはドリルでの穴あけ検知用の振動センサを接続したものとする。同様に、バーナーでの穴あけ検知用の温度センサを接続させた通信ノードとしても良い。
第３図に示すようにコンテナ２０１の内部には、通信ノード２１１はコンテナの内壁にランダムに装着される。ただし、扉の開閉検知をするために、第４図に示す左右の扉２６０，２６０のそれぞれに、少なくとも１個は通信ノードを配置する必要がある。第４図において、制御装置２２０とケーブルで接続された電磁誘導型ＲＦＩＤタグ４１１が、左右の扉の継ぎ目の防水ゴム帯４１０に接してコンテナの内側に設置される。防水ゴム帯４１０に接してコンテナの外側には、電磁誘導型のＲＦＩＤアンテナ４１２（コンテナの外側）が設置される。電磁誘導型ＲＦＩＤタグ４１１と電磁誘導型のＲＦＩＤアンテナ４１２とは、コンテナの扉２６０が閉鎖された状態では防水ゴム帯４１０を挟んで対向する位置になるように設置する。これにより、電磁誘導型のＲＦＩＤアンテナと電磁誘導型ＲＦＩＤタグとは、防水ゴム帯４１０によりコンテナの扉２６０が防水性能を保った状態で閉鎖されていても相互に電磁誘導によって通信ができる。電磁誘導型のＲＦＩＤアンテナ４１２には図示しない無線送受信装置が接続されていて、電磁誘導型のＲＦＩＤ４１２と遠隔通信用アンテナ４１３の間を中継する。図示しない前記無線送受信装置の働きで、コンテナ内部からの情報は制御装置２２０から電磁誘導型ＲＦＩＤタグ４１１に伝達され、さらに電磁誘導型ＲＦＩＤタグ４１１から電磁誘導型ＲＦＩＤアンテナに行き、そこから図示しない前記無線送受信装置を経て、遠隔通信用アンテナ４１３にてコンテナから離れた場所に伝送される。コンテナの外部からの情報は、これと逆の経路をたどって、制御装置２２０に至る。
コンテナ内の通信ネットワーク
第２図に示すような無線通信機能を持った複数の通信ノード１４０が、監視対象であるコンテナ内部の扉や壁や天井に配置されて、第５図（Ａ）、第５図（Ｂ）に示すような通信ネットワーク５００、５００‘を形成している。この通信ネットワークは、所定周期のタイミングで、通信ネットワークのネットワーク構造情報である、第６図（Ａ）、第６図（Ｂ）に示すネットワークグラフマトリックス６００、６００’を生成する。コンテナの扉を閉鎖した後、最初に生成されるネットワークグラフマトリックスは、通信ネットワークごとに固有の情報となる。この通信ネットワーク５００，５００‘、およびネットワークグラフマトリックス６００、６００’については詳細に後述する。
制御装置２２０は、コンテナの内部にあり、コンテナ内の通信ネットワーク２１０の各通信ノードと無線によってデータ通信をしたり、通信ノード間のリンク情報を検知する通信ノードの１つとなる。制御装置２２０の指令に応じて、コンテナ内の通信ネットワークは通信ネットワークの自己組織化をする。ここで言う自己組織化とは、各通信ノードが自ノードからみた他のノードとの関係を示すノード配置情報を生成することである。このノード配置情報を米国特許６，０２８，８５７におけるＨｏｐ数テーブルと同様に用いて、通信ノード間の通信経路を決定できる。自己組織化によって生成したノード配置情報を、各通信ノードは他の通信ノードに通報する。各通信ノードでは他の通信ノードから得たノード配置情報を総合して、それぞれネットワークグラフマトリックスを生成する。各通信ノードで生成さえるネットワークグラフマトリックスは同一になるはずである。制御装置２２０が、コンテナ内の通信ネットワークの初期化指令を発すると、コンテナ内の通信ネットワークは、初期ネットワークグラフマトリックスを生成して、各通信ノードで記憶する。したがって、制御装置２２０も初期ネットワークグラフマトリックスを記憶することになる。制御装置２２０は送受信機能を持っており、第４図に示すコンテナの左右の扉の継

ぎ目の防水ゴム帯４１０を内側と外側からはさむように設置された電磁誘導型のＲＦＩＤタグ４１１とＲＦＩＤアンテナ４１２を用いてコンテナ内外の通信を電磁誘導によって実行する。

制御装置２２０は、コンテナに荷物を積んでも積まなくても、扉を閉めた後に外部から初期化指令を受け取ると、各通信ノードに初期化指令を与え、その後、さらにネットワークグラフマトリックスの生成を、各通信ノードに指令する。制御装置２２０へ与えられる初期化指令は、外部の専用端末で発信した電波によって、遠隔通信用アンテナ４１３を通じて、伝えられる。これにより、通信ネットワークの各通信ノード２１１は他の通信ノードと通信をして、ネットワークグラフマトリックスを６００生成する。このネットワークグラフマトリックスを受け取った制御装置２２０は、これを第４図に示す電磁誘導によるコンテナ内外の通信手段を使用して、無線で監視センター２３０に通報する。監視センター２３０は、受信したこれらの情報を、そのコンテナの特有の情報として記憶する。すなわちコンテナの扉を閉鎖した後、最初に生成されるネットワークグラフマトリックス６００は、通信ネットワーク２１０ごとに固有の情報となる。

出荷地を出発したコンテナ内では仕向港または仕向地に到着するまで、所定の時間間隔で上述のネットワークグラフマトリックスが生成され、各通信ノードに記憶される。

通信ネットワーク内での異常検知

通信ネットワーク２１０内での異常検知は、本発明では２つの方法により行なわれる。すなわち実施例１では、各通信ノード間のリンク情報を自己組織型無線通信ネットワーク内のメッセージ中継回数を示すＨＯＰ数で定義し、実施例２ではＵＷＢ（Ｕｌｔｒａ　Ｗｉｄｅｂａｎｄ）電波を用いて測定された通信ノード間の距離で定義する。そして、任意の２つの通信ノード間のリンク情報をマトリックス要素とするネットワークグラフマトリックスを生成する。このネットワークグラフマトリックスは、コンテナの扉を閉じた直後に生成されて、Ｆｉｎｇｅｒｐｒｉｎｔとして監視センターおよび通信ノードに記憶される。そして、その後、ネットワークグラフマトリックスは定期的に生成されて、前記のＦｉｎｇｅｒｐｒｉｎｔとしての初期ネットワークグラフマトリックスと比較される。この比較の結果、変化したノード間リンクの個数または個数の割合が、所定値を越えていた場合には、異常発生と判断する。異常発生と判断された中で、さらに所定の条件（例：動作停止した通信ノードが短時間の間に急増したり、変化したノード間リンクの個数がさらに大きな所定値を越えたという条件）を満たした場合には、コンテナを監視する通信ネットワーク２０１に攻撃があったと判断する。攻撃があった場合には、Ｆｉｎｇｅｒｐｒｉｎｔおよび通信ノードのノード番号を消去して、再生不能にする。これにより、監視センターにそのコンテナ管理番号のものとして登録されているＦｉｎｇｅｒｐｒｉｎｔをコンテナは保持できなくなり、異常コンテナであるという事実を隠せなくなる。

本発明による監視のための処理手順

第２２図、第２３図、および第２４図は、第３図に示す本発明に係る監視システム２００における処理手順を示すフローチャートであり、実施例１にも実施例２にも共通する。このうち第２２図は、本発明において、コンテナにノードを設置してコンテナ内のＦｉｎｇｅｒｐｒｉｎｔを生成して登録後、コンテナを輸送し、目的地に到着して扉を開けるまでを示す処理フローチャートである。第２３図は、本発明の各ノードにおける処理手順を示すフローチャートである。第２４図は、本発明の制御装置２２０における処理手順を示すフローチャートである。

まず第２２図に示すように、コンテナ内に荷物を積み込む前に、作業員が、コンテナ内に通信ノード、制御装置２２０および電磁誘導型ＲＦＩＤタグ４１１を設置し、コンテナの扉に電磁誘導型ＲＦＩＤアンテナ４１２と無線送受信機と遠隔通信用アンテナ４１３を設置する（ＳＴ２２０１）。これらの装置を、コンテナ運送業者の作業員が、設置するか、すでに設置されてるものについてバッテリ交換、動作確認、修理などをして稼動可能な状態にする。　コンテナ運送業者の作業員がこのような作業をしない場合には、荷主の作業員が、このような作業を実行する。この作業が終わったら、コンテナの扉を一時的に閉めて、コンテナを荷主の場所に搬送する。（ただし、空コンテナを回送する場合には、コン

