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

特許第4567275号
(P4567275)

(45)発行日　平成22年10月20日(2010.10.20)　(24)登録日　平成22年8月13日(2010.8.13)

(51)Int.Cl.　　F I
G06F 21/22 (2006.01)　　G06F 9/06 66ON
H04W 4/00 (2009.01)　　H04B 7/26 M

請求項の数 4　(全 15 頁)

(21)出願番号　特願2002-54243(P2002-54243)
(22)出願日　平成14年2月28日(2002.2.28)
(65)公開番号　特開2003-256229(P2003-256229A)
(43)公開日　平成15年9月10日(2003.9.10)
審査請求日　平成16年10月12日(2004.10.12)
審判番号　不服2007-33804(P2007-33804/J1)
審判請求日　平成19年12月13日(2007.12.13)

(73)特許権者　392026693
株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目１１番１号
(74)代理人　100088155
弁理士　長谷川　芳樹
(74)代理人　100092657
弁理士　寺崎　史朗
(74)代理人　100121980
弁理士　沖山　隆
(74)代理人　100128107
弁理士　深石　賢治
(72)発明者　茂呂田　聡
東京都千代田区永田町二丁目１１番１号
株式会社エヌ・ティ・ティ・ドコモ内

最終頁に続く

(54)【発明の名称】移動通信端末、情報処理装置、中継サーバ装置、情報処理システム及び情報処理方法

(57)【特許請求の範囲】
【請求項１】
ウィルスの検出対象となるデータを格納する移動通信端末において、
処理しようとするデータにコンピュータウィルスが含まれているか否かの検出処理を情報処理装置に対して依頼するためにデータを当該情報処理装置に送信する送信手段と、
前記送信手段により送信されたデータに対する検出処理結果をウィルス管理情報として受信する受信手段と、
前記送信手段により送信されたデータと、前記受信手段により受信された検出処理結果若しくは検出処理が未処理であることを示すウィルス管理情報とを関連付けて格納する格納手段と、
前記移動通信端末が格納するデータに対するアクセス要求があると、前記格納手段に格納されているウィルス管理情報に基づいて、コンピュータウィルスが含まれている場合、または検出処理が未処理である場合には、前記格納手段に格納されているデータに対するアクセスを拒否するようにアクセス制御を行い、コンピュータウィルスが含まれていない場合には、前記格納手段に格納されているデータに対するアクセスを可能とするようにアクセス制御を行う制御手段とを備え、
前記格納手段は、前記受信手段により検出処理結果が受信されると、対応するデータのウィルス管理情報を更新することを特徴とする移動通信端末。
【請求項２】
請求項１に記載の移動通信端末から送信されたデータを受信する受信手段と、

前記受信手段によって受信されたデータについてコンピュータウィルスが含まれるか否かを検出する検出手段と、
前記検出手段による検出結果を前記移動通信端末に送信する送信手段とを備えることを特徴とする情報処理装置。
【請求項３】
請求項１に記載の移動通信端末と、請求項２に記載の情報処理装置とを備え、前記移動通信端末と前記情報処理装置間で通信を行うことを特徴とする情報処理システム。
【請求項４】
ウィルスの検出対象となるデータを格納する移動通信端末の情報処理方法において、
処理しようとするデータにコンピュータウィルスが含まれているか否かの検出処理を情報処理装置に対して依頼するためにデータを当該情報処理装置に送信する送信ステップと、
前記送信ステップにより送信されたデータに対する検出処理結果をウィルス管理情報として受信する受信ステップと、
前記送信ステップにより送信されたデータと、前記受信ステップにより受信された検出処理結果若しくは検出処理が未処理であることを示すウィルス管理情報とを関連付けて格納手段に格納する格納ステップと、
前記移動通信端末が格納するデータに対するアクセス要求があると、前記格納手段に格納されているウィルス管理情報に基づいて、コンピュータウィルスが含まれている場合、または検出処理が未処理である場合には、前記格納手段に格納されているデータに対するアクセスを拒否するようにアクセス制御を行い、コンピュータウィルスが含まれていない場合には、前記格納手段に格納されているデータに対するアクセスを可能とするようにアクセス制御を行う制御ステップとを備え、
前記格納ステップは、前記受信ステップにより検出処理結果が受信されると、対応するデータのウィルス管理情報を更新することを特徴とする移動通信端末の情報処理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、移動通信端末、情報処理装置、中継サーバ装置、情報処理システム及び情報処理方法に関する。
【０００２】
【従来の技術】
昨今の情報通信技術の発展はめざましく、情報化社会といわれる現代における我々の日常生活はますます便利になっている。例えば、インターネットの普及により、有用なアプリケーションプログラムやデータファイルをパーソナルコンピュータなどの端末装置に容易にダウンロードし、かつ利用できるようになってきた。
【０００３】
しかし、インターネットを介して端末装置にダウンロードされるものは、必ずしも有用なアプリケーションプログラムやデータのみではない。すなわち、有用なアプリケーションプログラムやデータを破壊するコンピュータウィルスもしばしば、インターネットを介して端末装置に侵入する。
【０００４】
端末装置にコンピュータウィルスが侵入したか否かを検出する技術としては、例えば、パターンマッチング方式のコンピュータウィルス検出技術が知られている。この技術は、コンピュータウィルスに含まれる特徴的なデータ列（以下、パターンデータという）を格納したデータベースをサーバ装置から端末装置に送信して端末装置に格納しておき、同じく端末装置に格納されているアプリケーションプログラムやデータと上述のパターンデータとの比較を行う。その結果、アプリケーションプログラムやデータが上述のパターンデータを含んでいたときは、そのアプリケーションプログラムやデータがコンピュータウィルスを含むと判断される。パターンマッチング方式のコンピュータウィルス検出技術を用い

る場合、コンピュータウィルスの検出確率を高めるためには、上記データベースが逐次最新のものに更新される必要がある。したがって、新種のコンピュータウィルスが発見されると、当該コンピュータウィルスに含まれる特徴的なパターンデータがサーバ装置から端末装置に対して送信され、端末装置の上記データベースが更新される。

