(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3923346号
(P3923346)
(45)発行日　平成19年5月30日(2007.5.30)　(24)登録日　平成19年3月2日(2007.3.2)

(51)Int.Cl.		F I		
H04M 11/00	(2006.01)	H04M	11/00	302
H04Q 7/38	(2006.01)	H04B	7/26	109A
H04M 1/725	(2006.01)	H04M	1/725	
H04B 7/26	(2006.01)	H04B	7/26	S
G06F 13/00	(2006.01)	G06F	13/00	610Q

請求項の数 6　(全 11 頁)

(21)出願番号　特願2002-94904(P2002-94904)
(22)出願日　平成14年3月29日(2002.3.29)
(65)公開番号　特開2003-298763(P2003-298763A)
(43)公開日　平成15年10月17日(2003.10.17)
審査請求日　平成16年9月14日(2004.9.14)

(73)特許権者　000006633
京セラ株式会社
京都府京都市伏見区竹田鳥羽殿町６番地
(74)代理人　100075513
弁理士　後藤　政喜
(74)代理人　100084537
弁理士　松田　嘉夫
(74)代理人　100114236
弁理士　藤井　正弘
(72)発明者　日高　寛之
神奈川県横浜市都筑区加賀原二丁目１番１号　京セラ株式会社横浜事業所内

審査官　田中　秀樹

最終頁に続く

(54)【発明の名称】無線通信機

(57)【特許請求の範囲】

【請求項１】

無線通信機の動作を制御する制御部を有し、無線通信網と接続してデータの送受信を行う無線通信機において、

前記制御部は、前記無線通信網から受信するデータ量が所定期間に渡り所定量以上であることを検出し、かつ、前記所定期間に渡り受信した前記データの送信元が所定数以上であることを検出すると、該無線通信機に対するデータの宛先を変更するように動作することを特徴とする無線通信機。

【請求項２】

前記制御部は、

前記無線通信機が受信しているデータの転送速度を検出する検出手段と、

前記データの送信元アドレスを記録する記録手段と、

前記無線通信網から受信するデータ量が所定期間に渡り所定量以上であることが検出された場合、前記所定期間中に前記記録手段に記録されたアドレス数が所定数以上であるか否かを判定する判定手段と、

該無線通信機に対するデータの宛先を変更するように動作する宛先変更手段と、を備えることを特徴とする請求項１に記載の無線通信機。

【請求項３】

第１の通信方式及び第２の通信方式によって前記無線通信網と接続してデータの送受信が可能であって、

前記制御部は、前記無線通信網との間で接続する通信方式を変更することによって、該無線通信機に対するデータの宛先を変更するように動作することを特徴とする請求項１又は２に記載の無線通信機。

【請求項４】

前記第２の通信方式は、無線通信機が接続される毎に該無線通信機に対するデータの宛先を割り当てることを特徴とする請求項３に記載の無線通信機。

【請求項５】

無線通信網と、前記無線通信網と接続しデータの送受信を行う無線通信機と、を備える無線通信システムにおいて、

前記無線通信機は、前記無線通信網から受信するデータ量が所定期間に渡り所定量以上であることを検出し、かつ、前記所定期間に渡り受信した前記データの送信元が所定数以上であることを検出すると、前記無線通信網に報知し、

前記無線通信網は、前記無線通信機からの報知に基づいて、該無線通信機に対するデータの宛先を変更することを特徴とする無線通信システム。

【請求項６】

第１の通信方式及び第２の通信方式によって前記無線通信網と前記無線通信機とを接続してデータの送受信が可能であって、

前記無線通信網と前記無線通信機との間を接続する通信方式を変更することによって、該無線通信機に対するデータの宛先を変更することを特徴とする請求項５に記載の無線通信システム。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】