テナには荷主はいないので、荷主の場所に搬送するということは省略される。）
荷主の場所で荷物が積み終わったら、作業員はコンテナの扉を閉鎖する。（ＳＴ２２０２）。
次に作業員が制御装置に初期化指令を与える（ＳＴ２２０３）。この指令は、作業員が所持する無線端末を用いて、コンテナ管理番号を指定した初期化指令の無線信号として発信される。そして、第３図のアンテナ２４０（第４図での遠隔通信用アンテナ４１３）で直接に受信され、すでに述べた経路で、コンテナ内の制御装置２２０に伝達される。この無線端末が携帯電話であれば、無線端末からの初期化指令の無線信号はコンテナ管理番号とともに基地局に伝送され、次に伝送された信号をもとに基地局から指定されたコンテナ管理番号のコンテナを宛て先とする初期化指令信号として発信される。発信された初期化指令信号は、アンテナ２４０を通じて前述の経路で、制御装置２２０に伝達される。制御装置は、あらかじめコンテナ管理番号を記憶しており、受信した初期化指令信号は自分宛のものかどうかを、初期化指令信号に付随したコンテナ管理番号と自分のコンテナ管理番号が一致するかどうかを判断する。コンテナ管理番号が一致して、自分宛の初期化指令信号であれば、その後の動作をして初期化を実行する。自分宛の初期化指令信号でなければ、無視する。（初期化指令信号を与えられた後の制御装置は、第２４図に示す処理フローを実行する。そして、同時に、通信ノードは第２３図に示す処理フローにて動作する。）
自コンテナ宛の初期化指令信号を与えられた制御装置は、第２４図のＳＴ２４０１の判断がＹｅｓとなり、ＳＴ２４０５を実行して、他の通信ノードに初期化指令信号を発する。各通信ノードは、第２３図の処理フローを実行する。制御装置からの初期化指令信号を受けると、ＳＴ２３０１の判断がＹｅｓとなり、ＳＴ２３０５を実行する。ＳＴ２３０５では、乱数を用いて自ノードのノード番号（ＩＤ番号とも言う）を設定する。なおＩＤ番号の桁数は、通信ネットワーク内にＩＤ番号の重複が起こる確率が無視できる程度の桁数とする。次に実行するＳＴ２３０６では、さらに処理Ａとして、各通信ノードは相互間の通信により、上述の自己組織型の通信ネットワークを用いる実施例１では他ノードまでのＨｏｐ数テーブルを作成して記憶する。Ｈｏｐ数テーブルとは他ノードと通信するための中継回数を示したデータである。またＵＷＢ通信を用いてノード間距離を求める実施例２では、他ノードとの距離データを作成して記憶する。
次に、制御装置は第２４図のＳＴ２４０５の次にＳＴ２４０６を実行して、各通信ノードに初期ネットワークグラフマトリックスの生成を指令する。初期ネットワークグラフマトリックスの生成指令を受信した通信ノードは、第２３図のＳＴ２３０２での判断がＹｅｓとなり、ＳＴ２３０７を実行する。実施例１ではノード配置情報としてこのＨｏｐ数テーブルを収集し、実施例２ではノード配置情報として他の通信ノードとの距離データを全て収集する。また、自通信ノードが生成したノード配置情報を他の通信ノードに送信する。ＳＴ２３０７が終わると、各通信ノードは、他の通信ノードから集めたノード配置情報を総合して、それぞれがネットワークグラフマトリックスを作成する（ＳＴ２３０８）。このようにするのは、どの通信ノードが動作停止しても、ネットワークグラフマトリックスの作成がシステム全体としては可能であるようにするためである。
この出荷時のネットワークグラフマトリックスを初期ネットワークグラフマトリックスとして、制御装置がＧＰＳ受信機から得たコンテナの位置と、時計から得た時刻の情報を、コンテナ管理番号とともに、監視センター２３０に暗号化して送信して登録する。（ＳＴ２４０７）。この時、この初期ネットワークグラフマトリックスとは、実施例１では第６図（Ａ）、実施例２では第１５図（Ａ）に示されたマトリックスである。
その後コンテナが出荷地を出発した後、一定の時間間隔で制御装置はネットワークグラフマトリックスの生成指令を各通信ノードに発信する（ＳＴ２４０２，ＳＴ２４０８）。
ネットワークグラフマトリックスの生成指令を受けた各通信ノードは、ネットワークグラフマトリックスを生成し、初期ネットワークグラフマトリックスと比較して差異を検出する。（ＳＴ２３０３，ＳＴ２３０９）。そして、最初に検出した差異であるかまたは、前回とは異なる差異の検出の場合には、差異を各通信ノードで時系列に記録する（ＳＴ２３０９）。またその差異を監視センタ１０に送ってよい。具体的には実施例１では第６図（

Ａ）と第６図（Ｂ）に示したネットワークグラフマトリックスを比較し、実施例２では第１６図（Ａ）と第１６図（Ｂ）に示したネットワークグラフマトリックスを比較する。
なお各通信ノードは、他の各通信ノードで検出した差異のデータを集計して、自己が多数決論理からみて間違っていると判断した場合には、自ノードのＩＤ番号付きのエラーメッセージを他の通信ノードに送信するとともに、自ノードでの差異データ記録を正しい差異データに修復する（ＳＴ２３１３）。そして監視用のネットワークグラフマトリックスは、目的地（例：仕向港）に到着するまで一定時間経過毎に繰り返し継続して行なわれ、ネットワークグラフマトリックスの差異データは蓄積される（ＳＴ２４０２，ＳＴ２４０８，ＳＴ２３０３，ＳＴ２３０９）。
初期ネットワークグラフマトリックスと、現在の監視用に生成したネットワークグラフマトリックスの差異が、所定基準を満たすほどに大きい場合には、コンテナまたはコンテナを監視している通信ネットワークに対する攻撃ありと判断する（ＳＴ２３１１）。ここで、「大きなネットワークグラフマトリックスの差異」には、所定割合以上の通信ノードとの通信が直接にも間接にもできなくなった場合が該当する。また、ネットワークグラフマトリックスのマトリックス要素の値（実施例１では１または０、実施例２では通信ノード間の距離）が変化したマトリックス要素の個数が所定割合以上となった場合もこれに該当する。
なおＳＴ２３１０で、ネットワークグラフマトリックスと初期ネットワークグラフマトリックスを比較して、コンテナへの不正侵入や通信ネットワークへの攻撃であると判断できる場合には、防御措置として次のことを行なう。
▲１▼各通信ノードは自己の保持しているネットワークグラフマトリックス（初期ネットワークグラフマトリックスおよび現時点のネットワークの状態を示すネットワークグラフマトリックスのデータ）を消去する。（ＳＴ２３１１）
▲２▼他の通信ノードに対して、ネットワークグラフマトリックスを消去する指令をそれぞれの通信ノード示発信する。（ＳＴ２３１２）
他の通信ノードからネットワークグラフマトリックスの消去指令が受信された場合にはそれに従う。（ＳＴ２３０４，ＳＴ２３１４）
次に、監視対象物、例えばコンテナが目的地の港に到着したときのコンテナの取り扱いについて説明する。第３図に示すように、目的地に到着したコンテナは、まずコンテナヤードでクレーン２７０で把持したり、吊り上げられて移動する。クレーンは、コンテナを移動させる前または移動途中に無線でコンテナの制御装置２２０と通信して、コンテナから初期ネットワークグラフマトリックスと、それを監視センター２３０に通報した時の時刻の情報およびコンテナの管理番号を読み出す（ＳＴ２２０５）。あるいはネットワークグラフマトリックスのヒストリーデータでも良い。この際、データは暗号化してクレーンに送られる。
上記のデータを読み取るクレーンは、読み取り不能（データが全て消去されている場合など）の場合には（ＳＴ２２０６）危険なコンテナと判断する（ＳＴ２２０８）。また、読み取りが成功した場合には、読み取ったデータをクレーンは監視センター２３０に送信する。監視センター２３０では、そのコンテナについてあらかじめ登録しているデータと読み取ったデータを比較する（ＳＴ２２０７）。比較した結果、クレーンから送られてきた初期ネットワークマトリックスが、あらかじめ監視センター２３０に登録されていた情報と不一致の場合には、危険なコンテナであると、監視センター２３０は判断してクレーンに通報する。また、初期ネットワークマトリックスと、ネットワークマトリックスのヒストリーを比較した結果、例えば、扉に取り付けていた通信ノードの位置が基準値よりも大きく移動していることが判明した場合にも、扉の不正な開閉があったとして、監視センター２３０はこのコンテナを危険なものと判断する。そして、監視センター２３０はクレーンに危険なコンテナであるとの通報をする。危険なコンテナであるとの判断結果となったコンテナについて、クレーンは危険コンテナを所定の場所に移すなどの所定の対応動作をする（ＳＴ２２０８）。
次に上記のステップで安全であると確認されたコンテナは、クレーンで降ろされたコンテ

ナの扉を開ける場合、電子ロック２５０が装着されているので、パスワードを入力しなければ開けることはできない。このパスワードは、監視センター２３０が初期ネットワークグラフマトリックスと、それを監視センター２３０に通報した時の時刻の情報から自動生成したものである。監視センター２３０は、このパスワードに対応する電子ロック用ソフトウェアまたはデータを、制御装置を通じて該当コンテナの電子ロックにダウンロードする（ＳＴ２２０９）。このダウンロードは、コンテナが目的地に到着して安全と確認された後が良い。このダウンロードを行なった後に、監視センター２３０は無線でそのコンテナの扉を開ける権限のある者（受取人、税関職員など）の携帯電話に電子ロックを解除するために、ダウンロードされたソフトウェアに対応するパスワードを通知する（ＳＴ２２１０）。このようにして、パスワードの通知を受けた者が、コンテナの扉を開けることができる（ＳＴ２２１１）。なおこのようにすることで、監視センター２３０はコンテナの扉を開ける者の範囲を管理することができる。

実施例１

自己組織型無線通信ネットワークを用いて、各通信ノードは、省電力のためと、通信ノード間の通信リンクが通信ノードの空間的な配置を表現できるようにするために、微弱な電波で通信するように設定している。その結果、各通信ノードは近傍の通信ノードとのみ直接の通信ができる。この自己組織型無線通信ネットワークについてはＵＳＰＮ６，０２８，８５７に開示されている。

まずコンテナ内に設置する通信ネットワークについて述べる。コンテナの内側の壁面や扉の部分に通信機能を有するノード（通信ノード）を多数、分散配置する。荷主が通信ノードを配置することが可能な場合には、コンテナ内の積荷にも配置しても良い。空コンテナや、荷主が通信ノードを配置できずコンテナ運送業者が通信ノードを配置するコンテナでは、積み荷には通信ノードは配置されない。この通信ノードは、各々が他の通信ノードと通信しながら通信ノードのノード配置情報を生成し、そのノード配置情報を各通信ノードから集めて、総合して、ネットワーク構造情報を生成する。またノード配置情報を用いて、通信ノード間の通信経路を決定する通信ネットワークを形成するものである。各通信ノードは、少なくとも次の１から４の機能を持つ。

１．ＩＤ記憶機能（通信ノードのノード番号を記憶する機能である）

２．すぐ近くの通信ノードとの無線通信機能

３．バッテリによる電源自給機能

４．隣接の通信ノードをたどって、他の通信ノードと通信する場合の他の通信ノードによる中継数を意味するＨｏｐ数を、コンテナ内の全通信ノードに関して記憶したコストテーブル（Ｈｏｐ数テーブルとも言う）を保持する機能

オプションとして、下記の機能５を備えた場合、この通信ネットワークはセンサーネットワークとなる。

５．その通信ノード位置におけるローカルな状態のセンシング機能（例：加速度、振動、温度、特定のガス濃度などを、センシング対象の信号に応じたセンサをその通信ノードに接続して検出する）

遠隔の通信ノードとの通信は、その通信ノードと自己との間にある通信ノードによる中継によって行われる。すなわち、各通信ノードは、他通信ノードからのメッセージが所定強度以上の電界強度で受信された場合に、動作する。相互に、相手通信ノードからのメッセージの電界強度が所定強度以上の場合、自通信ノードと相手通信ノードとの間にリンクを設定する。このようにして、通信ノード間のリンクを設定すると、第５図（Ａ）に示すようなグラフが形成される。これが上述のネットワークグラフ５００と呼ばれるものである。また、ネットワークグラフを構成する各通信ノードｐとｓにおいて、通信ノードｐとｓの間に直接のリンクがあれば、値が１となり、直接のリンクが無く他のノードを中継して通信が行なわれる場合を値が０となるようなマトリックス　Ｍ（ｐ，ｓ）が上述の第６図（Ａ）に示すネットワークグラフマトリックス６００である。