【０００５】

【発明が解決しようとする課題】

しかし、上記従来の技術を携帯電話のような移動通信端末におけるコンピュータウィルスの検出に用いる場合、以下に示すような問題点があった。すなわち、移動通信端末は、パーソナルコンピュータなどの端末装置と比較して、メモリ容量やＣＰＵ能力が十分でない。したがって、上記データベース全体を移動通信端末に格納しておき、当該データベースに含まれるパターンデータ全てを網羅的に移動通信端末内のアプリケーションプログラムやデータと比較することは困難である。また、パーソナルコンピュータなどの端末装置とサーバ装置とは有線回線で接続されることが多いのに対して、移動通信端末とサーバ装置とは無線回線で接続される。したがって、上記データベース全体をサーバ装置から移動通信端末に対して送信したのでは、莫大な無線リソースを消費してしまう。これらの理由から、上記従来技術を用いたのでは、移動通信端末で使用されるデータについてコンピュータウィルスの検出を効率よく行うことができない。

【０００６】

そこで本発明は、上記問題点を解決し、移動通信端末で使用されるデータについてコンピュータウィルスの検出を効率よく行うことを可能とする移動通信端末、情報処理装置、中継サーバ装置、情報処理システム及び情報処理方法を提供することを課題とする。

【０００７】

【課題を解決するための手段】

上記課題を解決するために、本発明に係る移動通信端末は、ウィルスの検出対象となるデータを格納する移動通信端末において、処理しようとするデータにコンピュータウィルスが含まれているか否かの検出処理を情報処理装置に対して依頼するためにデータを当該情報処理装置に送信する送信手段と、前記送信手段により送信されたデータに対する検出処理結果をウィルス管理情報として受信する受信手段と、前記送信手段により送信されたデータと、前記受信手段により受信された検出処理結果若しくは検出処理が未処理であることを示すウィルス管理情報とを関連付けて格納する格納手段と、前記移動通信端末が格納するデータに対するアクセス要求があると、前記格納手段に格納されているウィルス管理情報に基づいて、コンピュータウィルスが含まれている場合、または検出処理が未処理である場合には、前記格納手段に格納されているデータに対するアクセスを拒否するようにアクセス制御を行い、コンピュータウィルスが含まれていない場合には、前記格納手段に格納されているデータに対するアクセスを可能とするようにアクセス制御を行う制御手段とを備え、前記格納手段は、前記受信手段により検出処理結果が受信されると、対応するデータのウィルス管理情報を更新することを特徴とする。

【０００８】

上記課題を解決するために、本発明に係る移動通信端末の情報処理方法は、ウィルスの検出対象となるデータを格納する移動通信端末の情報処理方法において、処理しようとするデータにコンピュータウィルスが含まれているか否かの検出処理を情報処理装置に対して依頼するためにデータを当該情報処理装置に送信する送信ステップと、前記送信ステップにより送信されたデータに対する検出処理結果をウィルス管理情報として受信する受信ステップと、前記送信ステップにより送信されたデータと、前記受信ステップにより受信された検出処理結果若しくは検出処理が未処理であることを示すウィルス管理情報とを関連付けて格納手段に格納する格納ステップと、前記移動通信端末が格納するデータに対するアクセス要求があると、前記格納手段に格納されているウィルス管理情報に基づいて、コンピュータウィルスが含まれている場合、または検出処理が未処理である場合には、前記格納手段に格納されているデータに対するアクセスを拒否するようにアクセス制御を行い、コンピュータウィルスが含まれていない場合には、前記格納ステップに格納されてい

るデータに対するアクセスを可能とするようにアクセス制御を行う制御ステップとを備え、前記格納ステップは、前記受信ステップにより検出処理結果が受信されると、当該検出処理結果をウィルス管理情報として記憶することを特徴とする。

【０００９】

これらの発明によれば、ウィルス管理情報に基づいて、格納手段に格納されているデータに対するアクセスを制御する。すなわち、ウィルス管理情報が、コンピュータウィルスが含まれることを示すデータ、又はコンピュータウィルスが含まれるか否かを検出する処理が未処理であることを示すデータに対しては、移動通信端末はアクセスを拒否する。これに対して、ウィルス管理情報が、コンピュータウィルスが含まれないことを示すデータに対しては、移動通信端末はアクセスを許可する。したがって、コンピュータウィルスに感染している、あるいは感染している可能性のあるデータが、アクセスにより読み出されることがない。その結果、コンピュータウィルスの拡大を未然に防止できる。

【００１１】

好ましくは、本発明に係る情報処理装置は、移動通信端末から送信されたデータを受信する受信手段と、前記受信手段によって受信されたデータについてコンピュータウィルスが含まれるか否かを検出する検出手段と、前記検出手段による検出結果を前記移動通信端末に送信する送信手段とを備える。

【００１２】

好ましくは、本発明に係る情報処理システムは、上述した移動通信端末と上述した情報処理装置とを備え、前記移動通信端末と前記情報処理装置間で通信を行う。

【００１４】

さらに、移動通信端末は情報処理装置にデータを送信し、送信されたデータについてコンピュータウィルスが含まれるか否かの検出結果をウィルス管理情報として受信する。すなわち、移動通信端末で使用されるデータについてのコンピュータウィルスの検出を情報処理装置が行う。したがって、移動通信端末は、高い処理負荷を伴うパターンデータの受信、格納、及び比較を行う必要がない。その結果、移動通信端末で使用されるデータについてコンピュータウィルスの検出を効率よく行うことが可能となる。また、移動通信端末は、コンピュータウィルスの検出対象となるデータと、当該データに関するウィルス管理情報とを関連付けて格納する。したがって、移動通信端末は、移動通信端末で使用されるデータについてコンピュータウィルスが存在するか否かを簡易迅速に識別できる。

【００２３】

【発明の実施の形態】

（第１の実施形態）

本発明の第１の実施形態に係る情報処理システムについて説明する。なお、本実施形態に係る情報処理システムは、本発明に係る移動通信端末、情報処理装置及び中継サーバ装置を含んでいる。

【００２４】

まず、本実施形態に係る情報処理システムの構成について説明する。図１は、本実施形態に係る情報処理システムのハードウェア構成図である。本実施形態に係る情報処理システム１は、携帯電話１００（移動通信端末）とウィルス検出装置２０（情報処理装置）と中継サーバ装置３０とサーバ装置４０とを備えて構成される。

【００２５】

携帯電話１００は、ウィルス検出装置２０と近距離無線通信が可能となっている。近距離通信技術としては、例えば、USB（Universal Serial Bus），Bluetooth（登録商標），IrDAなどが利用可能である。また、携帯電話１００は、移動通信網１０４を介して中継サーバ装置３０と接続されており、互いにデータ通信が可能となっている。更に、中継サーバ装置３０は、情報通信網１０２を介してサーバ装置４０と接続されており、互いにデータ通信が可能となっている。