本発明は、無線通信機に関し、特にインターネットに接続される無線通信機に関する。

【０００２】

【従来の技術】

携帯電話機等の無線通信機は、無線基地局との間に電波による通信回線を設定し、無線により音声、データ等を送受して通信を行うものである。データ通信においては、コンピュータ間のデータ通信方式の１つとしてＩＰを利用したインターネットが広く利用されている。このＩＰ接続は、これまでは主にコンピュータ同士の接続に用いられていたが、ＩＰｖ６の普及により、これまでネットワークとは無縁だった様々な組込み機器もネットワークに対応できるようになる。このように今後様々な機器がネットワーク化されてくると、インターネットにおいて問題となっている様々なクラッキング行為（不正アクセス、盗聴、改ざん、なりすまし、ＤｏＳ攻撃等）に、これらの機器がさらされることが予想される。

【０００３】

特に、ＤｏＳ攻撃（負荷攻撃）は、多数のコンピュータ機器を乗っ取り、その乗っ取った機器を駆使し、攻撃目標とするネットワークやコンピュータ機器へ一斉にアクセスすることで異常負荷をかけ、目標のネットワーク及びコンピュータ機器を過負荷状態に陥れ、事実上利用不可能とする攻撃である。この攻撃方法の特徴は、１つ１つのアクセスはプロトコル上問題がないため、攻撃を目的としたアクセスか通常アクセスが偶然同時期に大量発生したのかは判断がつかない。

【０００４】

このＤｏＳ攻撃の対策として、例えば、特開２００１－３４５５３号公報に見られるような、２つのネットワークの間にアクセス制御装置（ファイヤーウォール）を設置し、ネットワーク間を通過する通信データを全て監視し、過負荷が発生した場合は通過データ、通信シーケンス、アクセスパターン等を解析して、不正な攻撃か、通常のアクセスかを判断する。そして、不正な攻撃と判断された場合は、該当する通信データをファイヤーウォールから先に通さないことで、ファイヤーフォールから先のネットワークへ被害が及ぶことを防いでいる。

【０００５】
【発明が解決しようとする課題】
以上説明したファイヤーウォールを設置し、通過する通信データを監視することによってＤｏＳ攻撃を防ぐ方法は、有線のネットワーク環境では有効である。しかし、携帯電話機のような無線通信を利用したネットワーク接続の場合、携帯電話機内部にファイヤーウォールを設置し、ネットワークからのＤｏＳ攻撃を防ぐことができたとしても、無線資源は浪費されるため有効な方法とはならない。
【０００６】
また、携帯電話機のような小型機器は、機器の大きさ、消費電力等の制限があるため、高速のＣＰＵを搭載することはできないことから、前述した特開２００１－３４５５３号公報に記載されているような、ファイヤーウォールを通過する全ての通信データを監視し、アクセスパターンをリアルタイムに解析して、不正な通信を検出する手法は、処理の負担が大きすぎるため、実現が困難である。
【０００７】
このため携帯電話機をインターネット接続端末として使用する無線通信システムでは、従来の有線環境で用いられていた方法とは異なる、携帯電話機に適したＤｏＳ攻撃に対する防御手段が必要となる。
【０００８】
本発明は、機器の大きさ、消費電力等を必要とせず、高速のＣＰＵを用いることなく不正な通信を検出することができる、無線通信システムに適したＤｏＳ攻撃に対する防御手段を有する携帯電話機を提供することを目的とする。
【０００９】
【課題を解決するための手段】
第１の発明は、無線通信機の動作を制御する制御部を有し、無線通信網と接続してデータの送受信を行う無線通信機において、前記制御部は、前記無線通信網から受信するデータ量が所定期間に渡り所定量以上であることを検出し、かつ、前記所定期間に渡り受信した前記データの送信元が所定数以上であることを検出すると、該無線通信機に対するデータの宛先（例えば、ＩＰアドレス）を変更するように動作することを特徴とする。
【００１０】
第２の発明は、第１の発明において、前記制御部は、前記無線通信機が受信しているデータの転送速度を検出する検出手段と、前記受信したデータの送信元アドレスを記録する記録手段と、前記無線通信網から受信するデータ量が所定期間に渡り所定量以上であることが検出された場合、前記所定期間中に前記記録手段に記録されたアドレス数が所定数以上であるか否かを判定する判定手段と、該無線通信機に対するデータの宛先を変更するように動作する宛先変更手段と、を備えることを特徴とする。
【００１１】
第３の発明は、第１又は第２の発明において、第１の通信方式及び第２の通信方式（例えば、cdma2000 1x-EV DO方式（又はHDR方式）及びcdma2000 1x方式と）によって前記無線通信網と接続してデータの送受信が可能であって、前記制御部は、前記無線通信網との間で接続する通信方式を変更することによって、該無線通信機に対するデータの宛先を変更するように動作することを特徴とする。
【００１２】
第４の発明は、第３の発明において、前記第２の通信方式は、無線通信機が接続される毎に該無線通信機に対するデータの宛先を割り当てることを特徴とする。
【００１３】
第５の発明は、無線通信網と、前記無線通信網と接続しデータの送受信を行う無線通信機と、を備える無線通信システムにおいて、前記無線通信機は、前記無線通信機は、前記無線通信網から受信するデータ量が所定期間に渡り所定量以上であることを検出し、かつ、前記所定期間に渡り受信した前記データの送信元が所定数以上であることを検出すると、前記無線通信網に報知し、前記無線通信網は、前記無線通信機からの報知に基づいて、