たとえば、通信ノード８８と３６０のあたりにあるヒンジを支点として外部に向かって開くような扉の場合、扉が開くと次のようなリンク群は、通信ノード間距離が大きくなるた

め、自通信ノードから送信した電波が相手の通信ノード上に形成する電界強度が所定値未満となるので、通信できなくなり消える。
消滅するリンク群：
｛Ｌｉｎｋ（１３２，１０），Ｌｉｎｋ（４４９，１０），Ｌｉｎｋ（４４９，９１）｝
また、扉が引き戸であった場合、今までコンテナ内では遠かった通信ノードが逆に近くなって新たなリンクが形成されることも有り得る。コンテナの扉のみが開閉の対象となるとは限らない。コンテナの内部に危険物を入れようとする者が、閉鎖されている扉を避けて、コンテナの通風口，側板をはずして内部に侵入したり何かを入れる可能性もある。そのような場合でも、上記と同様に通信ノード間のリンクに変化が生じる。通信ノード間のリンクの状況は、ネットワークグラフマトリックスの変化として現われる。
この結果、コンテナ内の第５図（Ａ）のネットワークグラフ５００で生成された第６図（Ａ）のネットワークグラフマトリックス６００は、扉が開放された時の第５図（Ｂ）に示すネットワークグラフ５００‘で生成された第６図（Ｂ）のネットワークグラフマトリックス６００’へ変化する。従ってコンテナに貨物を積み込んで閉鎖した時のネットワークグラフマトリックスと、現在のネットワークグラフマトリックスが異なるということは、コンテナに異常が発生した可能性があることとなる。具体的には第６図（Ｂ）に示すように、通信ノード１３２と１０間、　通信ノード４４９と１０間、および通信ノード４４９と９１間では、値が１から０へ変化する。
上述のようにＵＳＰＮ６，０２８，８５７で開示されている自己組織型無線通信ネットワークでは、いわゆるＨＯＰ数と呼ばれる通信中継回数を用いてノード間の通信が制御されている。本発明による実施例１では、コンテナの扉が閉まった状態でドアとそれに対向するコンテナ本体に設けられた通信ノードでは、直接通信ができるためＨＯＰ数が０である。これに対して、ドアが開けられると該当する通信ノード間の距離が広くなり、直接通信ができず、従って他の通信ノードを経由して初めて該当ノード間で通信が出来るためにＨＯＰ数が変化する。Ｈｏｐ数が変化すると、ネットワークグラフマトリックスが第６図（Ａ）の６００から第６図（Ｂ）の６００‘へ変化する。この変化は、コンテナが例えば仕向港のコンテナヤードで、現在のネットワークグラフマトリックスを、初期ネットワークグラフマトリックスと比較することでコンテナ内に異常があったか否かが検出される。すなわちネットワーク構造情報がＨＯＰ数から求められたネットワークグラフマトリックスで求められる。
なお上述の例はドアの開閉のみを説明したが、これに限らず例えばコンテナ内にそれまで無かった不審物を持ち込まれた場合、あるいは逆に荷物を持ち出された場合にも、出入りした物が通信ノード間の通信に影響を与える位置や大きさであれば、その前後で各通信ノード間の通信状態が変化し、結果としてＨＯＰ数が変化する。このためにこれらの異常事態を示すネットワーク構造情報が第６図のネットワークグラフマトリックス６００‘として検知することができる場合もある。通信ノードを多数配置し、様々な通信ノード間にリンクが発生するようにした場合、コンテナへの物の出入りが、ネットワークグラフマトリックスの値に反映できるようになる。
コンテナに貨物を積み込んで閉鎖した時のネットワークグラフマトリックスと、現在のネットワークグラフマトリックスが異なるということは、コンテナに異常が発生した可能性があることを示す。
実施例２
実施例２の処理手順は、第２２図、第２３図、および第２４図は、第３図に示す本発明に係る監視システム２００における処理手順において、ＳＴ２３０９の部分を第１３図に示す処理として実現することで、通信ノードに生じ得る問題状況（通信ノード間の障害物、通信ノードの動作停止、通信ノード脱落、直接波の遮断と反射波の伝播）が発生してもロバストに、その機能を維持することを特徴としている。これらの特徴は、通信ノード間の距離が計測できることに起因してもたらされている。
本実施例では第７図に示すような通信ネットワーク２１０のネットワーク構造情報が、各通信ノード間でＵＷＢ電波を用いて通信を直接行なうことにより求められる。すなわち、

あるノードＡから所定のデータが他の全ノードＢ１、Ｂ２，…Ｂｎに対して送信される。そのデータを受け取ったノードＢ１、Ｂ２，…Ｂｎは受信したデータを直ちにノードＡに送り返し、ノードＡでは発信時と受信時の時間差から距離が算出される。この距離の算出方法については後で詳述する。この各ノード間の距離によりネットワークグラフマトリックスが表され、実施例１と同様に初期ネットワークグラフマトリックスと、その後、定期的に測定されたネットワークグラフマトリックスを比較することで、コンテナ内の変化を検知することで異常の有無が判断される。このＵＷＢによる距離測定は、必ずしもノード間の直接波による通信が行なわれるとは限らず、コンテナ壁面からの反射波により通信が行なわれる場合もあるが、一旦荷物が積み込まれれば、通信の状況は不変の筈であり、通信ノード間の距離の測定値が変化したことは、コンテナ内に何らかの変化があったものと推測することが可能となる。

上述のように本実施例では、ＵＷＢ電波を用いて通信ノードが相互に通信をして、通信ノード相互間の距離を計測する。そして、通信ノード間距離を用いて作成したネットワーク構造情報の変化から、通信ノードを装着された対象物であるコンテナの変形（例：扉の開閉、側板の取り外し、窓の開閉など）を検知する。しかし、ネットワーク構造情報の変化をもたらすものには、対象物の変形以外に、次の（１）、（２）、（３）、（４）の場合がある。これらの場合があっても、ネットワーク構造情報の変化から対象物の変形を検出しなければならない。

（１）　通信ノード間の通信を不能とする障害物が一部の通信ノード間に発生する場合、ネットワーク構造情報に欠落が生じる（第８図）。

（２）　一部の通信ノードが電池切れや衝撃によって動作停止した場合、ネットワーク構造情報に欠落が生じる（第９図）。

（３）　一部の通信ノードがその装着位置から脱落した場合でも、ネットワーク構造情報が変化する（第１０図）。

（４）　通信ノード間の直接波の伝播が遮断され、反射波のみが伝播するが、通信は継続される（第１１図）。

なおネットワークグラフマトリックス上では、通信ノードＮｓと通信ノードＮｔの間の関係を示す要素α（ｓ，ｔ）を次のように定義する。

α（ｓ，ｔ）＝ｄ（ｓ，ｔ）　：　通信ノードＮｓとＮｔ間の距離

＝　－１　　：　通信不能

実際の各通信ノードはその全てが所定の位置で完全に機能するとは限らない。これはコンテナ内は高温かつ振動が激しい環境にあるためである。従ってネットワークグラフマトリックスでは、上述の第８図、第９図、第１０図、第１１図の場合、通信ノード間の距離で示されたネットワーク構造情報を用いて、通信ノードを装着された対象物の変形を検知するため異常を判断する上で本実施例では以下のように前提を立てる。

前提１：　通信ノード間に障害物１００が発生しても、障害物が発生していない通信ノード間の距離は、対象物が変形しない限り、変化しない。

前提２：　故障や電池切れで動作停止した通信ノード２１１ａは他のどの通信ノードとの間でも通信ができず、距離計測ができない。

前提３：　装着位置から脱落した通信ノード２１１ｂでは、他の全通信ノードとの距離が変化する。

前提４：　対象物が変形する場合には、相対距離関係が変化しない複数個の通信ノードからなるグループが、複数個発生する。

前提５：　２個以上の通信ノードとの距離が変化しないのに、１個の通信ノードとの間の距離だけが長くなったのは、その１個の通信ノードとの通信が直接波で行なわれていた状態（直接波の消滅のために消えた距離１０１）から、間接波で行なわれる状態（反射に伴う経路（間接波）で計測した距離１０２）に変化したためである。

第１２図（Ａ）のネットワーク構造情報を有するネットワークにおいて、扉に装着された２つの通信ノードＮ１とＮ２は、第１２図（Ｂ）に示すように、Ｎ１とＮ２の間の距離を変化させないまま、扉の開閉に伴なって、他の通信ノードとの距離を変化させる。このよ

うな変化を、ネットワーク構造情報の初期値（例えば第１２図（Ａ）の状態）と、現在のネットワーク構造情報（例えば第１２図（Ｂ）の状態）を比較することで検出する。この検出は、第９図、第１０図のような動作停止の通信ノードと、脱落した通信ノードを比較対象から排除した上で、距離計測ができた通信ノード対の情報だけを用いて、ネットワーク構造情報の初期値と現在値を比較して行なう。この具体的な処理フローチャートを第１３図に示す。

第２３図のＳＴ２３０９の処理をロバストにするために、第１３図に示す処理を実行する。まず、各通信ノードは他の通信ノードとの間の距離が計測される（ＳＴ１３０５）。この距離計測は全ノードで行なわれ、各通信ノードが保持する他ノードまでの距離のリストを収集して、現在のネットワーク構造情報、すなわち第１５図（Ｂ）に示すようなネットワークグラフマトリックスが生成される（ＳＴ１３０６）。

なお上述のように全てのノードが必ずしも所定の位置で機能しているとは限らないので、ネットワークグラフマトリックスを初期値と比較し、解析して、動作停止通信ノードと脱落通信ノードを検出する（ＳＴ１３０７）。この場合、第１５図（Ｂ）に示すように、他の通信ノードとの距離データが全て－１である通信ノード（例：Ｎ３）は動作停止中のノードであると判定される。またネットワークグラフマトリックスの初期値におけるノード間距離と比較して、全てのノード間距離が所定値以上変化している通信ノード（例：Ｎ５）を脱落通信ノードと判定する。

そして動作停止通信ノードと脱落通信ノード以外の通信ノードから構成される第１６図（Ａ）、第１６図（Ｂ）に示すネットワークグラフマトリックスの部分を、第１５図（Ａ）および第１５図（Ｂ）に示す初期ネットワークマトリックスおよび現在のネットワークグラフマトリックスから抽出する（ＳＴ１３０８）。

次に、後から第１４図で詳述する処理フローで、第１６図（Ａ）、第１６図（Ｂ）に示す抽出した部分のネットワーク構造情報を比較し、対象物の変形と、通信ノード間への障害物の侵入と、間接波での距離計測部分を検知する（ＳＴ１３０９）。