【００２６】

次に、本実施形態に係る携帯電話の構成について説明する。図２は、携帯電話１００のハ

ードウェア構成図である。携帯電話１００は、ＣＰＵ１００ａ、半導体メモリなどのメモリ１００ｂ、中継サーバ装置３０との間でデータの送受信を行う通信装置１００ｃ、操作ボタンなどの入力装置１００ｄ、ＬＣＤ（Liquid Crystal Display）やＥＬ（Electro Luminescence）などの表示装置１００ｅ、マイクやスピーカなどの音声処理装置１００ｆを備えて構成される。ＣＰＵ１００ａ、メモリ１００ｂ、通信装置１００ｃ、入力装置１００ｄ、表示装置１００ｅ、音声処理装置１００ｆそれぞれは、バス１００ｇによって接続されており、互いにデータの送受信が可能となっている。

【００２７】

本実施形態に係るウィルス検出装置の構成について説明する。図３は、ウィルス検出装置２０のハードウェア構成図である。ウィルス検出装置２０は、ＣＰＵ２０ａ、メモリ２０ｂ、磁気ディスクや光ディスクなどの格納装置２０ｃ、携帯電話１００との間で近距離通信（Bluetooth, IrDAなど）を行う送受信装置２０ｄ、キーボードやマウスなどの入力装置２０ｅ、ディスプレイなどの表示装置２０ｆを備えて構成される。ＣＰＵ２０ａ、メモリ２０ｂ、格納装置２０ｃ、送受信装置２０ｄ、入力装置２０ｅ、表示装置２０ｆそれぞれは、バス２０ｇによって接続されており、互いにデータの送受信が可能となっている。

【００２８】

なお、本実施形態に係る中継サーバ装置３０のハードウェア構成は、ウィルス検出装置２０のハードウェア構成と同様である。すなわち、中継サーバ装置３０は、ＣＰＵ３０ａ、メモリ３０ｂ、格納装置３０ｃ、送受信装置３０ｄ、入力装置３０ｅ、表示装置３０ｆをそれぞれ備えて構成される。但し、送受信装置３０ｄは、移動通信網１０４を介して携帯電話１００との間で通信を行う点においてウィルス検出装置２０と異なる。

【００２９】

図４は、携帯電話１００とウィルス検出装置２０のシステム構成図である。携帯電話１００は、ウィルス検出装置とデータの送受信を行う移動通信端末であって、機能的には、データ格納部１０１と、データ送信部１０２（送信手段）と、検出結果受信部１０３（受信手段）と、ウィルス管理情報格納部１０４（格納手段）と、ウィルス検出結果処理部１０５とを備えて構成される。ここで、データ格納部１０１とウィルス管理情報格納部１０４とは、図２に示したメモリ１００ｂに対応する。データ送信部１０２と検出結果受信部１０３とウィルス検出結果処理部１０５とは、図２に示したメモリ１００ｂに格納されたソフトウェアがＣＰＵ１００ａによって実行されることにより実現する。

【００３０】

ウィルス検出装置２０は、コンピュータウィルスを検出する情報処理装置であって、機能的には、パターンデータデータベース２１と、データ受信部２２と、ウィルス検出部２３と、検出結果送信部２４とを備えて構成される。好適な実施例では、ウィルス検出装置２０は、コンビニエンスストアなどの店舗に設置されるタッチパネル操作の情報端末（Multi Media Kiosk端末）である。ここで、パターンデータデータベース２１は、図３に示したメモリ２０ｂに対応する。データ受信部２２とウィルス検出部２３と検出結果送信部２４とは、図３に示したメモリ２０ｂに格納されたソフトウェアがＣＰＵ２０ａによって実行されることにより実現する。

【００３１】

以下、携帯電話１００の各構成要素について詳細に説明する。データ格納部１０１には、ウィルスの検出対象となるデータ（アプリケーションプログラムやデータファイルを含む）が格納されている。データ送信部１０２は、ウィルス検出装置２０に対して、データ格納部１０１に格納されているデータをウィルス検出要求と共に送信する。検出結果受信部１０３は、ウィルス検出装置２０の検出結果送信部２４から送信される検出結果を受信する。

【００３２】

ウィルス管理情報格納部１０４には、ウィルス管理情報が格納されている。図５は、ウィルス管理情報格納部１０４の構成図である。ウィルス管理情報格納部１０４には、データ名とウィルス管理情報とが関連付けて格納されている。ここで、ウィルス管理情報とは、

対応するデータ名が示すデータについてコンピュータウィルスの検出処理が行われているか否か、及び検出処理が行われている場合にはコンピュータウィルスに感染している否かを示す情報である。例えば、ウィルス管理情報が「ＯＫ」とはデータがウィルスに感染していないことを示し、ウィルス管理情報が「ＮＧ」とはデータがウィルスに感染していることを示し、ウィルス管理情報が「未処理」とはデータについてコンピュータウィルスの検出処理が行われていないことを示す。なお、説明の便宜上、ウィルス管理情報格納部１０４には、データを特定するためのデータ名が格納され、データ自体はデータ格納部１０１に格納されているものとして説明したが、ウィルス管理情報格納部１０４にデータ自体が格納されているものとしてもよい。

【００３３】

図４に戻って、ウィルス検出結果処理部１０５は、検出結果受信部１０３が受信した検出結果を、ウィルス管理情報格納部１０４に格納し、検出結果をユーザに通知（表示を含む）する。

【００３４】

以下、ウィルス検出装置２０の各構成要素について詳細に説明する。パターンデータデータベース２１には、コンピュータウィルスに含まれる特徴的なデータ列であるパターンデータ（ファイル化されて「パターンファイル」と呼ばれることもある）が格納されている。なお、説明の便宜上、パターンデータデータベース２１にパターンデータ自体が格納されているものとして説明したが、パターンデータデータベース２１にはパターンデータの格納箇所を示すポインタが格納され、パターンデータ自体は当該ポインタによって示される格納箇所に格納されていてもよい。

【００３５】

データ受信部２２は、携帯電話１００のデータ送信部１０２から送信されたデータをウィルス検出要求と共に受信する。

【００３６】

ウィルス検出部２３は、パターンデータデータベース２１に格納されているパターンデータを用いて、データ受信部２２によって受信されたデータについてコンピュータウィルスが含まれるか否かを検出（ウィルススキャン）する。より詳細には、パターンデータデータベース２１に格納されたパターンデータと、データ受信部２２によって受信されたデータとを比較し、当該データに上記パターンデータと一致する部分が有るか否かを判断する。ここで、ウィルス検出部２３は、データに上記パターンデータと一致する部分が有る場合、当該データにコンピュータウィルスが含まれると判断し、データに上記パターンデータと一致する部分が無い場合、当該データにコンピュータウィルスは含まれないと判断する。