該無線通信機に対するデータの宛先を変更することを特徴とする。

【００１４】

第６の発明は、第５の発明において、第１の通信方式及び第２の通信方式によって前記無線通信網と前記無線通信機とを接続してデータの送受信が可能であって、前記無線通信網と前記無線通信機との間を接続する通信方式を変更することによって、該無線通信機に対するデータの宛先を変更することを特徴とする。

【００１５】

なお、第５又は第６の発明において、前記第２の通信方式は、無線通信機が接続される毎に該無線通信機に対するデータの宛先を割り当てるように構成するとよい。

【００１６】

【発明の作用および効果】

第１の発明では、無線通信機の動作を制御する制御部を有し、無線通信網と接続してデータの送受信を行う無線通信機において、前記制御部は、前記無線通信網から受信するデータ量が所定期間に渡り所定量以上であることを検出し、かつ、前記所定期間に渡り受信した前記データの送信元が所定数以上であることを検出すると、該無線通信機に対するデータの宛先を変更するように動作するので、無線通信機へ一斉にアクセスすることで異常負荷をかけ該無線通信機を利用不可能とするＤｏＳ攻撃を受けたときでも、無線通信機が利用不可能となることを回避することができる。また、無線通信機に対するデータの宛先が変更されるので、該一斉アクセスのデータが無線通信機に届かず、無線通信回線が占有されることがなく、無線資源を有効に利用することができる。

【００１７】

第２の発明では、前記制御部は、前記無線通信機が受信しているデータの転送速度を検出する検出手段と、前記データの送信元アドレスを記録する記録手段と、前記無線通信網から受信するデータ量が所定期間に渡り所定量以上であることが検出された場合、前記所定期間中に前記記録手段に記録されたアドレス数が所定数以上であるか否かを判定する判定手段と、該無線通信機に対するデータの宛先を変更するように動作する宛先変更手段と、を備えるので、第１の発明の効果に加え、ＤｏＳ攻撃と通常のアクセスとを簡単に判別することができる。

【００１８】

第３の発明では、第１の通信方式及び第２の通信方式によって前記無線通信網と接続してデータの送受信が可能であって、前記制御部は、前記無線通信網との間で接続する通信方式を変更することによって、該無線通信機に対するデータの宛先を変更するように動作するので、前述した発明の効果に加え、２つの無線方式を備えた無線通信機に特別なハードウェアを追加することなく、ＤｏＳ攻撃に対する防御を可能とし、無線通信機が利用不可能となることを回避することができる。