第１４図を参照して、上述のＳＴ１３０８で述べた第１６図（Ａ），第１６図（Ｂ）に示す抽出したネットワーク構造情報を比較し、対象物の変形と通信ノード間への障害物の侵入、および間接波での距離計測部分を検知する処理の詳細を説明する。

まず第１６図（Ａ）の初期ネットワークグラフマトリックスと、第１６図（Ｂ）に示すと現在のネットワークグラフマトリックスを読みこむ（ＳＴ１４０１）。順番に１つの通信ノードの情報を読み込み（ＳＴ１４０２）、着目している通信ノードと、他の通信ノードとの間のリンク情報としての距離データの変化を１つづつチェックする（ＳＴ１４０３）。例えばＮ１ノードと他のノードであるＮ２、Ｎ４、Ｎ６の距離データの変化をチェックする。距離算出できていたリンクが、距離算出できなくなったら、そのリンクへ障害物侵入と判定する（ＳＴ１４０４、ＳＴ１４０５）。

もし距離が算出できて、かつ距離データが所定基準以上に変化し、かつ距離データが所定基準以上に変化したリンクが、着目ノードにおいて他にもあれば（ＳＴ１４０６、ＳＴ１４０７）、対象物の変形と判定し、距離データが所定基準以上に変化していなかったら次のノードに対するチェックが続けられる（ＳＴ１４１０、ＳＴ１４１１、ＳＴ１４０３）。また距離データが所定基準以上に変化していなければ、間接波での距離計測と判定する（ＳＴ１４０９）。すなわち当初の直接波による測定から間接波による距離測定に通信経路が変化したと判断される。上記の処理は全てのノードの、他の全てのノードに対して判断される。

第１６図（Ａ），第１６図（Ｂ）は、上述の処理の具体例である。すなわち初期ネットワークグラフマトリックスから抽出された第１６図（Ａ）のＦｉｎｇｅｒｐｒｉｎｔと、第１６図（Ｂ）の現在値を比較する。ここではα（Ｎ２，Ｎ４）が、Ｆｉｎｇｅｒｐｒｉｎｔと現在値の間で変化しており、しかもプラスの値が－１に変化している。これから、通信ノードＮ２とＮ４の間に侵入があると判定できる。また通信ノードＮ１とＮ６の間の距離が、８０から９３に変化している。変化量は１３である。この変化量が所定の基準値以内であれば、距離の測定誤差であるとみなせる。しかし、もしこの値が基準値以上であり

、そのような基準値以上の距離変化が通信ノードＮ１との間で生じた通信ノードが他にもあれば、通信ノードを装着した対象物に変形が生じたとみなせる。この場合、Ｎ１とＮ４の間の距離も２５から３５に増加している。したがって、通信ノードＮ１に対応した対象物の部分（例えばドア側）は、通信ノードＮ４，Ｎ６に対応した対象物の部分（例えばドアの枠側）に対して変形したと判定できる。この場合、侵入と判定された通信ノード対の個数や、変形と判定された通信ノード対の個数が所定の基準値以上あったり、変形の量の総和が所定の基準値以上であったら、攻撃とみなすことが出来る。

各通信ノードのハード構成

第１７図に示すのは、第２実施例のＵＷＢ電波を用いて、他の通信ノードとの間の距離の測定を行なう通信ノードの機能ブロック図である。通信ノード１７００は、通信ノードの動作を制御するコントローラ１７０１と、送信アンテナ１７０２，受信アンテナ１７０３，パルス増幅器（ＰＡ）１７０４，低雑音増幅器（ＬＮＡ）１７０５，インパルス生成器１７０６，インパルス復調器１７０７，測距用系列（ＰＮ符号）発生器１７０８，ＰＮ符号再生器１７０９，相互相関器１７１０，距離計算器１７１１，データ復調器１７１２、切り替え器１７１３からなる。ここで、コントローラ１７０１は、実施例２に関して上記で説明した処理も実行する。コントローラ１７０１には図示していないが、自ノード番号およびネットワーク構造情報としてのネットワークグラフマトリックスの初期値および現在値が記憶される。

各通信ノードは第１８図に示す距離測定と第２０図に示すデータ通信を実行する機能を有する。他の通信ノードとのデータ通信にしても、他の通信ノードとの距離の計測をするにしても、各通信ノードは、対象とする通信ノードのノード番号を知っておく必要がある。すなわちこのような距離測定およびデータ通信に先だって、各通信ノードは、公知の方法（例：オムロンの特許出願である特開平５－７５６１２号の技術）を用いて、直接に通信可能な他の通信ノードのノード番号および間接に通信可能（他の通信ノードによる中継により通信可能）な他の通信ノードを含めて、ネットワーク内の全ての通信ノードのノード番号の情報を得て、それを記憶する。

ＵＷＢ電波を用いた距離計測のための前処理

例えば通信ノードＡから通信ノードＢへの距離を、ＵＷＢ電波を用いて距測定する場合を説明する。まず、全ての通信ノードにおいて、切替え器１７１３のスイッチはＡ端子に接続されている。この状態では、通信ノードは送信アンテナからデータを送信し、受信アンテナから受けたデータは、データ復調器１７１２を経て、コントローラ１７０１に与えられる。この状態では、全ての通信ノードは受信アンテナから来る情報を監視している。

通信ノードＡは、通信ノードＢとの距離を計測しようとする前に、「Ｂ以外の通信ノードは、距離測定用に送信されるＰＮ符号を受信しても返信せず無視せよ。通信ノードＢは受信したＰＮ符号をそのまま返信せよ。」との趣旨を示すコマンドＲｅｑＤｉｓｔ（Ｂ）を送信する。通信ノードＢでは、前記コマンドを受信したら切替え器のスイッチをＣ側に接続して、データ復調器の出力が直接にインパルス生成器１７０６に入力される状態に移行する。通信ノードＢは、ＲｅｑＤｉｓｔ（Ｂ）を受けた後、一定時間を経過するか又はデータ復調器１７１２がＰＮ符号を切替え器に出力し終わったら、切替えスイッチをＡ側に戻すとともに、データ復調器１７１２の出力をコントローラ１７０１が監視する状態に戻る。

ＵＷＢを用いた距離計測の実行

通信ノードＡは、前記のコマンドＲｅｑＤｉｓｔ（Ｂ）を送信した後に、切替え器１７１３のスイッチを第１７図に示すＢ側に接続して、測距用系列（ＰＮ符号）１７０８をインパルス生成器１７０６とＰＡ１７０４を介して送信アンテナ１７０２から送信する。この送信によって通信ノードＡは、通信ノードＢからの返信として、自己が送信したＰＮ符号と同じ符号を受信する。これを通信ノードＡは受信アンテナ１７０３で受信し、ＬＮＡ１７０５で増幅した後に、インパルス復調１７０７でインパルス復調する。インパルス復調した出力からＰＮ符号を再生する。この再生したＰＮ符号と、送信したＰＮ符号の時間差を示すチップ数を相互相関器１７１０で計測する。ただし、各通信ノードの相互間距離の

最大値に対応するＰＮ符号でのチップ数の差はＰＮ符号周期を示すチップ数以内であるとする。
送信したＰＮ符号と受信したＰＮ符号の時間差を示すチップ数から、通信ノード内での遅延時間を示す定数を差し引いた値を２で割り算することで、通信ノードＡと通信ノードＢの距離をチップ数で示した値が計算される。この値に、１チップに対応する距離を掛け算して、通信ノードＡと通信ノードＢの間の距離が算出される。すなわち第２０図で概略を示すように、通信ノードＡから通信ノードＢへ、測距用のコードを送信し、通信ノードＢは、通信ノードＡから送られたデータをそのまま返信する。通信ノードＡでは、受信データ中のＰＮ符号と送信データ中のＰＮ符号との相関をとる。相関の最大値を与えるズレ量に相当するチップ数をもとに、通信ノード間を電波が伝播するための時間を計測し、伝播時間をもとに、通信ノード間の距離を算出する。この通信距離測定時の、送信データと受信データ間のＰＮ符号の遅れは、第１９図（Ａ）と第１９図（Ｂ）のように計測される。また通信ノードＡと通信ノードＢ間のデータの送受信は第２０図に示すように行なわれる。
その後、通信ノードＡは、直接に通信可能な他の通信ノードのノード番号を順次に指定して、前記の方法で同様に他の通信ノードとの間の距離を測定していく。通信ノードＡは、測定できた他の通信ノードまでの距離のリスト（ノード配置情報）をコントローラ内のメモリーに記憶する。そして、この距離のリストの通報要求があったら、他の通信ノードに通報する。通信ノードＡも他の通信ノードも距離測定のジョブが終了すると、切替え器をＡ側に接続するとともに、データ復調器の出力をコントローラが監視する状態に移行する。すなわち、第２０図に示すデータ通信が可能な待機状態に移行するのである。このような処理を全通信ノードが実行することで、通信ノード間の距離が測定されていく。
通信ノード近傍の物体までの距離測定
実施例２において、次のような処理を付加するだけで、通信ノードの近傍の物体までの距離を測定できるようになり、通信ノード間の距離のみを計測して、対象物の監視をしていた場合よりも、監視できる内容がきめこまかくなる。
すなわち、通信ネットワーク内の各通信ノードの間の距離の測定が終了した後に、第２１図に示すように、それぞれの通信ノードが順に自己の近傍の物体までの距離を計測する。各通信ノードは、自通信ノードと最も近い通信ノードまでの距離よりも少し短い距離（例えば、最も近い通信ノードまでの距離の９０％）までだけを計測する。これは、距離計測の際に送信ＰＮ符号をシフトさせながら受信ＰＮ符号との相関をとる場合の最大シフト量の上限を、自通信ノードと最も近い通信ノードまでの距離よりも少し短い距離に対応した値に設定することで実現できる。
第２１図からも判るように、通信ノードで構成されるグラフでは、一直線上にない３つの通信ノードによって三角形状のメッシュが構成される。ここで、通信ノードＡ，Ｂ，Ｃから構成されるメッシュの内部には他の通信ノードは存在しないが、例えば通信ノードＥ，Ｆ，Ｂから構成されるメッシュには他の通信ノードであるＡが内部に含まれる。内部に他の通信ノードを含まないメッシュをメッシュセルと名付ける。メッシュセルごとに電波を反射する物体Ｒが存在するかどうかおよびその特性を記録できる。
ここで例えば、任意に取り出した３つの通信ノードの組Ａ，Ｂ，Ｃがメッシュセルかどうかを判定する方法は以下のように行なうことが出来る。すなわち、条件１と条件２の両者を満足するものがメッシュセルである。
まず、条件１を満足していれば、通信ノードの組Ａ，Ｂ，Ｃは三角形のメッシュを構成する。
条件１：下記の全ての条件を満足すること
Ｌｅｎｇｔｈ（Ａ，Ｂ）＜（Ｌｅｎｇｔｈ（Ｂ，Ｃ）＋Ｌｅｎｇｔｈ（Ｃ，Ａ））
Ｌｅｎｇｔｈ（Ｂ，Ｃ）＜（Ｌｅｎｇｔｈ（Ｃ，Ａ）＋Ｌｅｎｇｔｈ（Ａ，Ｂ））
Ｌｅｎｇｔｈ（Ｃ，Ａ）＜（Ｌｅｎｇｔｈ（Ａ，Ｂ）＋Ｌｅｎｇｔｈ（Ｂ，Ｃ））
次に、条件２を満足していれば、そのメッシュＡ，Ｂ，Ｃはメッシュセルである。
条件２：下記の条件を満足する物体Ｒが存在しないこと