【００３７】

検出結果送信部２４は、ウィルス検出部２３によるコンピュータウィルスの検出結果を携帯電話１００に対して送信する。

【００３８】

続いて、本実施形態に係る情報処理システムの動作について説明し、併せて、本発明の実施形態に係る情報処理方法について説明する。図６は、本実施形態に係る情報処理システム１の動作を示すフローチャートである。本実施形態に係る情報処理システム１において、まず、データ送信部１０２によって、携帯電話１００からウィルス検出装置２０に対して、コンピュータウィルスの検出対象となるデータがウィルス検出要求と共に送信される（Ｓ１０２）。携帯電話１００から送信されたデータとウィルス検出要求とは、ウィルス検出装置２０のデータ受信部２２によって受信される（Ｓ１０４）。なお、携帯電話１００からウィルス検出装置２０に送信されるデータは、ユーザが明示的に選択してもよいし、ウィルス管理情報格納部１０４を基に未処理データを抽出してもよい。

【００３９】

ウィルス検出装置２０のデータ受信部２２によってデータとウィルス検出要求とが受信されると、ウィルス検出部２３によってコンピュータウィルスの検出が開始される（Ｓ１０

６）。すなわち、ウィルス検出部２３によって、パターンデータデータベース２１に格納されているパターンデータと、データ受信部２２によって受信されたデータとの比較が行われ、受信されたデータに上記パターンデータと一致する部分が含まれるか否かが判断される。なお、受信されたデータとパターンデータとの比較は、データの受信時、あるいは受信から一定時間経過後に開始されてもよいし、携帯電話１００のユーザの指示によって開始されてもよい。

【００４０】

次に、ウィルス検出部２３によるコンピュータウィルスの検出結果が、検出結果送信部２４から携帯電話１００に対して送信される（Ｓ１０８）。検出結果は、データ受信部２２によって受信されたデータにコンピュータウィルスが含まれるか否かを示す情報である。送信された検出結果は、携帯電話１００の検出結果受信部１０３によってウィルス管理情報として受信される（Ｓ１１０）。

【００４１】

ウィルス管理情報は、ウィルス検出結果処理部１０５により、ウィルス管理情報格納部１０４に格納され（Ｓ１１２）、コンピュータウィルスが存在したか否かの結果を表示して、ユーザに通知する（Ｓ１１４）。

【００４２】

続いて、本実施形態に係る情報処理システムの作用及び効果について説明する。本実施形態に係る情報処理システム１によれば、携帯電話１００はウィルス検出装置２０にデータを送信し、送信されたデータについてコンピュータウィルスが含まれるか否かの検出結果をウィルス管理情報として受信する。すなわち、携帯電話１００で使用されるデータについてのコンピュータウィルスの検出をウィルス検出装置が行う。したがって、携帯電話１００は、高い処理負荷を伴うパターンデータの受信、格納、及び比較を行う必要がない。その結果、携帯電話１００で使用されるデータについてコンピュータウィルスの検出を効率よく行うことが可能となる。

【００４３】

また、携帯電話１００は、コンピュータウィルスの検出対象となるデータと、当該データに関するウィルス管理情報とを関連付けて、データ格納部１０１とウィルス管理情報格納部１０４とに格納する。したがって、携帯電話１００は、携帯電話１００で使用されるデータについてコンピュータウィルスが存在するか否かを簡易迅速に識別できる。

【００４４】

（第２の実施形態）

続いて、本発明の第２の実施形態に係る情報処理システムについて説明する。

なお、本実施形態に係る情報処理システムは、本発明に係る移動通信端末を含んでいる。

【００４５】

まず、本実施形態に係る情報処理システムの構成について説明する。本実施形態に係る情報処理システムのハードウェア構成は、図１、図２及び図３を用いて説明した上記第１の実施形態に係る情報処理システム１のハードウェア構成と同様である。

【００４６】

図７は、本実施形態に係る携帯電話２００とウィルス検出装置２０のシステム構成図である。携帯電話２００は、機能的には、データ格納部２０１と、データ送信部２０２（送信手段）と、検出結果受信部２０３（受信手段）と、ウィルス管理情報格納部２０４（格納手段）と、ウィルス検出結果処理部２０５と、ウィルス管理情報取得部２０６と、アクセス制御部２０７（制御手段）とを備えて構成される。ここで、データ格納部２０１とウィルス管理情報格納部２０４とは、図２に示したメモリ１００ｂに対応する。データ送信部２０２と、検出結果受信部２０３と、ウィルス検出結果処理部２０５と、ウィルス管理情報取得部２０６と、アクセス制御部２０７とは、図２に示したメモリ１００ｂに格納されたソフトウェアがＣＰＵ１００ａによって実行されることにより実現する。

【００４７】

すなわち、本実施形態に係る携帯電話２００のシステム構成は、ウィルス管理情報取得部

２０６と、アクセス制御部２０７とを更に備える点において携帯電話１００と異なる。その他の構成要素であるデータ格納部２０１、データ送信部２０２、検出結果受信部２０３、ウィルス管理情報格納部２０４、ウィルス検出結果処理部２０５は、第１の実施形態に係るデータ格納部１０１、データ送信部１０２、検出結果受信部１０３、ウィルス管理情報格納部１０４、ウィルス検出結果処理部１０５とそれぞれ同様の構成を有する。なお、本実施形態に係るウィルス検出装置のシステム構成は、第１の実施形態に係るウィルス検出装置２０と同様の構成を有する。以下、ウィルス管理情報取得部２０６及びアクセス制御部２０７の各構成要素について詳細に説明する。

【００４８】

ウィルス管理情報取得部２０６は、データ格納部２０１に格納されているデータへのアクセス要求があると、データ名をキーにして、アクセスを要求されたデータに対応するウィルス管理情報をウィルス管理情報格納部２０４から取得する。

【００４９】

アクセス制御部２０７は、ウィルス管理情報取得部２０６によって取得されたウィルス管理情報に基づいて、データ格納部２０１に格納されているデータに対するアクセスを制御する。具体的な処理については後述する。

