(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2013 年 5 月 16 日(16.05.2013)

WIPO | PCT

(10) 国際公開番号
WO 2013/069695 A1

(51) 国際特許分類:
G06F 21/56 (2013.01)

(21) 国際出願番号: PCT/JP2012/078868

(22) 国際出願日: 2012 年 11 月 7 日(07.11.2012)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2011-244002 2011 年 11 月 7 日(07.11.2011) JP
特願 2011-264038 2011 年 12 月 1 日(01.12.2011) JP

(71) 出願人: 株式会社アドバンス(KABUSHIKI KAISYA ADVANCE) [JP/JP]; 〒1038354 東京都中央区日本橋小舟町５番７号 Tokyo (JP).

(72) 発明者: 浦壁 伸周(URAKABE, Nobuchika); 〒1038354 東京都中央区日本橋小舟町５番７号 株式会社アドバンス内 Tokyo (JP).

(74) 代理人: 青木 篤, 外(AOKI, Atsushi et al.); 〒1058423 東京都港区虎ノ門三丁目５番１号 虎ノ門３７森ビル 青和特許法律事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

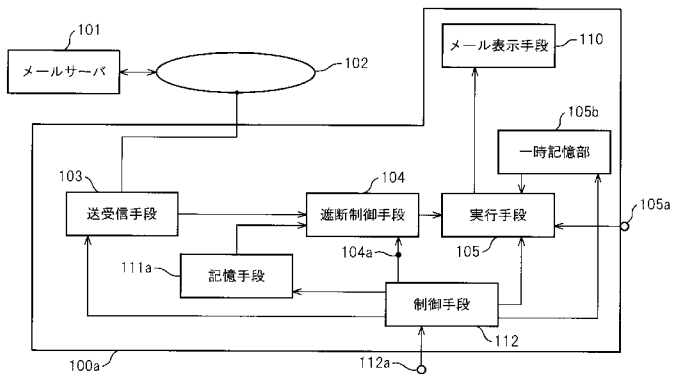
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）

(54) **Title**: SECURITY BOX

(54) 発明の名称 : 安全ボックス

図1A



101 Mail server
103 Transceiving means
104 Isolation control means
105 Execution means
105b Temporary storage
110 Mail display means
111a Storage means
112 Control means

(57) **Abstract**: Provided is a security box including: an input means for input of external data; an execution means for executing, in a predetermined area, external data input by the input means; and an isolation control means for isolating the execution area from other areas during execution. The security box can be further equipped with: a display means for displaying the behavior of external data executed by the execution means; a determination means for determining, on the basis of the behavior displayed by the display means, whether the external data is normal data; and a deletion means for deleting data that the determination mean has determined is not normal data and/or all of the data of the execution means.

(57) 要約: 外部データを入力する入力手段、前記入力手段で入力した外部データを所定の領域で実行する実行手段、前記実行時、前記実行領域をその他の領域から遮断する遮断制御手段を含んでなる安全ボックス。本安全ボックスは、前記実行手段で実行された外部データの挙動を表示する表示手段、前記表示手段で表示された挙動に基づいて、前記外部データが正常データか否かを判定する判定手段、前記判定手段で正常データでないと判定されたデータ及び／又は実行手段の全部のデータを消去する消去手段を更にさらに備えることができる。

WO 2013/069695 A1

明　細　書

発明の名称 ： 安全ボックス

技術分野

[0001] 本発明は、インターネットなどのネットワーク上のＷＥＢ（ウエブ）サーバ等への攻撃やダウンロードアプリケーション、メール関連データ、携帯メディアに記録されたデータ等に起因するウィルスプログラムの活動に影響されず、安全を確保した、プログラム実行環境を形成する安全ボックスに関するものである。

背景技術

[0002] 今般、ファイル名等、普通を装ったウィルス感染電子メールを用いる手法であって、感染相手を特定したいわゆるスピア型ウィルスの攻撃による感染が企業、官公庁、在外公館等で多発している。電子メールに添付されたファイルを開いただけで、表面的には、何ら変化が無い状態でありながら、コンピュータ内部で、悪意のソフトウェアが実行され、機密情報の外部への流出、外部からの遠隔操作、トロイの木馬的感染、コンピュータ機能動作の停止、さらには、感染相手によっては、電力、水道等の公共インフラを停止させたり、コンピュータ機能の停止等様々な事態を生じさせるおそれがある。このような感染相手を特定して配信される普通を装ったファイル名等を用いるウィルスプログラムを含む電子メールを送りつける手法は古典的ともいわれているが、未知のウィルスを利用することが容易で、既存のウィルス検査では、検出が困難なウィルスプログラムの感染を防御するためには、電子メール使用者が気をつけるしか有効な手だてがなく、このようなウィルスプログラムを含む電子メールの被害は、今後も引き続き生じ得ると考えられる。

[0003] また、遠隔操作を行う為にバックドア（裏口）を開いて、コンピュータを支配するトロイの木馬タイプのコンピュータウィルスは、相手が不特定であっても良く、又、その出現頻度が高いことから、ウィルス駆除ソフトウェアでは検出しにくい。又、一度コンピュータを支配してしまえば、自らの目的

の為に他人のコンピュータを利用できる為、メールに限らず、ホームページからの感染も多く発生している。

[0004] 一般的なウィルスプログラムを含む電子メールに対する駆除手法としては、例えば、ＰＯＰサーバにおいて受信した電子メールを、ウィルス駆除ソフトウェアによりパターンファイルと照合し、ウィルスが発見された場合にそれを駆除する操作をクライアントに電子メールが到着する事前または事後に駆除する手法がある。この方法において、パターンファイルは、過去のウィルスの情報や行動パターンが記載されたパターンファイル（定義ファイル）と、疑わしいファイルとを照合し、その内容と一致するか似ている場合、ウィルスと判断することから、データ名等に共通のウィルスの特徴があるような汎用的なウィルスに対してのものであり、特定の相手に感染させようとする為に普通を装ったファイル名やパターンファイルが未知のパターンを持った場合、検出はほぼ不可能な状況となる。また、未知のウィルスの発現が、数秒間隔で生じているとの報告がある現状では、更に汎用化されたウィルス阻止ソフトウェアでの保護を困難にしている。

[0005] 特開２００５－１５７５９８号公報には、添付ファイルと本文を分離した後、添付ファイルの構成データを安全な形式のデータに変換し、この変換後のデータにより構成されるファイルを形成し、先に使用者に配布された電子メールの本文と、添付ファイルを開く為のキーに基づいて、安全な添付ファイルを開く手法が記載されている。また、特開２００４－３８２７３号公報には、仮想ホストを構築して、ファイルを実行しウィルス感染を防止しながらウィルス検査をする装置が記載されている。

[0006] これらの手法で普通を装ったウィルスを含む電子メールを見抜くには、すべての添付ファイルをチェックする必要があり、安全化処理に時間と手間がかかる等、メールサーバ管理側の負担が大きくなり、簡易的な解決策までには至っていない。結局、普通を装った電子メールによる古典的な攻撃は、まず開けずに確認したあと削除するか、別の記録メディア等に移動させて、そこでウィルスチェックソフトにより、ウィルスチェックを行う予防策くらい

しかないのが現状である。

[0007] ウィルスメールの拡散は、メンテナンス不足の多数のサーバに感染した場合、時限的に特定のＷＥＢサーバに攻撃パケット等を送付して、コンピュータシステムの動作を不安定にして、商業的損害を与えたりする。

[0008] ここで、特定のＷＥＢサーバに攻撃パケットを集中的に送るＤＯＳ攻撃やＤＤＯＳ攻撃は、ファイヤーウオールに設けられているフィルタリング機能により、防ぐことができる。使用し得るフィルタリング機能には、静的フィルタリング、動的フィルタリング、ステートフル・インスペクション、アプリケーション・データの検査などがある。

[0009] しかしながら、上記のフィルタリング機能を使用するときには、あて先ＩＰアドレス、送信元ＩＰアドレス、プロトコル番号、あて先ポート番号、送信元ポート番号等を事前に登録しておく必要があった。また、これらの情報に該当しないものは、フィルタリング効果が得られなかったり、関連する動作（例えば、インターネット→ＬＡＮ→送信元ポート番号８０・送信元ＩＰアドレスが・・・，あて先ポート番号が・・・，あて先ＩＰアドレス・・・）を事前に動的に登録しておくことが必要であった。しかし、このように関連する動作に適合するものだけ通過させる場合でもやはり、事前の登録が必要である。