（Ｌｅｎｇｔｈ（Ｒ，Ａ）＋Ｌｅｎｇｔｈ（Ｒ，Ｂ）＋Ｌｅｎｇｔｈ（Ｒ，Ｃ））＜（Ｌｅｎｇｔｈ（Ａ，Ｂ）＋Ｌｅｎｇｔｈ（Ｂ，Ｃ）＋Ｌｅｎｇｔｈ（Ｃ，Ａ））

通信ノード間距離を示す第１６図（Ｂ）のマトリックスを解析することで、メッシュセルを抽出できる。抽出したメッシュセルごとにメッシュセル番号を付与し、次の式を満足する物体Ｒが存在するかどうかなどの情報を、メッシュセル番号をキーにしてアクセスできる近傍状態テーブルに記録する。

（Ｌｅｎｇｔｈ（Ｒ，Ａ）＋Ｌｅｎｇｔｈ（Ｒ，Ｂ）＋Ｌｅｎｇｔｈ（Ｒ，Ｃ））＜（Ｌｅｎｇｔｈ（Ａ，Ｂ）＋Ｌｅｎｇｔｈ（Ｂ，Ｃ）＋Ｌｅｎｇｔｈ（Ｃ，Ａ））

例えば、通信ノードＡ，Ｂ，Ｃからなるメッシュセルの番号を５番とする。そうすると、近傍状態テーブルの第５行には、メッシュセル５番に含まれる対象物Ｒの存在の有無、対象物Ｒからの反射波としてメッシュセルの各通信ノードに受信された電波の強度、メッシュセルの各通信ノードと対象物Ｒの距離が記録される。全てのメッシュセルについて、この処理をすることで、初期状態におけるメッシュセル内の物体の有無と物体の属性の情報が記録されるので、その後の任意の時点での状態と比較して、状態変化を検出できる。メッシュセルに状態変化があったという事は、物体の侵入または退出がメッシュセル付近で発生したことを意味する。物体の退出の例としては、コンテナ内の貨物の盗難がある。物体の侵入の例としては、通信ノードが装着されたコンテナの壁に穴が開けられて、そこから物体がコンテナ内に入れこまれている状態であったり、物体のコンテナへの入れこみが完了し、コンテナの扉の閉鎖直後には存在していなかった物体が存在するようになったことを意味する。コンテナ内への危険物の搬入である可能性もある。

コンテナ船上での不正アクセス

なおコンテナに対する不正なアクセスは、必ずしも陸上でコンテナが移動中とは限らない。すなわちコンテナ船上でも積み上げられたコンテナに不審者がアクセスすることは不可能ではない。このような人間がアクセス可能な状態のコンテナでは、そのコンテナの扉に取り付けたアンテナ２４０を用いて、そのコンテナ船に搭載した無線機と通信が可能である。しかしコンテナの扉に取り付けたアンテナは、コンテナ船に搭載した図示しない無線機用のアンテナを、その間に障害物なしに直接に見渡せる位置には存在しないのが通常である。この場合、甲板上のコンテナに関しては、コンテナ船の甲板の端をぐるりと取り囲んで乗組員が海上に転落するのを防止するためのフェンスに無線アンテナを一定間隔で配置し、端に積まれたコンテナの扉部分に装着された無線アンテナから見渡せる近い位置に、その甲板フェンスに位置するどれかの無線アンテナがあれば、コンテナ船に搭載したコンピュータと、全てのコンテナが無線通信できる。これは、各コンテナの扉に装着された無線アンテナで、上下左右に隣接するコンテナは、通信できるので、自己組織無線通信ネットワークを形成することが可能となる。これが、コンテナ船に積載されたコンテナの各列ごとに行なわれる。また、各コンテナ列ごとに、その列の端にあるコンテナは、甲板のフェンスにある無線機と通信リンクを形成する。さらに、甲板フェンスに分散配置した無線機は、それぞれが自己組織通信ネットワークでの通信ノードとなり、相互に自動的に通信リンクを形成する。その結果、積載されたコンテナ内から外にアンテナを出して通信ノードとなっている各制御装置、甲板のフェンスに位置する無線機、コンテナ船の通信室に位置する無線機からなるシステムは全体としても、自己組織通信ネットワークを構成する。同様のことを船倉に積まれたコンテナに関しても可能である。船倉において、コンテナの列の端にあるコンテナの扉に取り付けられた無線アンテナとの間で伝播の送受信が可能な無線アンテナを船倉の適切な位置に配置しておく。そうすると、各コンテナを通信ノードとした自己組織無線通信ネットワークが形成でき、船倉の任意のコンテナと船倉に置いた通信装置が通信でき、この通信装置に接続されたコンテナ船の通信室の無線機が通信して、前記と同様の外部へのコンテナ状態の通報や問い合わせなどができる。

その結果、コンテナ船に積載されたすべてのコンテナは、他の通信ノードによる中継により、コンテナ船の通信室に位置する無線機と通信が可能となる。

そして、各コンテナは定期的にその状態を通信室にある無線機に通報することが可能となるので、コンテナ船に搭載している状態で各コンテナの扉の開閉やコンテナの扉への穴あ

けの監視ができる。その結果、コンテナ船が例えば、米国の領海にはいる前から搭載コンテナの異常の有無を米国のコーストガードなどに通報することが可能となる。

産業上の利用可能性

本発明ではコンテナをシールするために、”Ｈａｇｏｒｏｍｏ”方式をｉｎｓｉｄｅ　ｓｅａｌとして用いている。従って従来のシール方式とは異なり、コンテナの外側からは目視することができない。この方式により例えばテロリスト等がコンテナのドアを不正に開閉するための事前準備をするのが防止される。またさらに電気回路を冷却してドア開閉検知機能を麻痺させることも防止することが出来る。

さらに本発明では、積荷の特性とは無関係に積荷が置かれた空間内の通信状態を検知するので、従来の監視方法に比べて汎用的であり、多種多様な積荷を入れるコンテナ内を監視することが容易になる。

また上述の”Ｈａｇｏｒｏｍｏ”方式の通信ノードは基本的にはコンテナ内にランダムに配置されるため、不正な操作やテロリスト等が本監視システムを不正に改造することが困難となる。

また本発明では、ドア開閉のパスワードはコンテナ運用会社とは別の監視センタで自動生成されるので、不正な操作者によりそのパスワードが漏洩するのが防止される。

さらにまた記憶されたネットワークグラフマトリックスと、その後に得られたネットワークグラフマトリックスの間に所定基準異常の差異が検知されると、データが消去され、同じデータは再生することが出来ない。従ってテロリスト等が同じデータをコピーして、偽のコンテナに移植することは不可能となる。

また本発明ではドアの不正開閉だけでなく、コンテナの壁面にはセンサーが設置されているために、ドリルやバーナーで壁面に穴を開けて危険物をコンテナ内に挿入することも検知することが出来る。

特に本発明の第１実施例では自己組織ネットワーク通信を用いているため、各通信ノードは、省電力で他の通信ノードと通信ができ、また通信ノード間の通信リンクが通信ノードの空間的な配置を表現できるように構成されているので、コンテナ内を汎用的な手法で監視することが出来る。また第２実施例ではＵＷＢ通信を用いて距離を計測して通信リンクが通信ノードの空間的な配置を表現しているので、正確に複数の通信ノード間の距離が測定できる。

【図面の簡単な説明】

第１図は従来技術の概略図である。

第２図は本発明でのセンシング方式を示す概略図である。

第３図は本発明に係るコンテナ監視システムの全体を示す構成図である。

第４図はコンテナの内外の通信の仕組みを示す概略図である。

第５図（Ａ）は扉が閉じられた直後のネットワークグラフであり、第５図（Ｂ）は扉が開けられた時のネットワークグラフである。

第６図（Ａ）は第１実施例に係る、扉が閉じられた直後のネットワークグラフマトリックスであり、第６図（Ｂ）は扉が開けられた時のネットワーク構造を示すネットワークグラフマトリックスである。

第７図は、第２実施例を説明するための、他のネットワーク構造を示す概略図である。

第８図は、第２実施例を説明するための、ネットワーク構造で、一部の通信ノード間に侵入物があった場合を示す概略図である。

第９図は、第２実施例を説明するための、ネットワーク構造で、一部の通信ノードに動作停止または欠落があった場合を示す概略図である。

第１０図は、第２実施例に係るネットワーク構造で、一部の通信ノードが脱落した場合を示す概略図である。

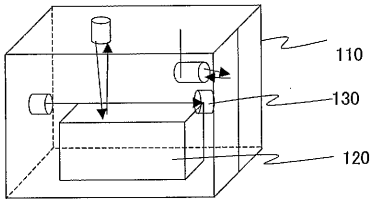
第１１図は、ネットワーク構造で、一部の通信ノード間で第２実施例の直接波でなく間接波で距離計測がされる場合の概略図である。