【００５０】

続いて、第１の実施形態と異なる携帯電話２００のウィルス管理情報取得部２０６とアクセス制御部２０７の動作について説明し、併せて、本実施形態に係る情報処理方法について説明する。図８は、本実施形態に係る携帯電話２００のウィルス管理情報取得部２０６とアクセス制御部２０７の動作を示すフローチャートである。本実施形態に係る携帯電話２００において、まず、データ格納部２０１に格納されているデータへのアクセス要求があると（Ｓ２０２）、ウィルス管理情報取得部２０６は、データ名をキーにして、アクセスを要求されたデータに対応するウィルス管理情報をウィルス管理情報格納部２０４から取得する（Ｓ２０４）。

【００５１】

ウィルス管理情報が「ＯＫ」である場合、アクセス制御部２０７は、アクセスを要求されたデータにコンピュータウィルスが存在しないものと判断し、当該データの読み出しを行う（Ｓ２０６）。一方、ウィルス管理情報が「ＮＧ」である場合、アクセス制御部２０７は、アクセスを要求されたデータにコンピュータウィルスが存在するものと判断し、当該データの読み出しを拒否する（Ｓ２０８）。この際に、データがウィルスに感染している旨を携帯電話２００のユーザに通知するメッセージを表示装置１００ｅに表示させてもよい。更に、ウィルス管理情報が「未処理」である場合、アクセス制御部２０７は、アクセスを要求されたデータに対してウィルス検出処理が施されていないものと判断し、当該データの読み出しを拒否する（Ｓ２０８）。この際に、データがウィルスに感染している可能性のある旨を携帯電話２００のユーザに通知するメッセージを表示装置１００ｅに表示させてもよい。

【００５２】

続いて、本実施形態に係る情報処理システムの作用及び効果について説明する。本実施形態に係る携帯電話２００によれば、第１の実施形態に記載した作用及び効果と同様の効果に加えて、アクセス制御部２０７は、ウィルス管理情報格納部２０４に格納されているウィルス管理情報に基づいて、データ格納部２０１に格納されているデータに対するアクセスを制御する。すなわち、ウィルス管理情報が、コンピュータウィルスが含まれることを示すデータ、又はコンピュータウィルスが含まれるか否かを検出する処理が未処理であることを示すデータに対しては、アクセス制御部２０７はアクセスを拒否する。これに対して、ウィルス管理情報が、コンピュータウィルスが含まれないことを示すデータに対しては、アクセス制御部２０７はアクセスを許可する。したがって、コンピュータウィルスに感染している、あるいは感染している可能性のあるデータが、アクセスにより読み出されることがない。その結果、コンピュータウィルスの拡大を未然に防止できる。

【００５３】

（第３の実施形態）
最後に、本発明の第３の実施形態に係る情報処理システムについて説明する。
なお、本実施形態に係る情報処理システムは、本発明に係る移動通信端末、中継サーバ装置及びサーバ装置を含んでいる。
【００５４】
まず、本実施形態に係る情報処理システムの構成について説明する。本実施形態に係る情報処理システムのハードウェア構成は、図１、図２及び図３を用いて説明した上記第１の実施形態に係る情報処理システム１のハードウェア構成と同様である。
【００５５】
図９は、携帯電話３００と中継サーバ装置３０とサーバ装置４０のシステム構成図である。携帯電話１００は、中継サーバ装置３０を介してサーバ装置４０からデータを受信する移動通信端末であって、機能的には、データ格納部３０１と、データ送信要求送信部３０２と、検出結果受信部３０３（受信手段）と、ウィルス管理情報格納部３０４（格納手段）と、ウィルス検出結果処理部３０５とを備えて構成される。ここで、データ格納部３０１とウィルス管理情報格納部３０４とは、図２に示したメモリ１００ｂに対応する。データ送信要求送信部３０２と検出結果受信部３０３とウィルス検出結果処理部３０５とは、図２に示したメモリ１００ｂに格納されたソフトウェアがＣＰＵ１００ａによって実行されることにより実現する。
【００５６】
中継サーバ装置３０は、サーバ装置４０から受信したデータについてコンピュータウィルスを検出する中継サーバ装置であって、機能的には、パターンデータデータベース３１と、データ受信部３２と、ウィルス検出部３３（検出手段）と、検出結果送信部３４（送信手段）とを備えて構成される。ここで、パターンデータデータベース３１は、メモリ３０ｂに対応する。データ受信部３２と、ウィルス検出部３３と、検出結果送信部３４とは、メモリ３０ｂに格納されたソフトウェアがＣＰＵ３０ａによって実行されることにより実現する。
【００５７】
以下、携帯電話３００の各構成要素について詳細に説明する。データ格納部３０１には、ウィルスの検出対象となるデータが格納されている。データ送信要求送信部３０２は、サーバ装置４０に対してデータ送信要求を送信する。検出結果受信部３０３は、中継サーバ装置３０の検出結果送信部３４から送信されるデータと検出結果とを受信する。
【００５８】
ウィルス管理情報格納部３０４は、第１の実施形態に係るウィルス管理情報格納部１０４と同一の構成を有する。すなわち、図５に示したように、ウィルス管理情報格納部３０４には、データ名とウィルス管理情報とが関連付けて格納されている。
【００５９】
図９に戻って、ウィルス検出結果処理部３０５は、検出結果受信部３０３が受信した検出結果によってデータにコンピュータウィルスが含まれると判断された場合、あらかじめ定められた設定情報に基づき、携帯電話３００のユーザへの警告処理、当該データの処理の禁止などを行う。また、データにコンピュータウィルスが含まれると判断されず、データをデータ格納部３０１に格納する場合には、データに合わせて、ウィルス管理情報をウィルス管理情報格納部３０４に格納する。
【００６０】
以下、中継サーバ装置３０の各構成要素について詳細に説明する。パターンデータデータベース３１には、コンピュータウィルスに含まれる特徴的なデータ列であるパターンデータが格納されている。なお、説明の便宜上、パターンデータデータベース３１にパターンデータ自体が格納されているものとして説明したが、パターンデータデータベース３１にはパターンデータの格納箇所を示すポインタが格納され、パターンデータ自体は当該ポインタによって示される格納箇所に格納されていてもよい。
【００６１】

データ受信部３２は、サーバ装置４０のデータ送信部４２から送信されたデータを受信する。ウィルス検出部３３は、パターンデータデータベース３１に格納されているパターンデータを用いて、データ受信部３２によって受信されたデータについてコンピュータウィルスが含まれるか否かを検出（ウィルススキャン）する。より詳細には、パターンデータデータベース３１に格納されたパターンデータと、データ受信部３２によって受信されたデータとを比較し、当該データに上記パターンデータと一致する部分が有るか否かを判断する。ここで、ウィルス検出部３３は、データに上記パターンデータと一致する部分が有る場合、当該データにコンピュータウィルスが含まれると判断し、データに上記パターンデータと一致する部分が無い場合、当該データにコンピュータウィルスは含まれないと判断する。