[0010] さらに、上記のような対処方法の場合、偽装されたパケットには必ずしも有効ではない。

先行技術文献

特許文献

[0011] 特許文献1：特開２００４－３８２７３号公報

特許文献2：特開２００５－１５７５９８号公報

特許文献3：特開２００６－２５４２６９号公報

特許文献4：特開２０１１－２２１９９３号公報

発明の概要

発明が解決しようとする課題

[0012] 感染相手を特定し、普通を装ったウィルスプログラムを含む受信メールおよび受信メールに添付されたデータファイル、未知のウィルスプログラムを含む受信メールおよび受信メールに添付されたデータファイル等による感染を防止する為には、使用者側が注意することしかなく、確実な防衛策は未だ存在しない。

[0013] このように、ウィルスメールの拡散は、ＤＤＯＳ攻撃やＤＯＳ攻撃の踏み台となるコンピュータを生産し、既存のフィルタリングでは除去不可能な偽装されたパケットによって、ＷＥＢサーバ、クラウドコンピューテイングシステム等に攻撃を加えてくる状態が依然として存在しており、これら悪意のある攻撃に対処する十分な手当する手法は未だ存在しない。

課題を解決するための手段

[0014] 上記に鑑み本発明は、電子メール関連データを送受信する送受信手段、該送受信手段で受信した電子メール関連データを実行し表示する実行領域と実行時、この実行領域とネットワーク接続部や、その他の接続領域を遮断する遮断手段、該遮断手段の遮断と接続を制御する制御手段の組み合わせ構成により前記実行領域で実行された電子メール関連データがたとえ、ウィルスプログラムを含むメールや、これらウィルスプログラムによって感染したデータが、普通を装った状態のものをうっかり開いたとしても、外部や、システムに影響を及ぼすことがなく、しかもウィルス感染を気にせず電子メールを開いて閲覧したり、返信、転送等の作業を可能とするシステムを実現した。換言すると、このシステムは、上記のような、プログラム実行環境を形成するに必要な複数の手段（ユニット）を備えたもの、すなわち、「安全ボックス」ということができる。

[0015] なお、コンピュータプログラムを用いたソフトウェアによる実行手段の場合、受信メールを実行させた後の実行領域におけるプログラムにウィルスが感染する場合もあることから、ウィルスプログラムを含む電子メール（以下、「ウィルスメール」という。）が確認された後、または受信したメール関

連データを開いて確認した後、等のタイミングで、制御手段は、記録手段等の記録データを消去するリセット信号を出力しても良く、また、上書きによって、消去に相当する状態を形成しても良い。

[0016] また、実行領域をＲＯＭ等の書き込み不可能なメモリにプログラムを記憶して、パラメータ等一部を記録する記録素子を用いる場合などもリセットする手段が不要になる場合もある。本発明における電子メールは、一般的なメールに限らず、相手が攻撃的に送信される情報であればよく、ＦＡＣＥＢＯＯＫ（登録商標）等、相手から送られてくる情報を受信し、表示する場合等も含まれ、少なくとも、相手が情報を得るためやシステムを破壊するため、その他、使用者を攻撃する為にウィルス情報を添付して、送信される情報であれば、本発明の電子メールに含まれるものである。メールの本文上から、特定の領域をクリックすると、ウィルス情報を含むサーバへ接続し、ウィルスプログラムをダウンロードして実行表示するＨＴＭＬメールも本発明で示す電子メールに含まれるものである。

[0017] 本発明における「ウィルスプログラム」とは、「コンピュータウイルス対策基準」(通商産業省告示)に示される、第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するものである。

（１）自己伝染機能：

自らの機能によって他のプログラムに自らを複製又はシステム機能を利用して自らを他のシステムに複製することにより、 他のシステムに伝染する機能。

（２）潜伏機能：

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能。

（３）発病機能：

プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能。

[0018] なお、その他の、例えば自己増殖機能をもち単独で活動するワームタイプ、自己増殖機能をもたないが、第三者のコンピュータを遠隔操作したり、パスワード等の個人情報を取得するトロイの木馬タイプ等もコンピュータウィルスとして示す。尚、ウィルスプログラムは、上述の他不正プログラム、すなわち設計者の意図が、個人情報取得、データ改ざん等にあり、最初から不正の目的で作られたプログラムも含まれ、ついうっかり開いてしまう様な内容の記載があるプログラムも含まれる。

[0019] 本発明におけるネットワークは、インターネット、イントラネット、エクストラネット、携帯電話、有線または光、電波、その他の電磁波等を伝達媒体とした無線による接続等が例示されるものである。

[0020] 「端末化した」とは、ノートブック、ネットブック、タブレット型ＰＣ、デスクトップパソコン、携帯電話、スマートフォン等を示すものであり、スタンドアロンタイプの独立したものを始め、仮想コンピュータモードのような一つのパーソナルコンピュータ上で駆動するソフトウェア上で仮想領域が形成された状態等を示す。

[0021] また、２次元の表示手段を用いずに、スイッチと、ＬＥＤの発光による表示程度の構成であっても良い場合もある。

[0022] 「メール関連データ」とは、メール本文、添付ファイル等を示すものであるが、少なくともウィルスが感染し得る形式のデータが含まれる。また、メールは、電子メールを意味する場合もあるが、少なくとも攻撃的な意図をもつデータであって、使用者または関連する者が起動させ実行させる可能性がある状況においてのデータを含むものであればよい。

[0023] なお、添付ファイルは、例えばＰＤＦファイルであれば、Ａｄｏｂｅ ｒｅａｄｅｒ（登録商標）が必要であるなど、データの形式によって、開く為のプログラムが異なるが、閲覧のみを可能とする容量の小さいビューアプログラムであってもよく、またウィルスプログラムを検出する目的だけの場合等は、開くためのプログラムを必要としない場合もある。

[0024] 本発明では、少なくとも、通常使用されるコンピュータの動作を行う構成

、ＯＳを備えていることが好ましいが、ウィルスプログラムの削除のみの場合は、閲覧表示を目的としたプログラムは不要になる場合もある。

[0025] 本発明における「その他の領域との遮断」とは、少なくとも、メール関連データがモニター上で実行されるかまたは、実行することを示す表示が表示される場合において、この表示操作以外の領域間の電気的接続が、一時的に遮断されることで、ネットワークとの接続や、起動関連プログラムとの接続との遮断を意味する場合もあるが、少なくともメール関連データが実行される際、影響があるその他のドライバソフトウェア、システムソフトウェア、ネットワーク接続関連ソフトウェアなど、ウィルスが目的としうるソフトウェアや、これらのソフトウェアが記録されている素子、接続機器、入出力端子とのデータ通信の遮断、ＯＳの相違、フォーマットの相違、信号パターンの相違等、電気的遮断が行われるものであれば「遮断」に含まれる場合もある。

[0026] 「一時的」とは、少なくとも、表示手段により電子メールの内容の表示がされている期間であって、ウィルスプログラムが実行状態となっている期間等を示すものである。

[0027] 遮断手段には、例えば、２入力以上の入力端と１出力端をもつＮＯＲ回路、ＮＡＮＤ回路等の論理回路、ロジックＩＣ、リレースイッチ、トランジスタ、ＦＥＴ等のスイッチング素子を用いた回路や一つのＯＳ上で異なる種類またはバージョンによる仮想的実行環境の形成による、形式の相違によるデータ伝達の遮断、異なるＯＳや、異なる形式を用いたプログラムを記録して実行する複数の素子の利用による実質的な遮断、等が例示されるが、特に限定されるものではない。

[0028] 本発明における制御手段は、遮断手段の遮断接続を行う入出力制御、実行手段の起動制御、記憶手段の記憶消去制御などを行うものであって、ロジックＩＣ、ＡＳＩＣ、等ハードウェアによる構成が好ましいが、ＲＯＭ、その他の記憶素子であって、書き込みが不可能な状態に設定された記憶素子にプログラムを記憶させたコンピュータ仕様のものであっても良い。

[0029] なお、制御手段は、使用者の手動による入力（ボタン、キーボード、マウス、タッチ操作等、マンマシンインタフェースによる入力）により、メールの閲覧開始終了、メールの削除できる機能を備えることが好ましい。ウィルスメールは、実際目的とする使用者を欺くタイトル、送信者を装っても、内容については、使用者の判断で、ウィルス添付の可能性が判断できることから、ウィルス検査機能が無くても、遮断手段によって、遮断された範囲で、電子メールの開封および閲覧、および削除機能だけでもよい場合もある。

[0030] 本発明における実行手段とは、例えばＣＰＵ、ＲＯＭ、ＲＡＭ等のメモリ素子を含むコンピュータ構成を示すもので、少なくともメール関連データが実行され、使用者が、視覚、聴覚等でメール内容が認識される出力手段が備わっているものであれば特に限定されない。