【００１９】

第４の発明では、前記第２の通信方式は、無線通信機が接続される毎に該無線通信機に対するデータの宛先を割り当てるので、前述した発明の効果に加え、第２の通信方式において携帯電話機に対するデータの宛先が固定されていないことから、前述した発明における効果に加え、多量に送信されたデータが無線通信機に届きにくくなり、ＤｏＳ攻撃に対して効果的に無線通信機の利用不可能状態を回避することができる。

【００２０】

第５の発明では、無線通信網と、前記無線通信網と接続しデータの送受信を行う無線通信機と、を備える無線通信システムにおいて、前記無線通信機は、前記無線通信網から受信するデータ量が所定期間に渡り所定量以上であることを検出し、かつ、前記所定期間に渡り受信した前記データの送信元が所定数以上であることを検出すると、前記無線通信網に報知し、前記無線通信網は、前記無線通信機からの報知に基づいて、該無線通信機に対するデータの宛先を変更するので、ＤｏＳ攻撃を受けたときでも、無線通信機が利用不可能となることを回避することができる。また、前記無線通信網は、該無線通信機に対するデータの宛先を変更するので、該一斉アクセスのデータが無線通信機に送信されず、無線

通信回線が占有されることがなく、無線資源を有効に利用することができる。

【００２１】

第６の発明では、第１の通信方式及び第２の通信方式によって前記無線通信網と前記無線通信機とを接続してデータの送受信が可能であって、前記無線通信網と前記無線通信機との間を接続する通信方式を変更することによって、該無線通信機に対するデータの宛先を変更するので、第５の発明の効果に加え、２つの無線方式を備えた無線通信機や無線通信網に特別なハードウェアを追加することなく、ＤｏＳ攻撃に対する防御を可能とし、無線通信機が利用不可能となることを回避することができる。

【００２２】

【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して説明する。

【００２３】

図１は、本実施の形態の携帯電話機１の主要な構成を示すブロック図である。

【００２４】

アンテナ１０は、切替部１７を介して、送受信部に接続されており、無線基地局からの電波を受信し、無線基地局に対し電波を送信する。送受信部は、cdma2000 1x-EV DO方式で無線通信をする1x-EV DO無線処理部１１と、cdma2000 1x方式で無線通信をするcdma2000 1x無線処理部１６とで構成されている。また、各無線処理部１１、１６には、各々送信部、受信部及びベースバンド処理部が設けられ、送信部はアンテナ１０から送信する高周波信号を生成する。受信部はアンテナ１０で受信した高周波信号を増幅、周波数変換等をして、ベースバンド信号を生成する。ベースバンド処理部は、ベースバンド信号を音声信号に復調し、音声信号を変調してベースバンド信号を生成する。すなわち、本実施の形態の携帯電話機１は、方式の異なる、1x-EV DO無線処理部１１と、cdma2000 1x無線処理部１６との２つの無線通信手段を備えたので、２つの無線通信手段を切り替えて、２つの無線通信方式にて基地局と通信（データ通信）することができる。

【００２５】

切替部１７は、ＣＰＵ１２によって制御され、アンテナ１０と無線処理部１１、１６とを選択的に接続して、基地局と接続する無線通信方式を切り替える。

【００２６】

ＣＰＵ１２は、メモリ１３に記憶されたプログラム及びデータに基づいて、無線処理部１１、１６、切替部１７、表示部１４、入出力部１５等の携帯電話機の各部を制御する。また、無線処理部１１、１６において送受信する周波数や、送受信タイミング、送信する電波の出力等も制御する。

【００２７】

メモリ１３には、無線通信回線を通じて取得したデータが保存される。特に本発明では、受信データの送信元ＩＰアドレスを収集したＤｏＳアクセスリストがメモリ１３に記憶される。