【００６２】

検出結果送信部３４は、データ受信部３２によって受信されたデータと、ウィルス検出部３３によるコンピュータウィルスの検出結果とを、携帯電話３００に対して送信する。

【００６３】

サーバ装置４０は、中継サーバ装置３０にデータを送信するサーバ装置であって、機能的には、データ格納部４１と、データ送信要求受信部４２と、データ送信部４３とを備えて構成される。以下、各構成要素について詳細に説明する。

【００６４】

データ格納部４１には、携帯電話３００に対して送信されるデータ（アプリケーションプログラムやデータファイルを含む）が格納されている。データ送信要求受信部４２は、携帯電話３００のデータ送信要求送信部３０２によって送信されたデータ送信要求を受信する。データ送信部４３は、データ格納部４１に格納されているデータと検出結果とを、中継サーバ装置３０を経由して携帯電話３００に送信する。

【００６５】

続いて、本実施形態に係る情報処理システムの動作について説明し、併せて、本発明の実施形態に係る情報処理方法について説明する。図１０は、本実施形態に係る携帯電話、中継サーバ装置及びサーバ装置の動作を示すフローチャートである。本実施形態に係る情報処理システムにおいて、まず、携帯電話３００のデータ送信要求送信部３０２によって、携帯電話３００からサーバ装置４０に対して、データ送信要求が送信される（Ｓ３０２）。携帯電話３００から送信されたデータ送信要求は、サーバ装置４０のデータ送信要求受信部４２によって受信される（Ｓ３０４）。

【００６６】

サーバ装置４０のデータ送信要求受信部４２によってデータ送信要求が受信されると、送信要求されたデータがデータ格納部４１から読み出され、データ送信部４３によって中継サーバ装置３０に送信される（Ｓ３０６）。送信されたデータは、中継サーバ装置３０のデータ受信部３２によって受信される（Ｓ３０８）。

【００６７】

中継サーバ装置３０のデータ受信部３２によってデータが受信されると、ウィルス検出部３３によって当該データについてコンピュータウィルスの検出が開始される（Ｓ３１０）。すなわち、ウィルス検出部３３によって、パターンデータデータベース３１に格納されているパターンデータと、データ受信部３２によって受信されたデータとの比較が行われ、受信されたデータに上記パターンデータと一致する部分が含まれるか否かが判断される。

【００６８】

ウィルス検出部３３による比較の結果、データ受信部３２によって受信されたデータに上記パターンデータと一致する部分が含まれない場合、上記データにはコンピュータウィルスが存在しないものと判断され、当該データと検出結果とが、検出結果送信部３４から携帯電話３００に対して送信される（Ｓ３１２）。送信された検出結果は、携帯電話３００の検出結果受信部３０３によってウィルス管理情報として受信される（Ｓ３１４）。

【００６９】

検出結果受信部３０３によって受信されたデータとウィルス管理情報とは、データ格納部３０１とウィルス管理情報格納部３０４とにそれぞれ格納される（Ｓ３１６）。データとウィルス管理情報とは、データ名をキーにして関連付けて格納される。

【００７０】

一方、ウィルス検出部３３による比較の結果、データ受信部３２によって受信されたデータに上記パターンデータと一致する部分が含まれる場合、上記データにはコンピュータウィルスが存在するものと判断され、検出結果が検出結果送信部３４から携帯電話３００に対して送信される（Ｓ３１８）。この場合、携帯電話３００のコンピュータウィルスの感染を防ぐため、データは送信されない。送信された検出結果は、携帯電話３００の検出結果受信部３０３によってウィルス管理情報として受信される（Ｓ３２０）。

【００７１】

続いて、本実施形態に係る情報処理システムの作用及び効果について説明する。本実施形態に係る携帯電話３００と中継サーバ装置３０とサーバ装置４０とによれば、携帯電話３００は中継サーバ装置３０からデータを受信する際に、受信するデータについてコンピュータウィルスが含まれるか否かの検出結果をウィルス管理情報として受信する。すなわち、携帯電話３００で使用されるデータについてのコンピュータウィルスの検出を中継サーバ装置３０が行う。したがって、携帯電話３００は、高い処理負荷を伴うパターンデータの受信、格納、及び比較を行う必要がない。その結果、携帯電話３００で使用されるデータについてコンピュータウィルスの検出を効率よく行うことが可能となる。なお、本実施形態において、携帯電話３００が受信するウィルス管理情報によって、携帯電話３００が受信するデータについてコンピュータウィルスが含まれるか否かの検出処理が未処理であることを通知するものとしてもよい。

【００７２】

本実施形態に係る情報処理システムを構成する中継サーバ装置とサーバ装置とは、物理的に別体の装置として配置されるものとしたが、物理的に１つのサーバ装置として配置されるものとしてもよい。反対に、中継サーバ装置が備える各構成要素は、複数のサーバ装置が分散して備えるものとしてもよい。同様に、サーバ装置が備える各構成要素は、複数のサーバ装置が分散して備えるものとしてもよい。

【００７３】

また、第２の実施形態においては、第１の実施形態に係る情報処理システムにウィルス管理情報取得部２０６とアクセス制御部２０７とが追加された情報処理システムについて説明したが、第３の実施形態に係る情報処理システムに、第２の実施形態で説明したウィルス管理情報取得部とアクセス制御部とを追加してもよい。これにより、携帯電話３００は、中継サーバ装置３０から受信したデータに対するアクセスをウィルス管理情報に基づいて制御することができる。

【００７４】

【発明の効果】

本発明の移動通信端末、情報処理装置、中継サーバ装置、情報処理システム及び情報処理方法によれば、移動通信端末は、高い処理負荷を伴うパターンデータの受信、格納、及び比較を行う必要がない。その結果、移動通信端末で使用されるデータについてコンピュータウィルスの検出を効率よく行うことが可能となる。