[0031] また、本発明における実行手段は、一つのＯＳプログラム上に、異なるバージョンで同一のＯＳが実行可能な環境、または異なる仕様のＯＳを実行させて、データ伝送上遮断した状態を形式する場合や、複数のＣＰＵを備えたマイコンチップ用いて、一方のＣＰＵでは、メールの送受信が行われ、他方のＣＰＵでは、メール関連データの実行表示が行われるが、必要に応じて、メール関連データ以外のデータの形式が相違する関係による遮断状態の形成を行うものであっても良い。

[0032] 一つのＯＳプログラム上で異なるバージョンのＯＳまたは異なる仕様のＯＳを用いる場合は、メール関連データを一時的に記憶できるＲＡＭ、ＵＳＢメモリ、ＳＤカード、ハードディスク、ＦＤ、ＣＤ－Ｒ等のメディア類からなる記憶手段であって、両ＯＳ間で読み取り書き込みができる記憶手段を備えることで、メール関連データの移動を行う場合もある。

[0033] 複数のＣＰＵを用いたマイコンチップの場合も同様に、上述した記憶手段を用いれば良い場合もある。

[0034] プログラムを読み込み実行する形式における実行手段の場合であって、ウィルスプログラムが実行され、プログラム記録部が、書き込み可能な領域の場合は、一つのメールを開く実行動作が終了した後、制御手段によりプログ

ラム記録部がリセットされ、他の記憶手段に記憶されたプログラムをプログラム記録部に記録または交換することで、実行手段自体の感染を防止することが好ましい。プログラム記録部のリセットは、データの完全消去と同等の操作が行われることが好ましく、さらには、デバイスの記憶を消去する電気的な操作を用いても良い場合もある。

[0035] 本発明におけるウィルスプログラムの検出手段として用いられる判定手段は、例えば、実行手段のＩ／Ｏポートの内のネットワークと接続するポートにおいて、電子メール本文の表示、添付ファイルの表示、実行の際、ほとんど出力が無い部分に、カウンタ、フリップフロップ、積分回路等を接続し、出力値がある一定の値を超えたとき、ウィルスが含まれているデジタル信号を出力する構成が好適に用いられる。

[0036] 本発明における「挙動」とは、実行手段で、データが実行される領域内のデータの移動に対応して外部で認識可能な情報であって、例えば、基板上のＩＣチップに入出力するデータによって生じる現象であって、目視での観察が可能なもの、例えば、光信号、超音波信号、音波信号、磁気信号、電磁気信号、熱信号から選ばれる１乃至複数の組み合わせを示す。

[0037] これらの観察可能な情報は、当然、センサーにより検出され、コンピュータ等による情報処理可能な装置に入力され、この入力により、様々なデバイスを駆動する構成も取り得る。すなわち、ウィルスプログラムの目的は、実行されることや感染すなわち、記憶、書き換え、データの消去等を行うこと、目的とする外部へデータを出力することにあり、感染のタイミングは、メール及び添付ファイルを開示し、確認する実行時点が最も多い。

[0038] このタイミングは、メーラープログラム上では、通常、データを書き込まないタイミングが生じることから、このデータを書き込まない状態及びデータを外部へ送信しない状態で、記憶手段への書き込み、ＬＡＮ等の外部へデータの送信といったデータの挙動が生じた場合、ウィルスプログラムの挙動を検出することになる。

[0039] また、データの挙動の時間、例えばメモリへの書込の際の、データの移動

量は、データの容量に対応する。ウィルスプログラムは、通常の文章データからくらべ、データ量が小さく、挙動も瞬間的である場合が多い。従って、挙動時間（例えば、メモリへのデータ書き込み時に、発光するＬＥＤの発光時間）によっても、ウィルスプログラムの存在を確認できる場合がある。又、ＲＡＭ等のデータが一時的に書き込まれ、実行する際、システムデータが記憶されるメモリの例えば、ＷＥ（ライトイネーブル）端子に接続されたＬＥＤの発光により、システム記憶用のメモリにデータが書き込まれたことを示し、通常、メールのデータを表示する場合、データの書き込みがされることがないタイミングで、データが書き込まれたことが検出されれば、そのデータがウィルスプログラムの実行の結果である可能性が十分高いことが理解される。尚、その際、マルチタスク型のＯＳでは、その他のタスクすなわちアプリケーションが動作していない方が好ましい場合がある。

[0040] また、データの移動順路が確認でき、データベースのデータが読み出され、ＬＡＮを介して外部へ送信される場合は、データベースのデータが読み出された記憶メモリに接続した読み出す挙動を表示する例えばＬＥＤが点滅、次にＬＡＮの送信状態を示すＬＥＤが点滅するなどの時系列的挙動を検出しても良い。ＬＥＤの点滅量は、データの大きさに対応している為、ウィルスプログラムが、実行され、データベースから、目的のデータを読み出し、ＬＡＮを介して、外部へ送信することの可能性が大きいことが認識できる。これが、メール及びメール添付データを開いた時点で発生した場合、ウィルスプログラムによる実行であることの可能性が更に大きくなる。

[0041] このような一連のメール開示操作の過程で、データの挙動を検出することで、ウィルスプログラムの存在が検出され、検出された結果、使用者にその存在を認識する表示を行うか、又は、ＯＳ及びその他のアプリケーションごと消去する操作をおこなっても良い。

[0042] この状態を構成する好適な例としては、例えば、フラッシュメモリ、ハードディスクとの接続が遮断され、且つＯＳ、アプリケーションがＲＡＭに書き込まれた状態での起動、いわゆるＲＡＭドライブによって起動した状態に

対し、リセットを手動又は自動で行う（消去手段）ことで、内部データを消去する手段が好ましい。この場合、ＯＳの容量が小さいもの例えば、ＷＩＮＤＯＷＳ　ＰＥ（商標）、ＷＩＮＤＯＷＳ　ＣＥ（商標）、ＡＮＤＲＯＩＤ（商標）又はＫＮＯＰＰＩＸ（商標）等を用いることにより、再起動時の時間が短縮される。このような、挙動の検出は、判断手段の一部を構成する場合もある。

[0043] 本発明で形成される端末例としては、スタンドアロンな端末であって、ネットワークと分離した状態では、特に遮断動作やその為の構成を設定する必要が無い場合もある。すなわち、ゲートアレイ化した状態や、ＲＯＭに記録されたプログラムによる実行であって、小容量の記憶素子を用いる場合は、遮断する必要がなく、そのまま実行されても良い場合もある。この場合の遮断とは、例えばネットワークとの接続が着脱自在な状態で、引き抜く様な仕様でネットワーク端子と本体を切り離す状態を意味する場合もある。

[0044] すなわち、電子メール本文、添付ファイル等のメール関連データを閲覧するだけの場合は、この状態の端末でもよい。

[0045] 更に、例えば、メール閲覧表示を行う端末で、ウィルスの感染をチェックし、感染が無い場合は、通常使用されるパーソナルコンピュータで再度、メールサーバから受信して、メール関連データを開くような仕様も例示される。

[0046] 返信、転送、保存など一連の実行を行う場合は、ウィルス検査のための判定手段を備えるものであってもよい。

[0047] システム領域のプログラムを遮断と接続する場合、例えば、システム関連のプログラムと、メール実行アプリケーションプログラムを異なる記憶手段に記憶させても良く、それぞれ異なるタイミングで、読み出して実行するものであっても良い。

[0048] また、システム領域、またはメール実行領域を含むアプリケーションを記憶する領域をＲＯＭ（リードオンリーメモリー）に記録する場合、この部分に遮断手段は不要となる場合もある。

[0049] ダウンロードアプリケーションに対する適用

本発明は、ＷＥＢサーバ、メールサーバから添付ファイル、メール本文をダウンロードしたアプリケーションプログラムや、データ及びＵＳＢメモリ等のメディアに既に含まれているウィルスプログラムをついうっかりと開いても、データの外部漏洩や、クラッキングによるコンピュータ破壊等の影響が無く、場合によってウィルスプログラムを識別して削除可能とする構成を具備する。

[0050] これは、例えば、データの伝送を遮断と接続の両方又は一方を外部信号によって制御可能な素子をメモリの入出力部やネットワークとの接続部に配置することで、実現可能とする。

発明の効果

[0051] 本発明は、メールの送受信を主とする端末化したものであって、メール関連データが実行される場合、ネットワーク、システムプログラム、その他ウィルスが感染を目的とする部分との接続を遮断することで、ウィルス感染がされていても問題なくデータが表示できることから、ウィルス感染を問題とすることなく、安定したメールのやりとりが可能となる。メール送受信専用端末であって、メールの安全を実現するボックス的な端末を実現する。