【００２８】

表示部１４は、表示素子と、ＣＰＵ１２からの表示データによって表示素子（液晶表示パネル）を駆動するドライバ回路とによって構成されており、無線通信回線を介して送られてきた文字情報や、操作に関する情報として操作メニュー、入力項目や、キー入力のエコーバック等を表示する。入出力部１５は、文字、数字の入力、携帯電話機への動作の指示を受け付けるキーボード及びキーボード制御回路によって構成されている。

【００２９】

さらに、携帯電話機には、音響信号を電気信号に変換する送話部（図示省略）、電気信号を音響信号に変換する受話部（図示省略）を有している。

【００３０】

図２は、本発明の実施の形態の携帯電話機が接続されるネットワークシステムの構成図である。

【００３１】

インターネットに接続可能な端末である携帯電話機１は、２つの無線方式によって通信可能であり、cdma2000 1x方式の携帯電話ネットワーク２、又は、cdma2000 1xEV-DO方式の高速データ通信ネットワーク３を選択して、いずれかのネットワークに接続され、該ネットワークを介してインターネットに接続されている。

【００３２】

cdma2000 1x方式携帯電話ネットワーク２は、cdma2000 1x方式の無線基地局２０、携帯電話網２１、公衆網接続ゲートウェイ２２及び制御装置（図示省略）とによって構成されている。cdma2000 1x方式無線基地局２０は、携帯電話機１との間にcdma2000 1x方式による無線通信回線を設定して、携帯電話機１とcdma2000 1x方式携帯電話ネットワーク２とを接続する。携帯電話網２１は、複数の無線基地局と公衆網接続ゲートウェイ２２とを接続して、無線基地局２０を公衆網接続ゲートウェイ２２を介して公衆回線網４に接続する。公衆網接続ゲートウェイ２２は、携帯電話網２１と公衆回線網４との間で通信プロトコルを変換し、携帯電話網２１と公衆回線網４とを接続する。制御装置はcdma2000 1x方式携帯電話ネットワーク２を統括的に制御するものである。

【００３３】

公衆回線網４は、cdma2000 1x方式携帯電話ネットワーク２とインターネット接続サーバ６との間を接続する電話網である。インターネット接続サーバ６は、公衆回線網を介してダイヤルアップ接続によって、端末装置をインターネット接続する接続サーバである。

【００３４】

cdma2000 1xEV-DO方式高速データ通信ネットワーク３は、cdma2000 1xEV-DO方式の無線基地局３０及び制御装置（図示省略）とによって構成されている。cdma2000 1xEV-DO方式無線基地局３０は、携帯電話機１との間にcdma2000 1xEV-DO方式による無線通信回線を設定して、携帯電話機１とcdma2000 1xEV-DO方式高速データ通信ネットワーク３とを接続する。このcdma2000 1xEV-DO方式無線基地局３０はTCP/IP方式によってインターネット５と直接接続されている。制御装置はcdma2000 1xEV-DO方式携帯電話ネットワーク３を統括的に制御するものである。

【００３５】

インターネット５には、インターネット接続サーバ６、cdma2000 1xEV-DO方式の無線基地局３０（cdma2000 1xEV-DO方式高速データ通信ネットワーク３）及びコンテンツサーバー（インターネット接続端末）７、８が接続されており、TCP/IP方式によってデータを転送する。

【００３６】

図３は、本発明の実施の形態の携帯電話機１で実行されるＤｏＳ検出手順を示すフローチャートである。図３に示すＤｏＳ検出処理は以下の３つに処理に大別される。

【００３７】

図３に示すＤｏＳ検出処理は、まず、所定時間（Ｔdos）受信データの送信元アドレスをＤｏＳアクセスリスト（図５参照）に記録する。その後、前記所定時間（Ｔdos）経過後、ＤｏＳアクセスリストの登録数Ｄnとあらかじめ設定しておいた閾値Ｄtを比較して、アクセスリストの登録数Ｄnが閾値Ｄtを上回った場合（Ｄn＞Ｄt）、ＤｏＳ攻撃状態であると判断して、ＤｏＳ攻撃回避のため無線通信方式を変更するシステム切替処理を行う。