【図面の簡単な説明】

【図１】情報処理システムのハードウェア構成図である。

【図２】携帯電話のハードウェア構成図である。

【図３】ウィルス検出装置のハードウェア構成図である。

【図４】第１の実施形態に係る情報処理システムのシステム構成図である。

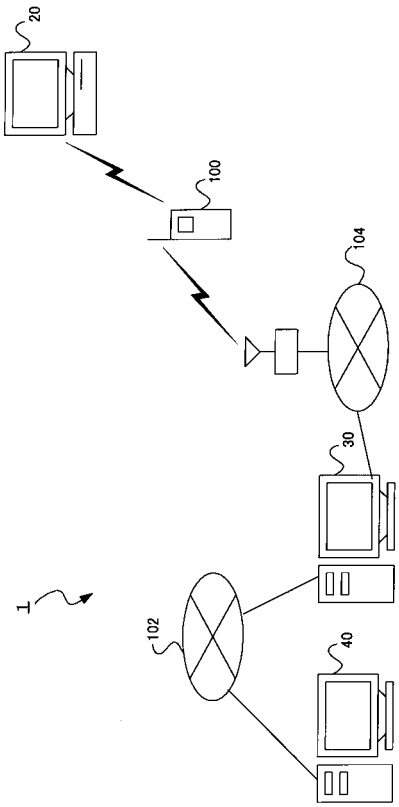
【図５】ウィルス管理情報格納部の構成図である。

【図６】第１の実施形態に係る情報処理システムの処理の流れを示すフローチャートである。

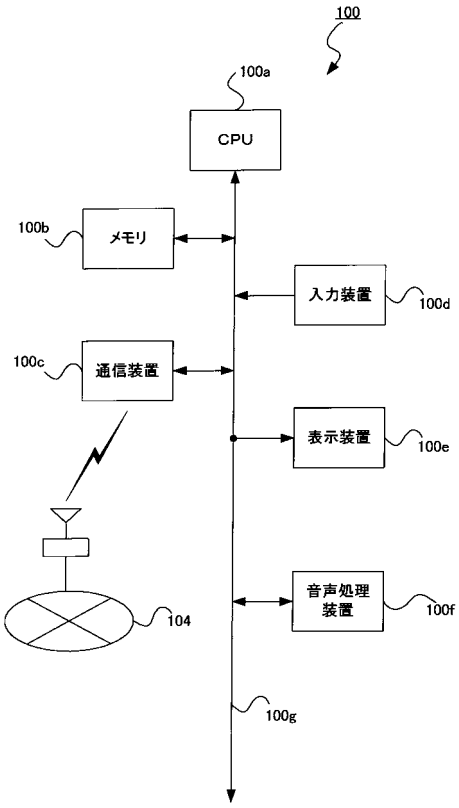
【図７】第２の実施形態に係る情報処理システムのシステム構成図である。

【図８】第２の実施形態に係る情報処理システムのウィルス管理情報取得部とアクセス制御部の処理の流れを示すフローチャートである。
【図９】第３の実施形態に係る情報処理システムのシステム構成図である。
【図１０】第３の実施形態に係る情報処理システムの処理の流れを示すフローチャートである。
【符号の説明】
１…情報処理システム、２０…ウィルス検出装置、３０…中継サーバ装置、４０…サーバ装置、１００，２００，３００…携帯電話