[0052] また、ウィルスプログラムの実行により、メール関連データの実行以外のＩ／Ｏポート等の入出力部分に信号が出力される場合、一度メモリに記憶して、宛先ＩＰアドレスを検索して検出された場合や、パケット信号に由来する情報を検出した場合、データを送信しようとする信号の出力をカウントしてある一定の閾値を超えた場合、又は、本来プログラムが相手に情報を送信する必要が無いのにもかかわらず、送信データを形成して出力している場合、その旨を液晶モニター、ＬＥＤに表示し、未知のウィルスの感染を検出することを可能とする場合もある。

[0053] この場合は、ウィルスのテンプレートファイルを必要とせず、更新も必要がなくなり、構成が簡素化される場合がある。

図面の簡単な説明

[0054] [図1A]図１Ａは、本発明の第１の実施形態を示すブロック図である。

[図1B]図１Ｂは、本発明の第２の実施形態を示すブロック図である。

[図2]図２は、本発明の第３の実施形態を示すブロック図である。

[図3]図３は、本発明の第４の実施形態を示すブロック図である。

[図4]図４は、本発明の第５の実施形態を示すブロック図である。

[図5]図５は、本発明の第６の実施形態を示すブロック図である。

[図6A]図６Ａは、本発明で使用しうる遮断接続手段の１回路構成を示す構成図である。

[図6B]図６Ｂは、本発明で使用しうる遮断接続手段の他の回路構成を示す構成図である。

[図6C]図６Ｃは、本発明で使用しうる遮断接続手段の他の回路構成を示す構成図である。

[図7]図７は、本発明の第７の実施形態を示すブロック図である。

[図8]図８は、本発明の第８の実施形態を示すブロック図である。

発明を実施するための形態

[0055] 引き続いて、本発明の好ましい形態を添付の図面を参照しながら説明する。なお、本発明は、以下に記載する特定の形態によって限定されるものではない。

[0056] 本発明は、ノートブック型、タブレット型、携帯型等に端末化されたもの（スタンドアロンタイプの端末）にメールの送受信手段および表示手段を備え、かつ受信したメールを実行手段で実行した場合、例えばネットワーク接続手段、起動システムプログラムと実行手段との間のデータ伝送を遮断する遮断手段を備える形態や、通常使用するコンピュータと接続可能で、コンピュータ側にメールの送受信手段を有し、接続端末側に遮断手段と実行手段を備えたものであっても良い。受信メールは、メールサーバ上で端末側が受信した時点で消去しない手段を設け、本発明で示す遮断手段を備えた実行手段によるメール表示を実行した後、ウィルスの感染等の確認をして、感染が無い場合、再度受信する形態もとることができる。

[0057] ウィルス感染メールが確認された後、遮断された領域の記憶データをリセットし、消滅させ、再度受信メールを読み込む前にプログラムをリセットされた記憶素子にコピーする構成を用いても良い。

[0058] 本発明は、データの伝送を遮断、接続を行う手段をハードディスク等、継続的に記憶する手段の入力部、ＬＡＮ、無線ＬＡＮ等のネットワークとの接続部であって、データの入出力部、ＵＳＢ等外部接続によって、データの記憶を行う手段とのデータの入出力部に配置することで、外部とのデータの入出力を規制し、またプロセッサによる実行を行う際のプログラム及ぶデータの記憶部分を一時的に記憶する記憶手段によって、ウィルスの感染を気にせず、データの処理を可能とする。また、外部攻撃に対しても、データ伝送の遮断後、データ処理を行う回路へ迂回させて、処理することで、防御可能となる。

[0059] 〔第１の実施形態〕

次に、図１Ａを参照して本発明の第１の実施形態を説明する。

[0060] 図１Ａにおいて、符号１００ａは本体を示す。本体１００ａは、スタンドアロンな形態を示すものであって、例えば、ディスプレイ、キーボード及びマウスを備えたもの、ディスプレイ、仮想キーボード、タッチパッド等を備えたものなどであり、より具体的には、ＰＤＡ型、デスクトップ型、ノート型、タブレット型、ネットブック型のコンピュータ仕様、スマートフォン、携帯電話等の形態により構成されることが好ましいが、これらの形態に限定されるものではない。本体１００ａは、使用者がメールを受信表示することができる態様であれば、如何なる形態も含まれる場合もある。

[0061] 符号１０１は、メールサーバを示す。メールサーバ１０１としては、一般的なＰＯＰサーバ、ＳＭＴＰサーバ等が例示され、送受信されるメールが一時的に蓄積される状態を形成し得る。

[0062] 符号１０２は、ネットワークを示す。ネットワーク１０２は、例えば、インターネット、エクストラネット、イントラネット、携帯電話回線等有線、無線または両方の組み合わせによって形成されている。

[0063] 符号１０３は、送受信手段を示す。送受信手段１０３は、ネットワーク１０２と有線または無線で接続され、メールおよびメール添付ファイルを送信または受信する部分であり、メールサーバとの交信が可能な状態に設定されていれば良い。

[0064] ネットワーク１０２と、送受信手段１０３とは、例えば、プロバイダを介してモデム、ルーター、無線ルーター、アンテナ等の中継端末で接続されていればよく、一般的な接続手段であれば良い。

[0065] 符号１０４は、遮断制御手段を示す。遮断制御手段１０４は、メール送受信の遮断と接続を行う部分であって、例えば、制御入力端を備えたＮＡＮＤ、ＮＯＲ等の論理回路、リレーの組み合わせ構成や、ソフトウェア的な遮断、例えば、異なるＯＳ間や異なるプログラム間での制限付きのデータの送受信構成等が例示される。遮断制御手段１０４は、少なくとも、データの遮断と接続を行うものであって、一方向にのみ移動可能な接続、または双方向に移動可能な接続が可能であれば良く、その目的で構成されるものであれば、特定されない。また、遮断制御手段１０４は、例えば、制御入力部１０４ａを介して入力されたデジタル信号の”１””０”信号によって、例えば、送受信手段１０３と実行手段１０５の間の遮断状態と接続状態の切り替え動作を実行することを可能としてもよい。

[0066] 実行手段１０５は、ＣＰＵおよびメモリ、記憶部および使用者から、キーボード、仮想キーボード、タッチパッド、マウス、その他のインタフェースによる入力部１０５ａを備えたコンピュータ仕様、あるいはゲートアレイ・セルベース(cell base):エンベッデドアレイ(embedded array):スタンダードセル(standard cell):ストラクチャードASIC等のＡＳＩＣを集積したカスタムあるいはセミカスタムＩＣ仕様で例示される。実行手段１０５は、少なくともメーラーと呼ばれるメール用プログラム、ＷＡＲＤ（登録商標）、Ａｄｏｂｅ ｒｅａｄｅｒ（登録商標）などの添付ファイルを開くプログラムが実行され、添付ファイルが開くことができる程度の機能が備われば良く、場合によっては、ＷＩＮＤＯＷＳ(登録商標）、ＬＩＮＵＸ(登録商標）、Ｍａｃ

ＯＳ（登録商標）等の汎用ＯＳが導入され、当該汎用ＯＳ上で動作するメーラープログラムがインストールされ実行される状態であってもよい場合もある。

[0067] 実行手段１０５において、メールを閲覧する場合は、キーボードは不要になる場合もあり、その他に、タッチパッド、マウス、ジョグダイヤル、スイッチ類、仮想スイッチ類で構成されても良い場合もある。

[0068] また、実行手段１０５は、遮断制御手段１０４の制御入力部１０４ａと接続し、遮断制御手段１０４のデータの接続、遮断を制御する出力を行っても良い場合もある。

[0069] 実行部に直接接続する記憶部は、書き込みが不可であって、添付ファイル表示用プログラム、ＯＳ、メーラーソフトウェア等が記憶されたものが好ましい場合もある。

[0070] また、実行手段１０５は、ストアードプログラム的なソフトウェアで形成される場合は、添付ファイルの開示等目的とする動作以外で使用されるドライバソフトウェアをあらかじめ取り除いた状態が好ましい場合もある。

[0071] 実行手段１０５は、送受信手段１０３から受信されたメールを一時記憶する一時記憶部１０５ｂを備えていることが好ましいが、特別に設ける必要はない。コンピュータ仕様であれば、一時記憶部に相当する記憶領域の一部を用いても良い場合もある。

[0072] なお、実行手段１０５は、例えばＰＤＦファイル（アドビ社）、ＷＡＲＤ（登録商標）ファイル、ＥＸＥＬ（登録商標）ファイルを読む為のソフトウェア（プログラム）であって、バージョンが更新される場合があるものを実行できるように、このソフトウェア（プログラム）を記憶した記憶メディアを着脱可能に備えていても良い場合もある。これらのバージョンアッププログラムを本体１００aに入力する為の入力部は、直接、実行手段１０５と接続している場合や、送受信手段１０３、遮断制御手段１０４を介して、設定されていても良く、その場合は、実行手段１０５で、データの安全性を確認する手段が備わっていても良い場合もある。尚、ファイル閲覧が主となる場合