【００３８】

以下、図３に示すＤｏＳ検出処理の詳細の動作を説明する。

【００３９】

携帯電話機を使った無線データ通信では、携帯電話機と無線基地局との間でデータ通信回線を設定する際に最大通信速度を設定する。この携帯電話機と無線基地局との間の最大通信速度には、携帯電話機の性能や無線機基地局の性能の他に、携帯電話機と無線基地局との間の無線通信回線の通信品質や、無線チャネルの空き状態等の無線通信回線の状態によって決定される（１００）。

【００４０】

データ通信中、携帯電話機は、受信するデータの転送速度（下り受信データレート）を監

視し、受信データ速度が最大通信速度に達したか否かを検出する（１０１）。
【００４１】
そして、受信データ速度が最大通信速度に達していれば、多量のデータが携帯電話機に送信されており、携帯電話機がＤｏＳ攻撃を受けている可能性があると判定して、送信元アドレスの収集を開始する。すなわち、受信データ速度が最大通信速度に達していれば、ＤｏＳ監視タイマが動作中であるか否かを判定する（１０２）。そして、ＤｏＳ監視タイマが動作中でなければ（１０２で”Ｎｏ”）、ＤｏＳ監視タイマが起動する前の処理として、ＤｏＳアクセスリストを初期化（クリア）して（１０４）、所定時間の間に携帯電話機にデータを送信してきた送信元アドレスを収集するために、ＤｏＳ監視タイマを起動する（１０５）。そして、受信データの送信元ＩＰアドレスをＤｏＳアクセスリストに記録する（１０６）。
【００４２】
一方、ＤｏＳ監視タイマが動作中であれば（１０２で”Ｙｅｓ”）、ＤｏＳ監視タイマ値を所定の監視時間に対応する値（Ｔdos）と比較し、ＤｏＳ監視タイマがタイムアウトしているか否かを判定する（１０３）。ＤｏＳ監視タイマがタイムアウトしていなければ（１０３で”Ｎｏ”）、受信データの送信元ＩＰアドレスをＤｏＳアクセスリストに記録する（１０６）。
【００４３】
一方、ＤｏＳ監視タイマがタイムアウトしていれば（１０３で”Ｙｅｓ”）、送信元アドレスデータの収集を終了し、収集した送信元アドレスデータを分析する。すなわち、ＤｏＳアクセスリストの登録数Ｄnとあらかじめ設定しておいた閾値Ｄtとを比較する（１０７）。この比較の結果、アクセスリストの登録数Ｄnが閾値Ｄtを上回っていれば（Ｄn＞Ｄt）、多数の送信元装置から該携帯電話機に多数のデータが送信されていると判断し、ＤｏＳ攻撃状態と判断する（１０９）。
【００４４】
ＤｏＳ攻撃状態と判断された場合には、携帯電話機の表示部１４に、ＤｏＳ攻撃を受けている可能性がある旨を報知する画面を表示し、使用者に無線通信方式の切替を促す（１０９）。使用者からの無線通信方式の切替指示を待って（１１０）、無線通信方式の切替処理（システム切替処理）を実行する（１１２）。なお、ＤｏＳ攻撃状態と判断された場合に、ＤｏＳ攻撃を受けている可能性がある旨を表示部１４表示することなく、無線通信システムの切替処理を実行するように構成してもよい（１１１、１１２）。
【００４５】
例えば、cdma2000 1xEV-DO方式で通信しているときに、ＤｏＳ攻撃状態と判定されると、携帯電話機からcdma2000 1x方式によって発呼し、データ通信回線を再接続することで、当該携帯電話機に割り当てられるＩＰアドレスが変更される。特に、cdma2000 1x方式はダイヤルアップ接続によってデータ通信回線を接続するので、cdma2000 1x方式による接続時に当該携帯電話機に割り当てられるＩＰアドレスは一定の値とならない。
【００４６】
なお、本実施の形態では、ＤｏＳ攻撃状態と判定されると、携帯電話機から発呼して通信方式を変更するように構成したが、携帯電話機がＤｏＳ攻撃状態と判定すると、携帯電話機から無線通信網（cdma2000 1x方式の携帯電話ネットワーク２、cdma2000 1xEV-DO方式の高速データ通信ネットワーク３等）にその旨を通知して、無線通信網側から携帯電話機に発呼して、通信方式を変更して、データ通信回線を再接続するように構成してもよい。
【００４７】
一方、この比較の結果、アクセスリストの登録数Ｄnが閾値Ｄtを上回っていなければ（Ｄn≦Ｄt）、多数の送信元装置から多量のデータが送信されている状態ではなく、通常アクセス状態であると判断して、データ通信の処理を継続する（１０８）。
【００４８】
一方、受信データ速度が最大通信速度に達してなければ（１０１で”Ｎｏ”）、多量のデータが携帯電話機に送信されている状態ではなく、携帯電話機がＤｏＳ攻撃を受けている