第１２図は、第２実施例で初期ネットワーク構造と監視時のネットワーク構造を示した概略図である。

第１３図は、第２実施例において、ネットワーク構造情報の初期値をＦｉｎｇｅｒｐｒｉｎｔとして登録し、さらにネットワーク構造情報の変化を監視し、シールへの攻撃やコンテナへの不正侵入があったと判定したときにＦｉｎｇｅｒｐｒｉｎｔを消去するという動作を示すフローチャートである。
第１４図は、第１３図のＳＴ１３０９の詳細を示したフローチャートである。
第１５図（Ａ）は第２実施例に係る、コンテナの扉が閉じられた直後のネットワーク構造の初期値を示すネットワークグラフマトリックスであり、第１５図（Ｂ）はネットワークグラフマトリックスの現在値である。
第１６図（Ａ）は第１５図（Ａ）に対応する有効な通信ノード間のみのネットワークグラフマトリックスである。第１６図（Ｂ）は第１５図（Ｂ）に対応する有効な通信ノード間のみのネットワークグラフマトリックスである。
第１７図は第２実施例のＵＷＢによる距離計測とデータ通信を行なう部分のブロック図である。
第１８図は、第２実施例のＵＷＢによる距離計測のための送受信を示す概略図である。
第１９図は、第２実施例の距離計測のために行なわれる送信データと受信データ間の相関演算を説明する概略図である。
第２０図は、第２実施例のデータ通信を示す概略図である。
第２１図は、第２実施例のメッシュセルを説明するための概略図である。
第２２図は、本発明において、コンテナにノードを設置してコンテナ内のＦｉｎｇｅｒｐｒｉｎｔを生成して登録後、コンテナを輸送し、目的地に到着して扉を開けるまでを示す処理フローチャートである。
第２３図は、本発明の各ノードにおける処理手順を示すフローチャートである。
第２４図は、本発明の制御装置２２０における処理手順を示すフローチャートである。
第２５図（Ａ）と第２５図（Ｂ）はメカ式の従来型シールの外観図である。
第２６図（Ａ）と第２６図（Ｂ）は電子式の従来型シールの外観図である。
第２７図は、米国特許で開示されているシールの一例である。
第２８図は、米国特許で開示されているシールの一例である。
第２９図（Ａ）は一般的なコンテナの外観図、第２９図（Ｂ）はその内部を示す概略図である。

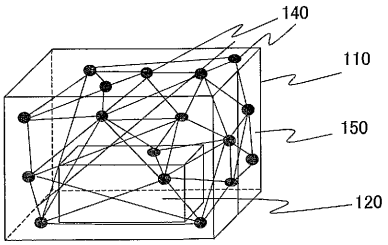
【図１】

FIG. 1



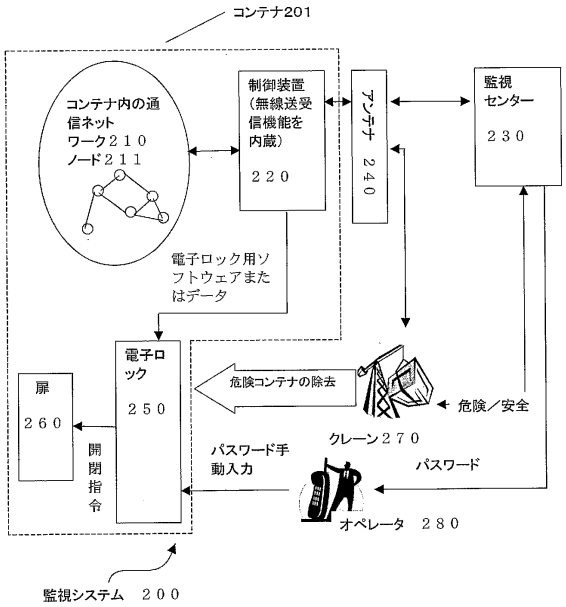
【図２】

FIG. 2



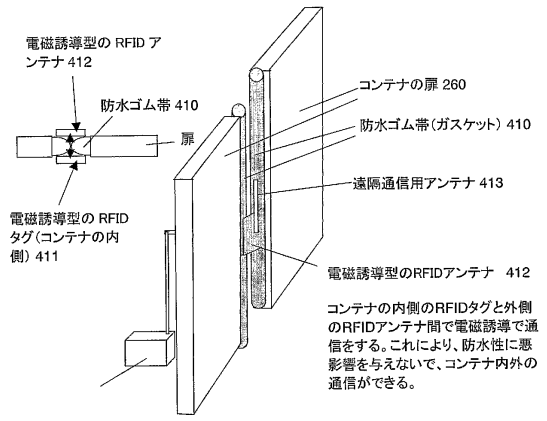
【図３】

FIG. 3



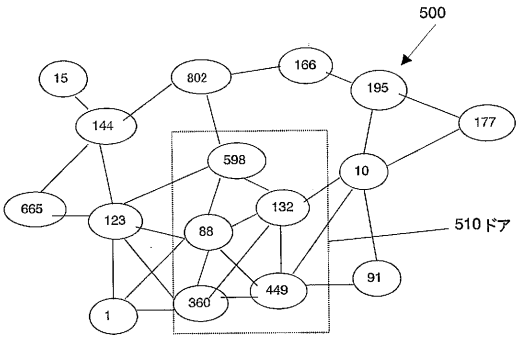
【図４】

FIG. 4



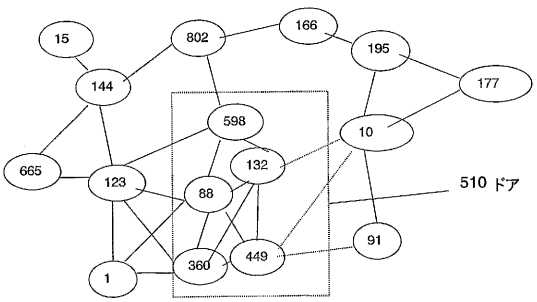
【図５（Ａ）】

FIG. 5(A)



【図５（Ｂ）】

FIG. 5(B)



【図６（Ａ）】

FIG. 6(A)

500

	15	665	144	123	1	802	598	88	360	166	132	449	195	10	91	177
15	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
665	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
144	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0
123	0	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0
1	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0
802	0	0	1	0	0	0	1	0	0	1	0	0	0	0	0	0
598	0	0	0	1	0	1	0	1	0	0	1	0	0	0	0	0
88	0	0	0	1	1	0	1	0	1	0	1	1	0	0	0	0
360	0	0	0	1	1	0	1	0	0	0	1	1	0	0	0	0
166	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
132	0	0	0	0	0	0	1	1	1	0	0	1	0	1	0	0
449	0	0	0	0	0	0	0	1	1	0	1	0	0	1	1	0
195	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1
10	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1
91	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0
177	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0

【図６（Ｂ）】

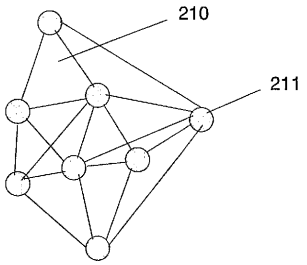
FIG. 6(B)

600'

	15	665	144	123	1	802	598	88	360	166	132	449	195	10	91	177
15	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
665	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
144	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0
123	0	1	1	0	1	0	1	1	1	0	0	0	0	0	0	0
1	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0
802	0	0	1	0	0	0	1	0	0	1	0	0	0	0	0	0
598	0	0	0	1	0	1	0	1	0	0	1	0	0	0	0	0
88	0	0	0	1	1	0	1	0	1	0	1	1	0	0	0	0
360	0	0	0	1	1	0	1	0	0	0	1	1	0	0	0	0
166	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0
132	0	0	0	0	0	0	1	1	1	0	0	1	0	0	0	0
449	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0
195	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1
10	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1
91	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
177	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0

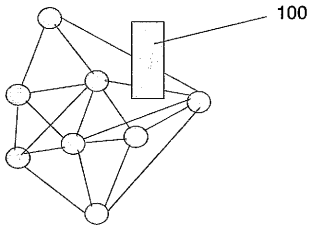
【図７】

FIG. 7



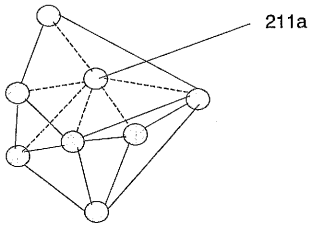
【図８】

FIG. 8



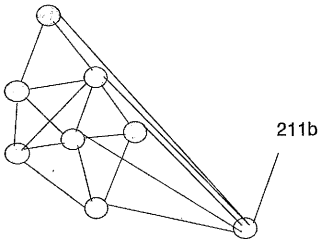
【図９】

FIG. 9



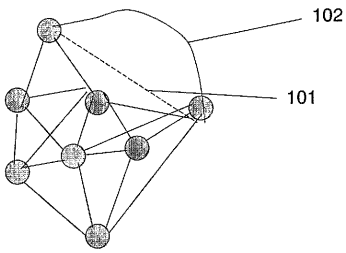
【図１０】

FIG. 10



【図１１】

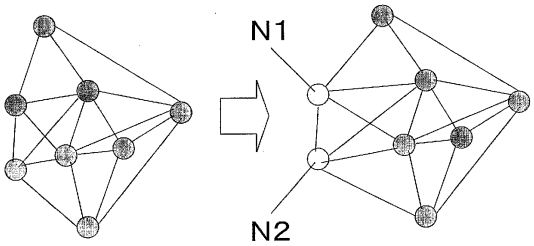
FIG. 11



【図１２（Ａ）】

FIG. 12(A)

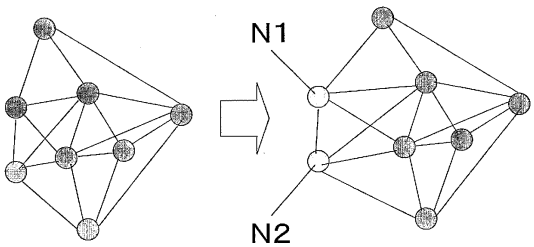
FIG. 12(B)



【図１２（Ｂ）】

FIG. 12(A)

FIG. 12(B)



【図１３】

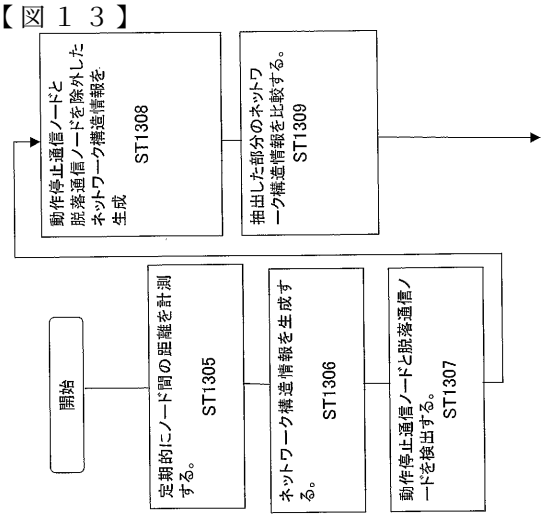


FIG.13

【図１４】

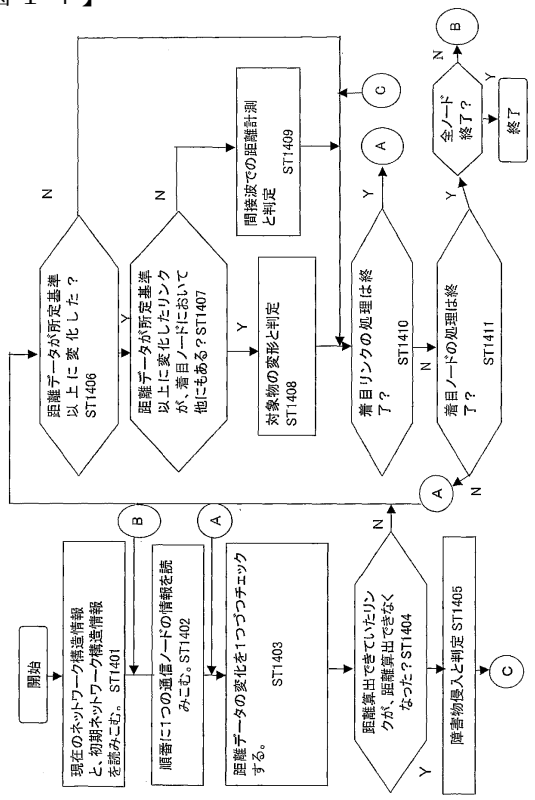


FIG.14

【図１５（Ａ）】

FIG.15(A)