は、ビューアー程度のプログラムで足りる場合もあり、バージョンアップの頻度は抑えられる場合がある。

[0073] 符号１１１ａは、記憶手段を示す。記憶手段１１１ａは、ＲＯＭのようなリードオンリーか読み取りだけ可能な状態に設定された記憶素子またはＲＡＭ等の読み書き可能な記録部である。記憶手段１１１ａとしては、例えば、フラッシュタイプの記憶素子、ＲＯＭ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ類、ＭＯ、ハードディスク、ＳＤカード、ＵＳＢメモリ、その他のメディアが例示される。記憶手段１１１ａは、本体１００aの大きさ、必要な記憶容量等により適宜選択できれば良い。

[0074] 保管手段（図示せず）、一時記憶部１０５ｂ、および削除保管手段（図示せず）は、記憶手段１１１ａで形成されても良いが、安全性を考慮して、別々の記憶素子、メディアで形成されても良い場合もある。また、記憶手段１１１ａは、遮断制御手段１０４と接続されている。これは、ウィルスが、実行手段１０５から記憶手段１１１aに侵入し記憶されることを阻止するためのものである。なお、メール関連プログラムがＲＯＭ化している場合、記憶手段１１１ａは、実行手段１０５に直接接続されていてもよい場合もある。

[0075] 記憶手段１１１ａには、メール開示プログラム、添付ファイル開示プログラム、および使用者のメールアドレス、パスワード、その他のアカウント情報が記録されている場合がある。使用者情報は、制御手段１１２に記録されていても良い場合もある。実行手段１０５がゲートアレイ等のカスタム、またはセミカスタムなハードウェアによる実行回路である場合は、記憶手段１１１ａには、メールアドレス、パスワード、アカウント等、電子メールによるデータの送受信に必要なデータだけが記録されても良い場合もある。

[0076] メール開示操作が終了した時点で、実行手段１０５に接続する一時的に記憶されたデータは削除されることが好ましい場合もある。

[0077] 削除が完了すると遮断制御手段１０４の遮断状態を接続状態にするために制御手段１１２は、制御入力部１０４ａに接続命令を出力する。制御手段１１２は、ゲートアレイ等のＡＳＩＣや、ロジックＩＣの組み合わせからなる

デジタル信号処理回路等のハードウェア構成または、ＲＯＭや読み取りだけ可能に設定された記憶素子に記憶されたプログラムで実行するコンピュータで構成され、使用者によるボタン操作、キーボード操作、タッチパッドによるタッチ操作等による制御入力部１１２ａを備えている。

[0078] 制御手段１１２は、遮断制御手段１０４の制御入力部１０４ａと接続する。また、制御手段１１２は、実行手段１０５、一時記憶部１０５ｂおよび記憶手段１１１ａ、送受信手段１０３と接続し、記憶のリセット、記憶手段１１１ａの記録プログラムを、一時記憶部１０５ｂへコピー、送受信手段１０３の送受信開始停止等の制御を行う手段である。制御手段１１２の動作は、制御入力部１１２ａからの入力により、または自動的に動作を行う場合がある。

[0079] 次に、図１Ａで示す実施形態の動作の説明を行う。なお、図１Ａでは、本体１００ａを上述したスタンドアロンな端末とした形態を示す。

[0080] 本体１００aの送受信手段１０３は、ネットワーク１０２と有線または無線で接続されている。

[0081] 制御入力部１１２ａから使用者の入力操作に基づいて、または予め設定された自動接続設定に基づいて制御手段１１２が、送受信手段１０３を起動させる。メールサーバ１０１の例えばＰＯＰサーバに一時的に蓄積された受信メールに対し、送受信手段１０３は、受信要求を行う。受信メールは、ネットワーク１０２を介して送受信手段１０３に入力され、遮断制御手段１０４へ出力される。制御手段１１２は、制御入力部１０４aに対し、接続する旨の信号を出力し、遮断制御手段１０４は、接続状態を形成して、実行手段１０５に受信メールが供給できる準備を整える。

[0082] 実行手段１０５は、この受信メールを例えば入力部１０５ａからの入力信号により受信する。なお、遮断制御手段１０４が遮断状態にあるばあいは、一時的に記録するバッファ的なメモリを備えておき、遮断制御手段１０４が接続状態を形成する迄記憶していても良い場合もある。

[0083] 制御手段１１２は、実行手段１０５に、受信メールが入力され、一時記憶

部１０５ｂに記憶されるか、送受信手段１０３で受信メールが受信された状態を検出し、遮断制御手段１０４の制御入力部１０４ａに接続を遮断する命令信号を出力する。

[0084] 遮断制御手段１０４は、実行手段１０５と送受信手段１０３間のデータ伝送を遮断するとともに、場合によっては、記憶手段１１１ａと、実行手段１０５間のデータ伝送を遮断する。

[0085] 一時記憶部１０５ｂに一時的に記憶された受信メールは、メール本文、添付ファイルともに実行手段１０５で入力部１０５ａからの入力に基づいてまたは自動設定がされている場合は、自動的に開示実行され、メール表示手段１１０で表示される。

[0086] メール表示手段１１０で表示された後、一時記憶部１０５ｂの受信メールは制御手段１１２からの信号により適宜消去される。この消去は、使用者の制御入力部１１２ａからの入力により行っても良く、自動消去設定の場合は、自動的に行っても良い。なお、この消去は、好ましくは、汎用メーラーの機能にあるような完全消去であることが好ましい場合もある。

[0087] 消去されるまで、制御手段１１２は、遮断制御手段１０４の制御入力部１０４ａに接続を遮断する命令信号を出力し維持する。

[0088] このように受信メールを参照するだけの場合は仮にウィルスに感染しても、遮断制御手段１０４によって、外部および記憶手段１１１ａへのデータ伝送が遮断されているため、ウィルスの外部への感染がないことから、使用者はウィルスの影響を受けることなくメールを読むことができる。

[0089] 制御手段１１２は、メールが開封され、メール表示手段１１０でメール表示動作を行った後、制御入力部１１２ａからの信号または、自動で、記憶手段１１１ａの記憶プログラムを接続状態の遮断制御手段１０４を介して実行手段１０５へ移転し、上書き的にコピーを行う場合もある。この上書きにより、仮に、実行手段１０５内に一時的に記憶されたプログラムにウィルスデータが挿入されたとしても、実質的にリセット状態となるからである。

[0090] 〔第２の実施形態〕

次に、図１Ｂを参照して本発明の第２の実施形態を説明する。図１Ｂでは、実行手段の読み書き可能な記録部がウィルスプログラムに感染した場合、これをリセットする構成を付加した実施形態を示す。なお、図１Ｂを参照した説明において、図１Ａと同じ構成の部分については、構成および動作の説明を省略する。

[0091] 図１Ｂにおいて、符号１１２は、制御手段を示す。制御手段１１２は、図１Ａで示した機能、動作の他に、例えば、記憶手段１１１ａに記録されたメーラー（電子メール表示作成用プログラム）を、実行手段１０５で実行させるために一時的に記録する第２記憶手段１１１ｂに記録したもの、その他記録バッファに記録されたデータなどを完全消去する手段を備えたものであり、ソフトウェア的な手法、ハードウェア的な手法のいずれを利用しても良いが、制御手段１１２が、例えば、デジタルのリセット信号を出力する出力回路の様なハードウェア的設定をすることが好ましい。

[0092] また、リセット後、制御手段１１２は、実行手段１０５で、受信メール関連データの実行表示を行うため、記憶手段１１１ａの記憶プログラムを第２記憶手段１１１ｂに移動コピーする機能を備える。この構成を形成する手法として、例えば、記憶手段間でデータをコピーするロジックＩＣによるハードウェア回路を備えても良い。

[0093] また、制御手段１１２は、記憶手段１１１ａから第２記憶手段１１１ｂへのデータのコピーを行うプログラムをＲＯＭとして持ち、第２記憶手段１１１ｂにこのＲＯＭの内容をコピーした状態とする手段も採用することができる。

[0094] また、制御手段１１２は、遮断制御手段１０４の制御入力部１０４ａと接続し、第２記憶手段１１１ｂの記憶内容がリセットさせた後、制御入力部１０４ａに記憶手段１１１ａと第２記憶手段１１１ｂを接続する旨の信号を出力する。