可能性がないものと判定して、送信元アドレスを収集を中止する。すなわち、受信データ速度が最大通信速度に達していなければ、ＤｏＳ監視タイマが動作中であるか否かを判定する（１１３）。そして、ＤｏＳ監視タイマが動作中であれば（１１３で”Ｙｅｓ”）、ＤｏＳ監視タイマの動作を停止する。一方、ＤｏＳ監視タイマが動作中でなければ（１１３で”Ｎｏ”）、ステップ１０１に戻り、受信データ速度が最大通信速度に達しているか否かを判定する（１０１）。

【００４９】

このように、携帯電話機に、多数の送信元装置から多数のデータが送信されているときに、ＤｏＳ攻撃状態と判断して、無線通信方式を切り替えて、携帯電話機に割り当てられるＩＰアドレスを変更するので、該携帯電話機に対して送信されるデータが当該帯電話機に届かないことから、ＤｏＳ攻撃を回避することができる。また、無線通信方式自体を切替えることにより、無線通信回線が切断され、無線資源の浪費を防ぐこともできる。また、切り替えた各無線通信方式を接続時に携帯電話機にＩＰアドレスを割り当てるデータ通信システム（例えば、ダイヤルアップ接続によって接続されるデータ通信システム）とすれば、回線接続毎に当該携帯電話機に割り当てられるＩＰアドレスが変わることから、該携帯電話機に対して送信されているデータを有効に遮断することができる。

【００５０】

図４は、携帯電話機１がＤｏＳ攻撃を検出した場合の表示部１４の表示内容を示す。

【００５１】

画面の最上部には、携帯電話機の動作状態を示す図形（ピクトグラム）が表示されるピクト部が設けられている。本実施の形態のピクト部には、左から順に、携帯電話機が受信している基地局からの電波の強さを示す電界強度表示、通話状態を示す通話中表示、メールの着信を示す着信表示、携帯電話機の動作時間を示す電池残量表示がされている。画面の中央部には、「ＤｏＳ攻撃を受けている可能性があります。システム変更をお勧めします。システム変更しますか？」と、携帯電話機が他のコンピュータ装置からのＤｏＳ攻撃を受けていることを検出した旨と、システム変更を促す表示をする。そして、システムを変更するか否かの選択肢を表示する。

【００５２】

図５は、ＤｏＳ検出処理（図３）のステップ１０６で記録されるＤｏＳアクセスリストを示す説明図である。

【００５３】

ＤｏＳアクセスリストには、受信したデータの送信元アドレスが受信順に蓄積されている。そして、所定の監視時間（Ｔdos）終了後に、Ｄn個のデータ送信元のＩＰアドレスが記録されている。