	N1	N2	N3	N4	N5	N6
N1	0	30	40	25	50	80
N2	30	0	24	67	43	75
N3	40	24	0	36	41	55
N4	25	67	36	0	74	58
N5	50	43	41	74	0	24
N6	80	75	55	58	24	0

Fingerprint（指紋）

【図１５（Ｂ）】

FIG.15(B)

	N1	N2	N3	N4	N5	N6
N1	0	30	-1	25	72	80
N2	30	0	-1	67	63	75
N3	-1	-1	0	-1	-1	-1
N4	25	67	-1	0	104	58
N5	72	63	-1	104	0	45
N6	80	75	-1	58	45	0

現在値

【図１６（Ａ）】

FIG.16(A)

	N1	N2	N4	N6
N1	0	30	25	80
N2	30	0	67	75
N4	25	67	0	58
N6	80	75	58	0

Fingerprint（指紋）

【図１６（Ｂ）】

FIG.16(B)

	N1	N2	N4	N6
N1	0	30	35	93
N2	30	0	-1	87
N4	35	-1	0	58
N6	93	87	58	0

現在値

【図１７】

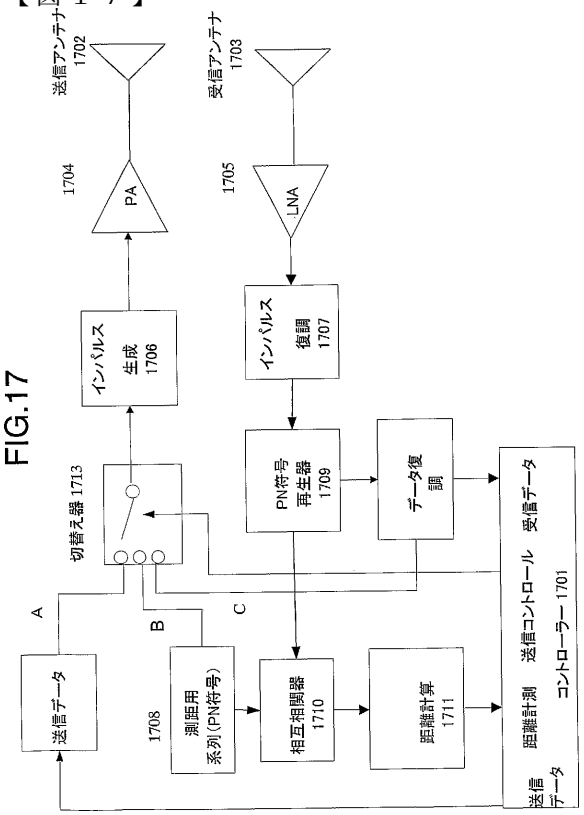


FIG.17

【図１８（Ａ）】

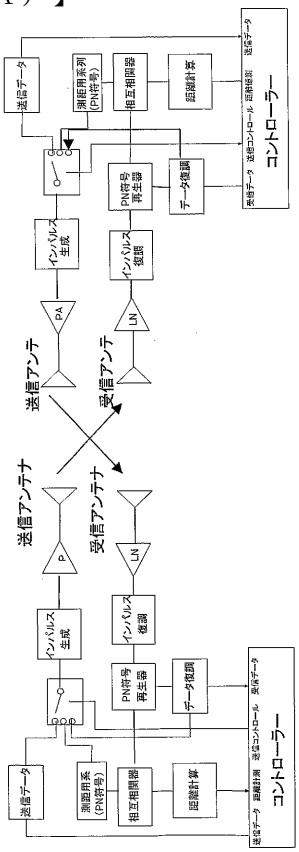


FIG.18(A)

FIG.18(B)

【図１８（Ｂ）】

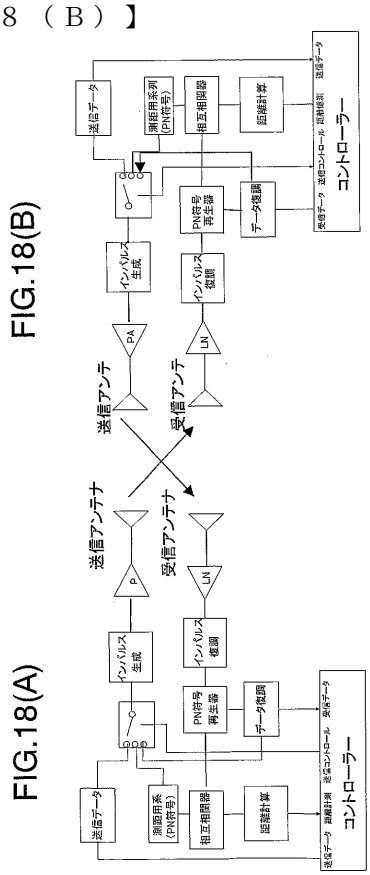


FIG.18(A)

FIG.18(B)

【図１９（Ａ）】

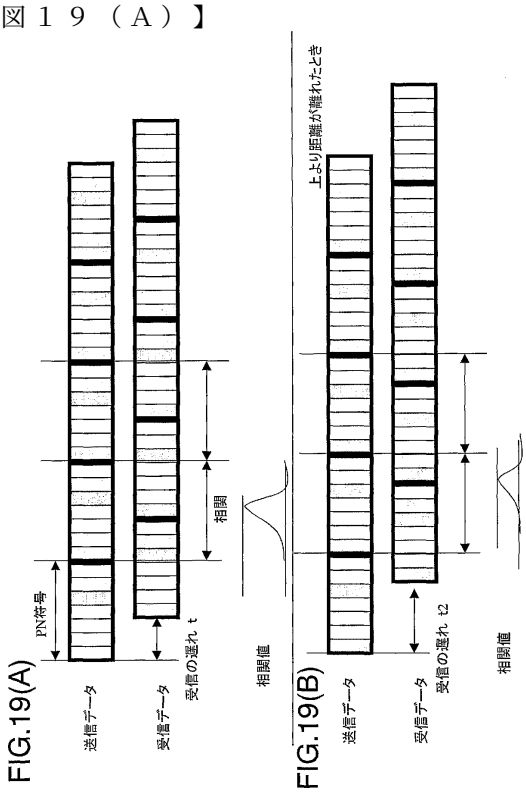


FIG.19(A)

FIG.19(B)

【図１９（Ｂ）】

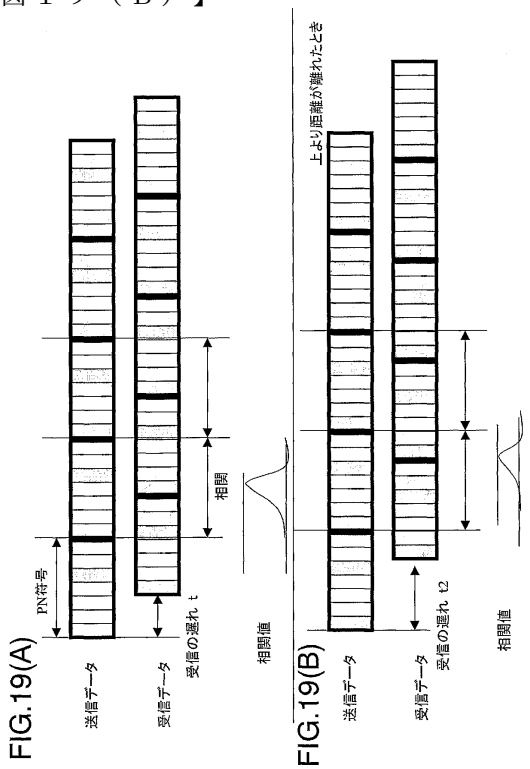


FIG.19(A)

FIG.19(B)

【図２０（Ａ）】

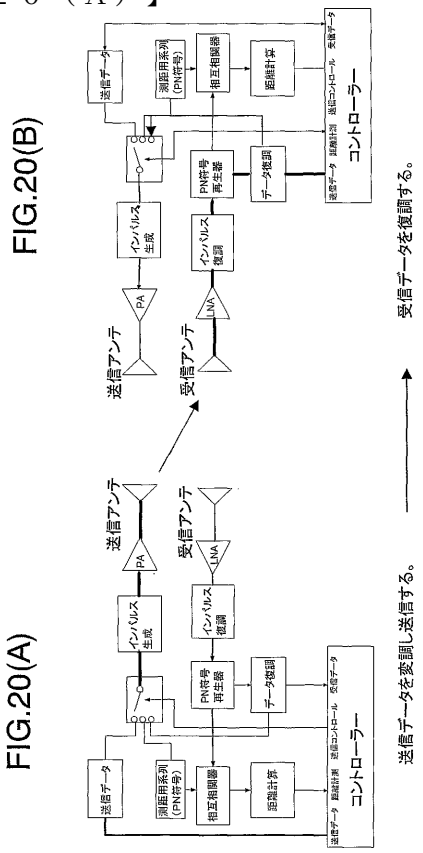


FIG.20(B)

FIG.20(A)