[0095] 第２記憶手段１１１ｂは、ＲＡＭ（ランダムアクセスメモリー）等、書き込み可能なチップで形成されることが好ましい。第２記憶手段１１１ｂは、

一時的記録領域であり、メーラー、メーラーによって作成されるパラメータ等を一時的に記録するものである場合もある。なお、プログラムが固定化されていて、ウィルスプログラムが内容を改ざん、削除、寄生的付加をせず、ＲＡＭ等、書き込み可能な記憶素子を備えないときは不要となる場合もある。

[0096] 次に、図１Ｂで示す実施形態の動作の説明を行う。なお、図１Ｂで示した実施形態は、ウィルス感染が確認された場合の動作以外は、図１Ａと同様の動作を行うので、説明を省略する。

[0097] 電子メールの本文の内容から、ウィルス感染が確認された電子メールである可能性がある場合、または、ウィルス感染を問題とすることなく電子メール閲覧作業が終了した場合、図１Ｂで示す制御手段１１２は、制御入力部１１２ａからの使用者による入力信号または自動入力信号により、実行手段１０５の受信メール開示動作をおこなったプログラムに起因した記録手段、記憶バッファの記録をリセットする為の信号を出力する。

[0098] 実行手段関連の記録がリセットされると、再度記憶手段１１１ａに記憶されたプログラムを読み込む必要がある場合がある。その場合は、制御手段１１２が出力する制御信号を、制御入力部１０４ａを介して遮断制御手段１０４に入力し、記憶手段１１１ａと第２記憶手段１１１ｂ間の接続を行い、記憶手段１１１ａに記憶されたプログラムを第２記憶手段１１１ｂに記憶させ、実行手段１０５が再度メーラープログラムを実行可能とするものであっても良い。このような初期設定用プログラムは、制御手段１１２が内蔵する書き込み不可能に制御された記録部に記録されることが好ましい。

[0099] なお、実行手段１０５が受信メールを受信して、それが、ウィルス感染のおそれが無い電子メールであった場合、必要に応じて、返信、転送手段を実行手段１０５が備えても良い。その場合、入力部１０５ａには、文章作成用のマンマシンインタフェースが接続されても良い。

[0100] 〔第３の実施形態〕

次に、図２を参照して本発明の第３の実施形態を説明する。

[0101] 図２で示す実施形態は、受信メールに対し、ウィルスの検出等を行う手段、ウィルス感染が無い場合のメールに対する返信、転送メール作成手段を付加したものである。なお、図２で示す構成において、図１Ａ及び図１Ｂと同様のものについては、同じ番号を付すことでここでの説明を省略する。なお、以下では、図１Ａ及び図１Ｂを総称して、図１と呼ぶこととする。

[0102] 符号１００ｂは、本体を示す。本体１００ｂは、スタンドアロンな形態を示すものである。本体１００ｂとしては、例えば、ディスプレイ、キーボード、マウスを備えたもの、ディスプレイ、仮想キーボード、タッチパッド等を備えたものが例示される。本体１００ｂは、より具体的には、ＰＤＡ型、デスクトップ型、ノート型、タブレット型、ネットブック型のコンピュータ仕様、スマートフォン、携帯電話等の形態により構成されることが好ましいが、これらの形態に限定されるものではなく、使用者が、メールを送受信することができる態様であれば、いかなる形態も含まれても良い。

[0103] 符号１０５ｂは、一時記憶部を示す。一時記憶部１０５ｂは、受信メールを一時的に記憶するためのものであり、受信メールは、この記憶部に一時的に記憶されている。

[0104] 符号１１２は、制御手段を示す。制御手段１１２は、図１で示した実施形態と同様、制御入力部１１２ａを備え、受信メールにウィルスメールが含まれている場合、一時記録手段（図示せず）の記録内容、実行手段１０５の記憶データを削除する信号を出力し、削除後、遮断制御手段１０４の制御入力部１０４ａへ、記録手段１１１ａと一時記録手段間の接続を行う信号を出力し、記録手段１１１ａのプログラム等の記録データを一時記録手段へ移動記録コピーする為の回路または手段を備えている。なお、制御手段１１２は、ハードウェア的な構成、ソフトウェア的な構成のいずれをも取り得るが、少なくとも、機能、動作が変更できない状態のものが好ましい。

[0105] 制御手段１１２は、送受信手段１０３、記憶手段１１１ａ、一時記憶部１０５ｂ、実行手段１０５、保管手段１０８、メール作成手段１０９と接続しても良く、動作の開始、停止、その他の記憶素子の記憶の消去などの信号を

出力するものであってもよい。

[0106] 符号１０６は、判定手段を示す。判定手段１０６は、実行手段１０５と同様のＣＰＵとメモリを備えたコンピュータ、ＡＳＩＣによるカスタムＩＣ等で形成され、メール本文およびメール添付ファイル等のメール関連データがウィルスに感染しているか否かを判定する手段である。

[0107] 判定手段１０６は、例えば、既存のウィルスチェックソフトウェア(プログラム)、ウィルスを示すデータ、プログラムとの照合が可能なデータベースを備えていても良い。また、判定手段１０６は、実行手段１０５のコンピュータにおいてマルチタスク的な同時処理、または時系列的に並べた処理であって、実行処理でのメール表示工程の前後でウィルス検査を行っても良い。

[0108] さらに、判定手段１０６は、通常のウィルスを示すデータとの照合を行う場合や、あるいは、ウィルスプログラムが動作する際生じる、実行手段１０５のＩ／Ｏポートへの信号出力、データの移動を監視し、メール表示には関係なく、通常出力がないポートから、ネットワーク接続を目的としたようなデジタル信号を検出し、そのデジタル出力量をカウントするなどして所定値を超えた際に、ウィルスが存在したメール関連データである旨の出力を行うものであってもよい。また、メールの実行動作に関係のないエラーが発生した場合やいわゆるウィルスプログラム等を実行したコンピュータがハングアップした場合警告出力を行うソフトウェアを備えていても良い。この場合は、未知のウィルスの存在を検出可能とする場合がある。

[0109] なお、主に時間によって動作が制御されるウィルスプログラムは、例えば、時間を進ませて、動作を観察し、Ｉ／Ｏポートなどへの出力状態等からウィルスの存在を監視する構成を取り入れてもよい。

[0110] 符号１０７は、削除保管手段を示す。削除保管手段１０７は、ＲＡＭ、ＲＯＭ、その他の記憶チップ、記憶メディア、記憶領域で形成され、ウィルスが感染したデータが一時的に保管される。場合によって削除ボタン操作などにより削除される。削除は、完全な削除が好ましい。

[0111] 符号１０７ａは、保存手段を示す。保存手段１０７ａは、未知のウィルス

が検出された場合、実行不能な状態、例えば、暗号化、圧縮化するなどして保存し、ウィルス阻止プログラム作成の要求が外部からあった時、例えば、制御手段１１２の制御出力に基づいて出力可能な状態が設定され出力する為のものである。

[0112] 保管削除手段１０７は、受信メールの実行プログラムが終了した時点で、完全消去されるものが記録され、保存手段１０７ａとの区別を付けても良い場合もある。

[0113] 符号１０８は、保管手段を示す。保管手段１０８は、ウィルスが検出されなかった場合、一時的に保管されるＲＡＭ、その他の読み書き可能な記憶チップ、記憶メディア、ハードディスク上の特定の記憶領域が例示され、場合によっては、転送ファイルとして、メールに添付されるべく、メール作成手段１０９と接続してもよい。

[0114] 符号１０９は、メール作成手段を示す。メール作成手段１０９は、一般的なメーラーソフトウェア(プログラム)の仕様に乗っ取りメールの作成、添付ファイルの形成、受信の指定、等が行われるものである。

[0115] メール作成手段１０９は、実行手段１０５と接続され、ウィルスが完全に削除された後、実行手段１０５が遮断制御手段１０４を接続状態とした後、送受信手段１０３と接続状態を形成する。メール作成手段１０９は、実行手段１０５と同じ構成を持つ別の構成として構成される他、実行手段１０５においてマルチタスク的にまたは時系列的な順番に従って実行されても良い場合もある。

[0116] 符号１１０は、メール表示手段を示す。メール表示手段１１０は、コンピュータディスプレイなどで形成され、添付ファイルの表示、動作表示などが行われるものである。

[0117] 符号１１１ａは、記憶手段を示す。記憶手段１１１ａは、読み書き可能な記録部である。記憶手段１１１ａとしては、ハードディスク、ＳＤカード、ＵＳＢメモリ、その他のメディアが例示され、本体１００ｂの容量により適宜選択される。保管手段１０８、一時記憶部１０５ｂ、および削除保管手段