【００５４】

このように、本実施の形態の携帯電話機１は、方式の異なる、1x-EV DO無線処理部１１と、cdma2000 1x無線処理部１６との２つの無線通信手段を備えたので、２つの無線通信手段を切り替えて、２つの無線通信方式にて基地局とデータ通信することができ、一方の無線通信方式でデータ通信を行っている状態で、インターネット５からのＤｏＳ攻撃等の過負荷攻撃を受けた場合、これを検出し、現在使用している無線方式を他方の無線通信方式に切替えることで、過負荷攻撃の被害を回避することができ、携帯電話機が利用不可能となることを回避することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態の携帯電話機の構成を示すブロック図である。

【図２】本発明の実施の形態の携帯電話機が接続されるネットワークシステムの構成図である。

【図３】本発明の実施の形態の携帯電話機のＤｏＳ検出手順を示すフローチャートである。

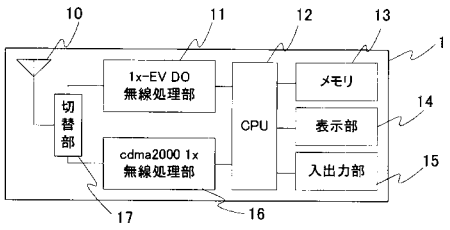
【図４】本発明の実施の形態の携帯電話機のＤｏＳ攻撃を検出時の表示内容である。メールの着信時の表示例である。

【図５】本発明の実施の形態の携帯電話機において蓄積されるＤｏＳアクセスリストの説明図である。

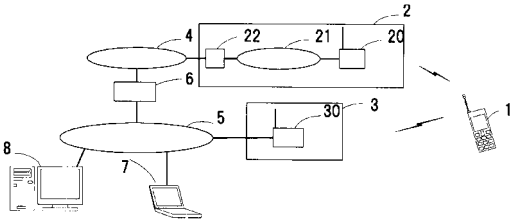
【符号の説明】

１　携帯電話機（インターネット接続端末）
２　携帯電話ネットワーク（cdma2000 1x）
３　高速データ通信ネットワーク（1xEV-DO）
４　公衆回線網
５　インターネット
６　インターネット接続サーバ
７　コンテンツサーバー（インターネット接続端末）
８　コンテンツサーバー（インターネット接続端末）
２０　無線基地局（cdma2000 1x）
２１　携帯電話網
２２　公衆網接続ゲートウェイ
３０　無線基地局（1xEV-DO）

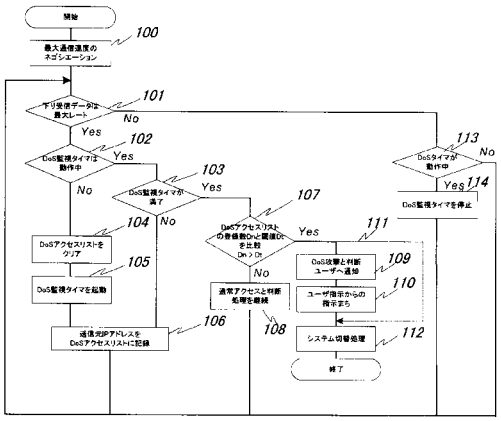
【図１】



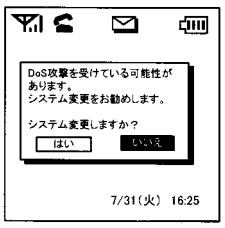
【図２】



【図３】



【図４】



【図５】

No	IP アドレス	
0	192 . 168 . 1 . 1	Dn
1	10 . 68 . 233 . 60	
2	12 . 31 . 45 . 34	
3	92 . 18 . 18 . 201	
n	133 . 206 . 60 . 21	

フロントページの続き

(56)参考文献 特開２０００－１６３３４１（ＪＰ，Ａ）
特開２００１－２１７８６１（ＪＰ，Ａ）
特開２００１－２３７８６９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 13/00、
H04B 7/24- 7/26、
H04L 12/00-12/26、12/50-12/66、
H04M 1/00、 1/24- 1/253、
1/58- 1/62、 1/66- 3/00、
3/16- 3/20、 3/38- 3/58、
7/00- 7/16、11/00-11/10、99/00、
H04Q 7/00- 7/38