【図２０（Ｂ）】

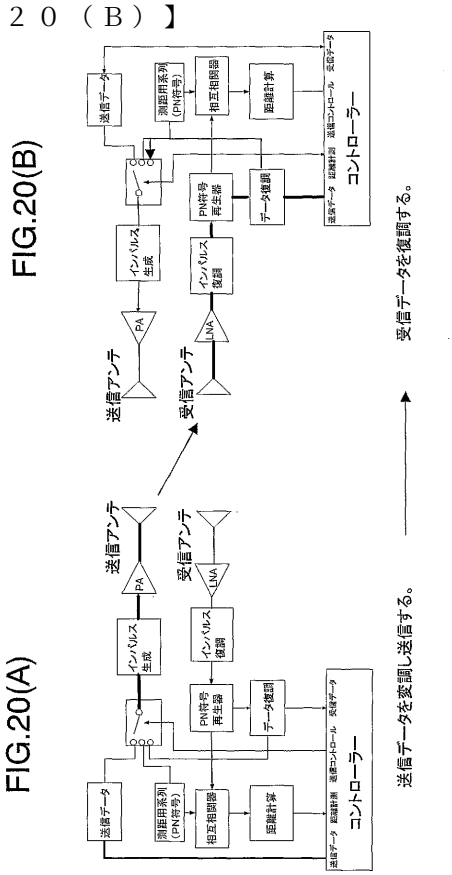
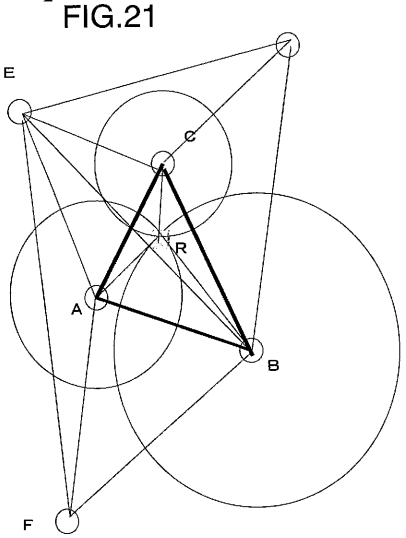


FIG.20(B)

FIG.20(A)

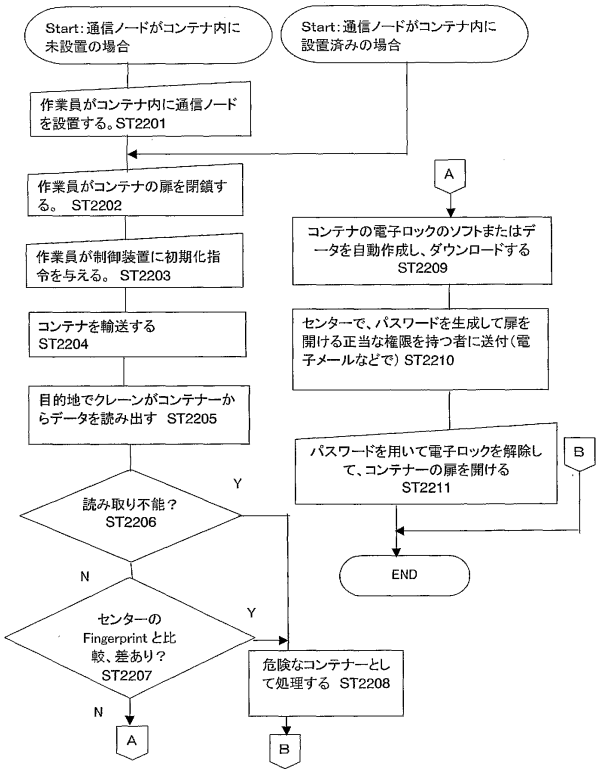
【図２１】

FIG.21



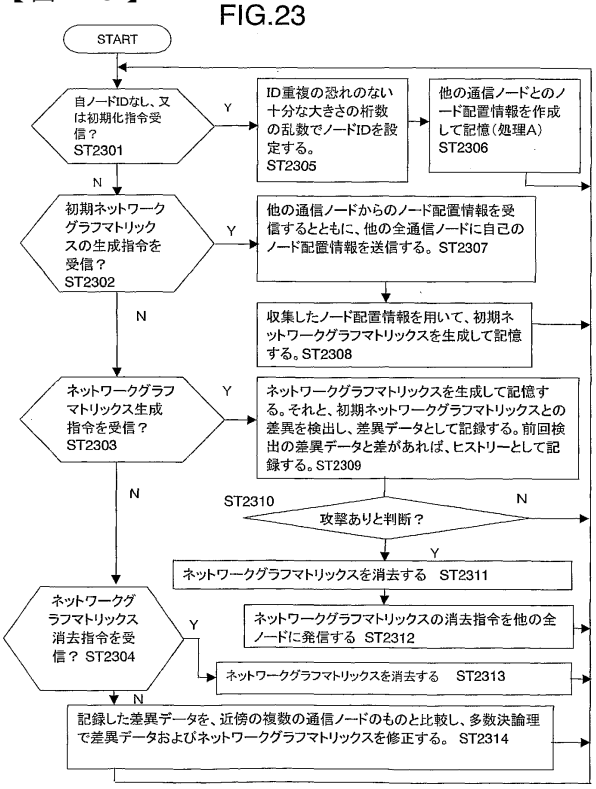
【図２２】

FIG.22



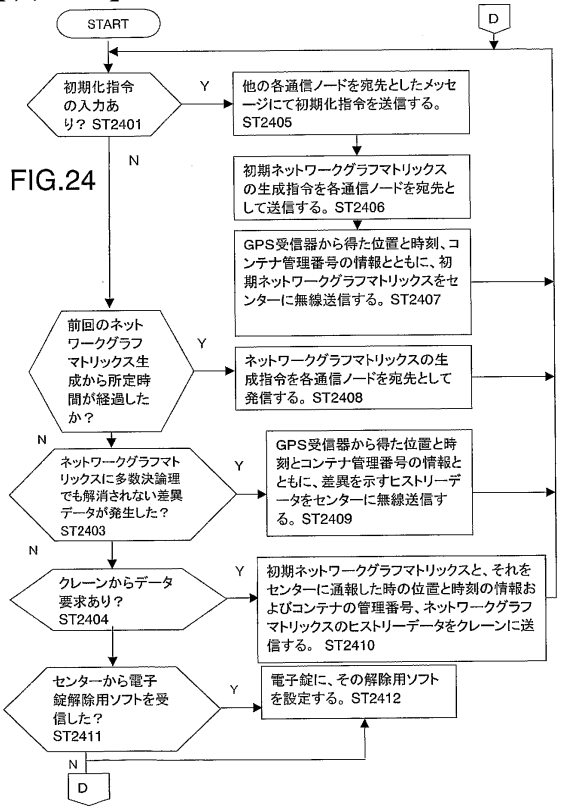
【図２３】

FIG.23



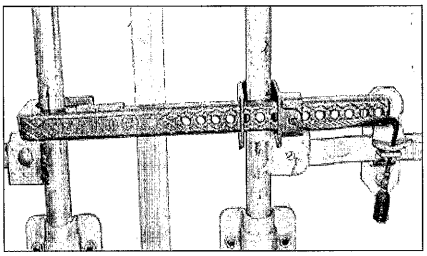
【図２４】

FIG.24



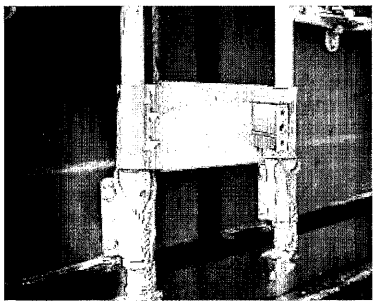
【図２５（Ａ）】

FIG.25(A)



【図２５（Ｂ）】

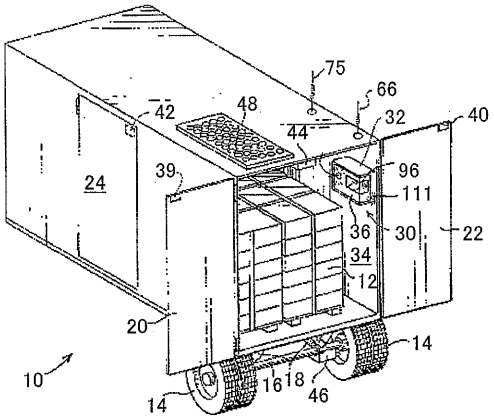
FIG.25(B)



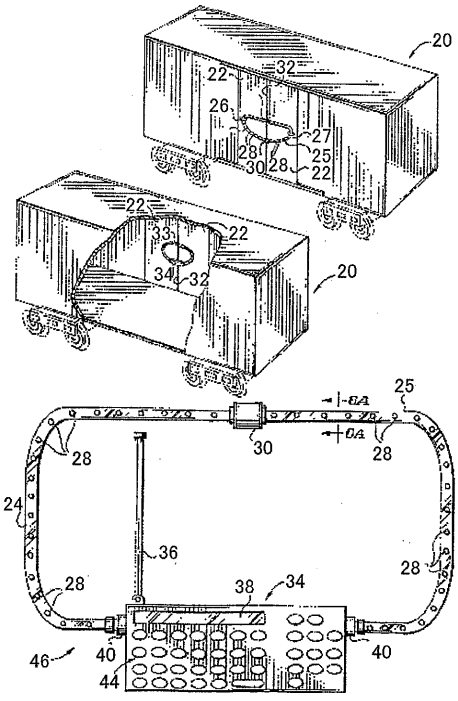
【図２６（Ａ）】
FIG.26(A)

【図２６（Ｂ）】
FIG.26(B)

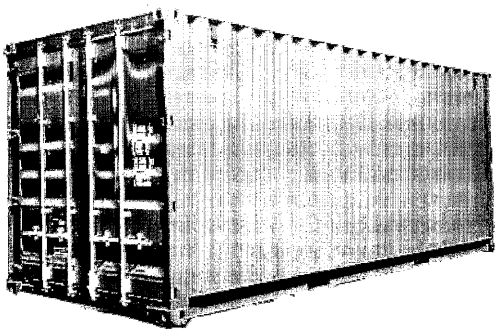
【図２７】
FIG.27



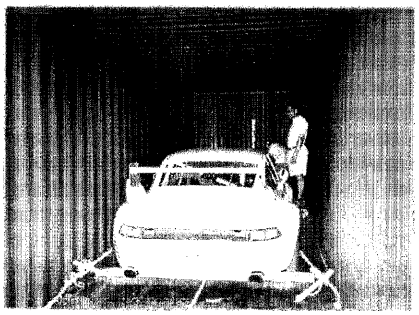
【図２８】
FIG.28



【図２９（Ａ）】
FIG.29(A)



【図２９（Ｂ）】
FIG.29(B)



フロントページの続き

(72)発明者　中村　明彦
日本国京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内

審査官　千壽　哲郎

(56)参考文献　国際公開第００／０１９６６７（WO，Ａ１）
特開２０００－３２４１４７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G08B 13/22
B65G 61/00
G08B 25/10
H04M 11/00