１０７は、記憶手段１１１ａで形成されても良いが、必要に応じて、安全性を考慮して、別々の記憶素子、メディアで形成されても良い。

[0118] 記憶手段１１１ａは、遮断制御手段１０４と接続する。これは、ウィルスが、トロイの木馬タイプであって、実行手段１０５の実行に影響を与えるものであって、記憶部に進入し、記憶、書き換え、改ざんされるものの記憶を阻止するためのものである。

[0119] 符号１１１ｂは、第２記憶手段を示す。第２記憶手段１１１ｂは、実行手段１０５で起動するプログラム等を一時的に記録する部分である。第２記憶手段１１１ｂは、記憶手段１１１ａから、遮断制御手段１０４を介して接続しており、遮断制御手段１０４が接続状態の時、制御手段１１２は、プログラム等のデータを記録手段１１１ａから第２記憶手段１１１ｂへ移動コピーする。

[0120] 次に、図２で示す実施形態の動作の説明を行う。

[0121] 本体１００ｂの送受信手段１０３は、ネットワーク１０２と有線または無線で接続されている。遮断制御手段１０４が送受信手段１０３と実行手段１０５の接続を行っている状態で、実行手段１０５は、制御入力部１０５ａから入力される受信命令信号等に基づいてメールサーバ１０１で一時的に記録している電子メールを受信する。

[0122] 受信が完了した後、制御手段１１２は、遮断制御手段１０４の制御入力部１０４ａを介して遮断する信号を出力し、遮断制御手段１０４は、実行手段１０５と送受信手段１０３間のデータ伝送を遮断するとともに、記憶手段１１１ａと、第２記憶手段（一時記憶手段）１１１ｂ間のデータ伝送を遮断する。

[0123] 一時記憶部１０５ｂに一時的に記憶された受信メールは、メール本文、添付ファイルともに実行手段１０５で入力部１０５ａからの入力に基づいてまたは自動設定がされている場合は、自動的に開示実行されるか、または、入力部１０５ａからの使用者の入力信号に基づいて、メール表示手段１１０で表示される。

[0124] メール表示手段１１０で表示された後、一時記憶部１０５ｂの受信メールは適宜消去される。この消去は、使用者による制御入力部１１２ａからの入力または自動消去設定の場合は、自動消去されても良い。なお、この消去は、好ましくは、汎用メーラーの機能にあるような完全消去であることが好ましい場合もある。

[0125] 消去されるまで、制御手段１１２は、遮断制御手段１０４の制御入力部１０４ａに接続を遮断する命令信号を出力し維持する。

[0126] 次に、受信メールに対して、保存、転送、返信を行う場合やウィルスの検出をしたい場合は、判定手段１０６で、このメール本文および添付ファイルが検査され、または、メールまたは添付ファイルが開いたときに発生したコードを検出し、ウィルスが感染しているかどうかを判定する。判定手段１０６は、受信メールをメール表示手段１１０で表示する前、または、同じタイミングでウィルス検査を行っても良い場合もある。

[0127] 感染している場合、感染しているメール関連データが削除保管手段１０７に移動する。この感染があった場合、例えば警報音、警報表示が備え付けのスピーカやメール表示手段１１０から出力されてもよい。

[0128] 制御手段１１２は、遮断制御手段１０４の遮断状態を維持する信号を出力する。

[0129] 使用者は、この感染メール関連データの削除を例えば、端末上のボタン、仮想化されたボタンを操作して制御入力部１１２ａを介して完全消去を実行する。

[0130] 完全消去されるか、ウィルスソフトウェアが実質的に無力化した場合や制御手段１１２によって第２記憶手段１１１ｂの記録データが消去された場合、その両方が行われた場合、制御手段１１２は、遮断制御手段１０４の遮断状態を、制御入力１０４ａを介して制御信号を出力し、遮断状態となっている実行手段１０５と送受信手段１０３との間を接続状態に切り替える動作を行わせる。

[0131] なお、ウィルスがシステムプログラムを破壊する種類の場合や寄生する種

類の場合等、感染の可能性がある実行手段１０５上のシステムプログラムを制御手段１１２で消去した後、制御手段１１２により遮断制御手段１０４を接続状態に切り替えて、記憶手段１１１ａのプログラムデータを実行手段１０５の第２記憶手段１１１ｂへコピーするような状態で移動記録させても良い場合もある。

[0132] ウィルスソフトウェアの実質的無力化とは、例えば、改変、一部消去、暗号化、圧縮等、そのままではプログラムとして実行できない状態であれば良い場合もあり、更に削除保管手段１０７のデータの入出力が遮断または制限が確実にされた状態も含まれ、その他の手法をとっても良い場合もある。

[0133] ウィルスが感染していない場合は、保管手段１０８へ、メール関連データが移動して一時的に蓄積される。

[0134] なお、このような判定手段１０６の判定動作は、メールに対して、転送、返信等、メール関連データを送信する場合に限り動作しても良い場合もある。

[0135] メール作成手段１０９は、使用者が、備え付けのキーボード、または仮想キーボード等を用いて、送信用のメールを作成する時に動作し、保管手段１０８に蓄積された、ウィルスの含まないメールを、添付した状態で、メールを送受信手段１０３を介して送信するものであるが、遮断制御手段１０４が遮断状態では、送信は遮断されておりできない状態であって、作成されたメールは一時的に保存されており、遮断制御手段１０４の遮断状態が解除され、接続状態となった時点で送信されることが好ましい場合もある。

[0136] また、制御手段１１２の制御信号による遮断制御手段１０４における送受信手段１０３と実行手段１０５の遮断接続操作および実行手段１０５と記憶手段１１１ａの遮断接続操作は、実行手段１０５におけるウィルスメールの削除または実質無力化されると同時に行われても良く、また、実行手段１０５においてメール開示操作が行われている途中、記憶手段１１１ａに記憶されたデータが必要になる場合もあることから、記憶手段１１１ａに安全な領域が確保されている場合等は、別々に行われても良い場合もある。

[0137] 判定手段１０６が、受信メールに感染したウィルスメールが未知のウィルスであるとした場合は、保存手段１０７ａに、暗号化、圧縮化して保存処理を行い、ウィルス感染阻止用プログラムの形成のために所望により取り出し可能として保存されてもよい。

[0138] 制御手段１１２は、削除保管手段１０７に保管されたデータが、実行手段１０５の出力信号等、ウィルスプログラムの実行により読み出されないように、制限する出力を行う場合もある。

[0139] それ以外の第２記憶手段１１１ｂ等に記録された記憶データ、プログラムは、制御手段１１２が出力するデジタル制御信号によって、完全に消去されることが好ましい。この場合、制御手段１１２は、遮断制御手段１０４の記憶手段１１１ａと第２記憶手段１１１ｂの接続を行う信号を制御入力部１０４ａに行った後、記憶手段１１１ａに記録されたプログラム等を第２記憶手段１１１ｂに移動しコピーする。

[0140] 以上の動作の例によれば、受信メールを読む限りは、何ら特定の操作もせず、注意も払う必要もなく、メールを読むことを可能とすることができ、しかも、ウィルスの感染は、遮断制御手段で遮断されていることから、実行手段自体の感染もなく安定したメール作業を可能とするものである。

[0141] 〔第４の実施形態〕

次に、図３を参照して本発明の第４の実施形態を説明する。

[0142] 図３で示す実施形態において、符号２０ａは、通常使用される汎用または専用のコンピュータ端末内部に設けられた、本体２０ｂと接続する為のコンピュータ端末の構成を示す。本体２０ｂは、図１及び図２で示した形態を備えた本体に同じである。

[0143] 符号２０１は、メールサーバを示す。メールサーバ２０１は、図１で示したメールサーバ１０１と同じである。また、符号２０２は、ネットワークを示す。ネットワーク２０２は、図１で示したネットワーク１０２と同じである。よって、メールサーバ２０１及びネットワーク２０２のここでの説明を省略する。

[0144] 符号２０３は、送受信手段を示す。送受信手段２０３は、汎用に用いられているメーラーのメール作成、送受信機能を有するものであってもよい。図示の送受信手段２０３は、メールを一時記録する一時記録部２０３ａを備えている。

[0145] 一時記録部２０３ａは、受信メールが一時的に記録され、受信メールが移動手段２０４によって、本体２０ｂの方向へ移動した場合は、消去または、暗号化、圧縮化されて無力化状態となることが好ましい。また、一時記録部２０３ａ内の受信メールは、移動手段２０４で、本体２０ｂへ移動するまで、暗号化、圧縮化などの復元可能に変形していることが、コンピュータ端末２０ａ上で、メールを開く危険性を低下させる点で好ましい場合もある。

[0146] 移動手段２０４は、送受信手段２０３で受信されたメールを、そのまま接続制御手段２０５の方向へ移動送信するものである。移動手段２０４は、受信されたメールを自動的に本体２０ｂの方向へ移動させるか、使用者の操作により移動させる機能を備えていることが好ましい。