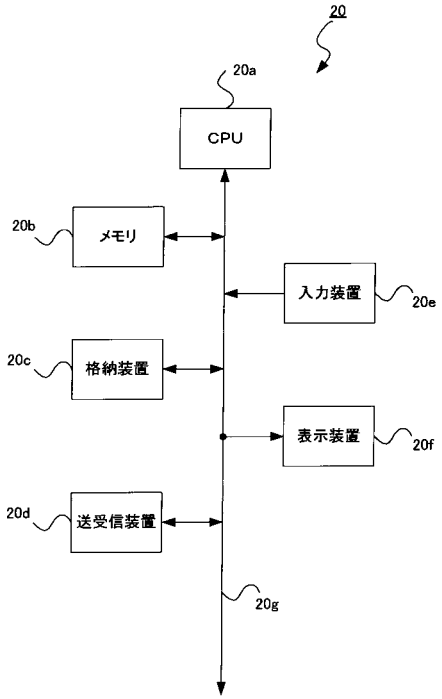
【図１】



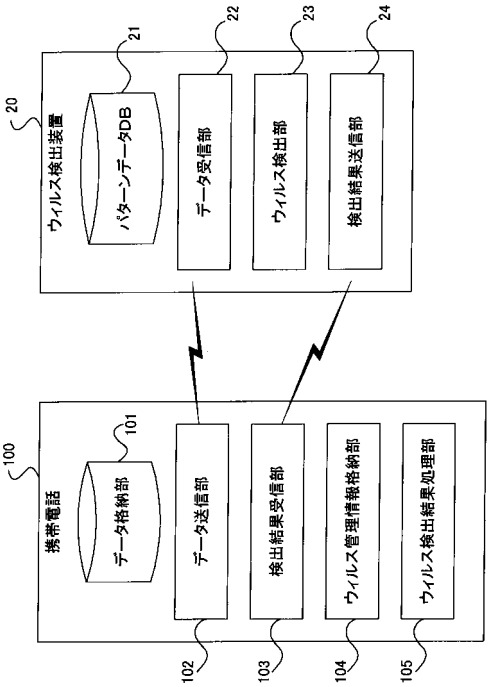
【図２】



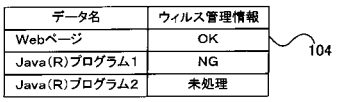
【図３】



【図４】



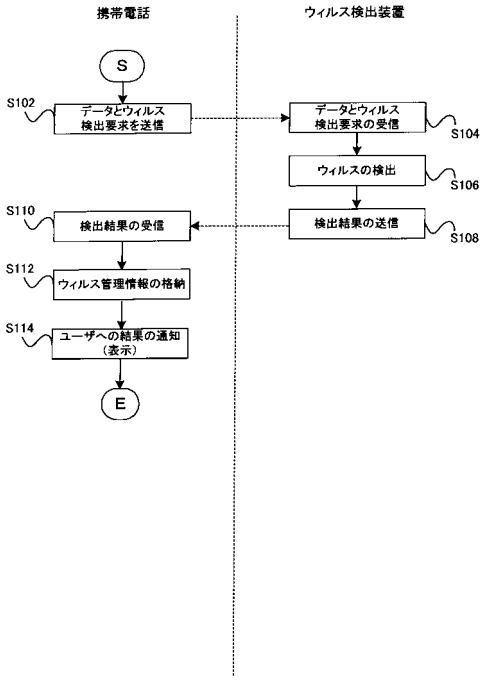
【図５】



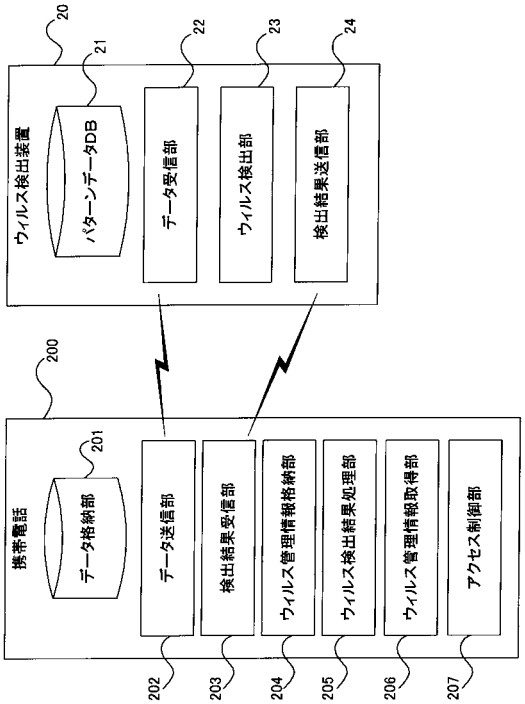
データ名	ウィルス管理情報
Webページ	OK
Java(R)プログラム1	NG
Java(R)プログラム2	未処理

104

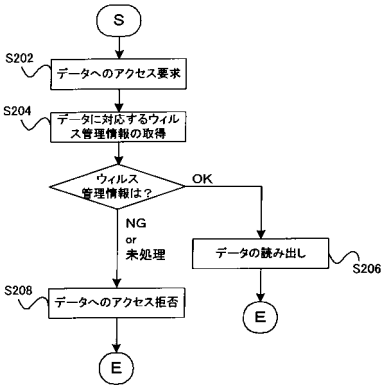
【図６】



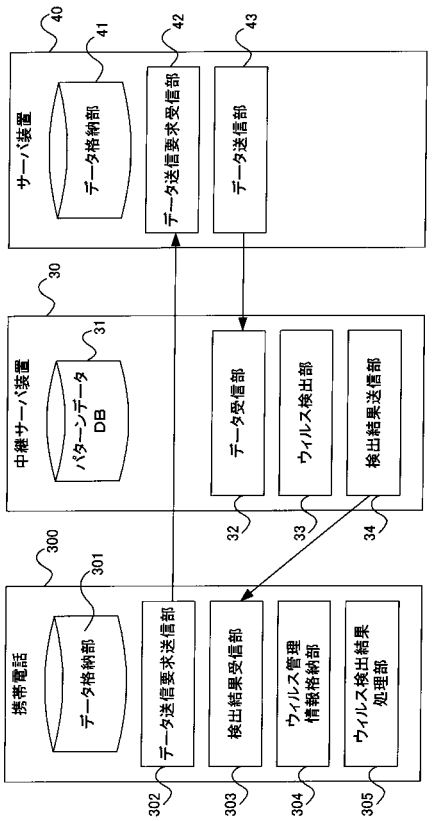
【図７】


20
21
22
23
24
ウィルス検出装置
パターンデータDB
データ受信部
ウィルス検出部
検出結果送信部
200
201
携帯電話
データ格納部
データ送信部
検出結果受信部
ウィルス管理情報格納部
ウィルス検出結果処理部
ウィルス管理情報取得部
アクセス制御部
202
203
204
205
206
207

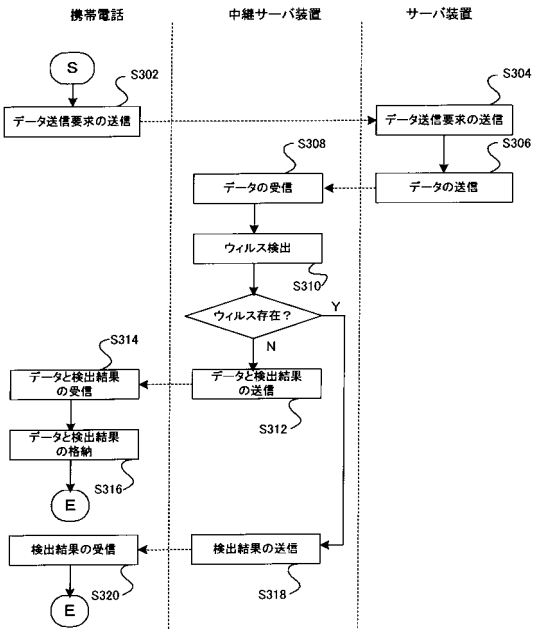
【図８】


S
S202
データへのアクセス要求
S204
データに対応するウィルス管理情報の取得
ウィルス管理情報は？
OK
NG
or
未処理
データの読み出し
S206
S208
データへのアクセス拒否
E
E

【図９】


40
41
42
43
サーバ装置
データ格納部
データ送信要求受信部
データ送信部
30
31
中継サーバ装置
パターンデータDB
データ受信部
ウィルス検出部
検出結果送信部
32
33
34
300
301
携帯電話
データ格納部
データ送信要求送信部
検出結果受信部
ウィルス管理情報格納部
ウィルス検出結果処理部
302
303
304
305

【図１０】


携帯電話
中継サーバ装置
サーバ装置
S
S302
データ送信要求の送信
S304
データ送信要求の送信
S306
データの送信
S308
データの受信
ウィルス検出
S310
ウィルス存在？
Y
N
S314
データと検出結果の受信
データと検出結果の送信
S312
データと検出結果の格納
S316
E
検出結果の受信
検出結果の送信
S318
E
S320

フロントページの続き

(72)発明者　浦川　康孝
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　加藤　達哉
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　石井　賢次
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内
(72)発明者　藤田　将成
東京都千代田区永田町二丁目１１番１号　株式会社エヌ・ティ・ティ・ドコモ内

合議体
審判長　赤川　誠一
審判官　清木　泰
審判官　吉岡　浩

(56)参考文献　“Ｇｒｏｕｐｍａｘ　Ｓｅｒｖｅｒ－Ｓｃａｎ　Ｖｅｒｓｉｏｎ６　解説・操作書　共通マニュアル”，株式会社日立製作所，２００１年1月３１日，第1版，2頁～8頁
高槻芳，“ファイル破壊ソフトも登場　ネットとの連係対策が不可欠”，日経コミュニケーション，日経ＢＰ社，２０００年１０月2日，第３２７号，９４頁～９６頁

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　9/06　660N，H04B　7/26　M