[0147] 符号２０ｃは、接続手段を示す。接続手段２０ｃは、ＵＳＢケーブル、ＵＳＢ接続機構等の有線接続、赤外線、可視光線、電波等の無線により形成されている。

[0148] 接続制御手段２０５は、接続手段２０ｃとデータ伝送可能な形式の入出力部を備えている。接続制御手段２０５は、例えば、イーサネット（登録商標）規格端子、赤外線受光部、無線送受信用のフロントエンド回路等である。更に、接続制御手段２０５は、本体２０ｂとコンピュータ端末２０ａとの接続を遮断させたり接続させたりするものであって、ロジック回路、リレー、電子スイッチ等で形成されるが接続手段２０ｃの態様によって適宜選択されるものである。

[0149] なお、接続制御手段２０５は、その目的とする構成に限らず、本体２０ｂから伸びた接続手段２０ｃとコンピュータ端末２０ａが着脱自在にしておくようなプラグとソケットの関係を形成するものであっても良い場合もある。これは、コンピュータ端末２０ａから延びた接続手段２０ｃと本体２０ｂを

引き離せば、一度本体２０ｂに移動した受信メールがウィルスソフトウェアに感染していても、ウィルスソフトウェアがコンピュータ端末２０ａに移動することがないからである。このように着脱式にすることで、簡単にウィルスソフトウェアの感染が阻止できる態様も可能である。

[0150] 符号２０６は、実行手段を示し、使用者からの入力部２０６ａおよび一時記録部２０６ｂと接続する。実行手段２０６の構成は、図１の実施形態で説明したものと同様であるので、ここでの説明を省略する。

[0151] 尚、実行手段２０６は、一つのＯＳ例えば、ＷＩＮＤＯＷＳ（登録商標）系のもののみが使用できるＣＰＵの他、ＡＮＤＯＲＯＩＤ（商標）、ＵＮＩＸ（商標）も使用できるＣＰＵ（例えば　ＩＮＴＥＬ（登録商標）ＡＴＯＭプロセッサー（インテル社製）等）及び周辺機器で形成されても良い。

[0152] この場合は、本実施形態が検出可能なウィルスプログラムの種類を格段に増やすことができる。また複数のＣＰＵを用いてそれぞれ対応するＯＳをインストールして用いても良い。

[0153] 又、ＷＩＮＤＯＷＳ（登録商標）のみ動かすＣＰＵであっても、ＷＩＮＤＯＷＳ（登録商標）上で、ＡＮＤＲＯＩＤ（商標）を動かすプログラムを用いることで、一つのＣＰＵで、複数の異なるＯＳに対応するアプリケーションプログラムを作動させても良い。

[0154] 符号２０７は保管手段を示し、符号２０８はメール表示手段を示し、符号２０９は判定手段を示し、符号２１０は削除保管手段を示し、そして符号２１１は記憶手段を示す。これらの手段は、それぞれ、図１で示す実施形態と同様の構成を有するので、ここでの説明を省略する。

[0155] 記憶手段２１１ａは、接続制御手段２０５を介して実行手段２０６と接続し、保管手段２０７は、接続制御手段２０５を介して接続手段２０ｃと接続し、実行手段２０６からの制御信号によって、それぞれの接続関係が遮断と接続を行うものが好ましい。遮断と接続の関係は、図１の実施形態で説明したように、同時または別々に行われても良い。

[0156] 符号２１１ｂは、第２記憶手段を示す。第２記憶手段２１１ｂは、記憶手

段２１１ａに記録された実行手段２０６が実行するメーラー（プログラム）等、実行手段２０６が実行するプログラムを一時的に記録するためのＲＡＭ等のメモリで形成されている。

[0157] 符号２１２は、制御手段を示す。制御手段２１２は、ゲートアレイ、ロジックＩＣ等の組み合わせからなり、接続制御手段２０５、第２記憶手段２１１ｂ、実行手段２０６、判定手段２０９、削除保管手段２１０、その他の構成と電気的に接続しても良い。制御手段２１２は、上記したそれぞれの手段の動作の開始、停止を行う信号を出力したり、第２記録手段２１１ｂやその他、保管手段２０７以外の手段で、データを記録、または一時的に記録したデータを消去する為の信号を出力したりする場合がある。

[0158] 更に、制御手段２１２は、リセット後、記録手段２１１ａのプログラムデータを、第２記録手段２１１ｂへ移動記録する動作を行う。

[0159] なお、制御手段２１２は、コンピュータ端末２０ａ側の一時記録部２０３ａ、移動手段２０４と制御可能に接続し、一時記録部２０３ａ内の受信メールの外部への読み出しを停止する等の制御をする信号を出力したり、移動手段２０４のデータの移動を開始または停止の信号を出力する場合もある。

[0160] 次に、図３で示す実施形態の動作の説明を行う。

[0161] コンピュータ端末２０ａには、送受信手段２０３および移動手段２０４がプログラムの形式として予めインストールされているかまたは、予めプログラムが記録されたメディアを挿入したり、これらの手段を電気回路として形成したものを装着したＰＣＩ仕様のボードやＵＳＢ接続型回路等として形成し、コンピュータに装着して使用されてもよい。なお、メール作成手段は、コンピュータ側に内蔵されている状態であり、図３では省略している。

[0162] 本体２０ｂをコンピュータ端末２０ａに装着する。ＵＳＢ接続の場合は、その挿入により装着され、無線の場合は、送受信可能な距離に据え付けられ、有線または無線による接続手段２０ｃが形成される。

[0163] メールサーバ２０１に記録された受信メールは、コンピュータ端末２０ａ上の使用者の操作に基づく求めに応じ、ネットワーク２０２を介してコンピ

ュータ端末２０ａの送受信手段２０３に入力され、一時記録部２０３ａに記録される。

[0164] この場合、一時記録部２０３ａ内に記録された受信メールは、制御手段２１２の制御信号、コンピュータ端末２０ａの設定等によって、コンピュータ上では、開くことができない状態になっていることが好ましい。受信メールは、使用者から制御入力部２１２ａを介して入力される制御信号に基づいて、または、自動的に出力される制御手段２１２からの制御信号により、移動手段２０４及び接続手段２０ｃを介して接続制御手段２０５に出力される。実行手段２０６は、接続制御手段２０５の制御入力部２０６ｃに接続状態を示す信号を出力し、受信メールを一時記録部２０６ｂへ記録させる。

[0165] 制御手段２１１は、接続制御手段２０５の制御入力部２０６ｃに遮断状態を示す信号を出力して遮断状態を形成させる。場合によっては、本体２０ｂをコンピュータ端末２０ａから引き離す動作を行うことで事実上の遮断状態を形成する。

[0166] このとき、一時記録部２０３ａに記憶された受信メールは、完全に削除かまたは改変、暗号化、または、解凍にはパスワードがかけられ容易に解凍不可能な状態で圧縮されて無能力化されることが好ましい場合もある。尚、本体２０ｂとコンピュータ端末２０ａを引き離した場合、制御手段２１２と一時記録部２０３ａ、移動手段２０４間の電気的接続も遮断される為、この場合は、制御手段２１２と一時記録部２０３ａは接続した状態を維持していることが好ましい場合もある。

[0167] この分離した状態で、実行手段２０６は、受信メールを開き、メール表示手段２０８に表示させる。この時点で、ウィルスがネットワークを介して外部へ情報を流出することが不可能な状態となることから、このようなウィルスを目的とした本体を形成する場合は、判定手段等は不要な場合もある。なお、その場合でも、制御手段２１２を設けておき、異なる受信メール関連データを開くようなプログラムを実行する度ごとに、プログラムを、記憶手段２１１ａから読み込むことで、前のプログラムを実質消去した状態として、

あらたなプログラムで、受信メール関連データを開くような実行動作を行っても良い場合もある。

[0168] 実行手段２０６でメールが開かれる場合は、記憶手段２１１ａと実行手段２０６との接続を制御手段２１２からの制御信号により、接続制御手段２０５が遮断する。このような遮断は、読み書き可能な記憶手段２１１ａに実行手段等を構成するプログラムであって、システム全体を制御するプログラムを含む場合、ウィルスプログラムが記憶手段２１１ａへ侵入できない点で好ましい場合もある。

[0169] 受信メールは、判定手段２０９において、実行手段２０６でメーラーが起動する前後または同時のタイミングで図２の実施形態で示したようなウィルス検査が行われる。

[0170] 受信メールがウィルスプログラムに感染している場合、制御手段２１２は、接続制御手段２０５における記憶手段２１１ａと実行手段２０６との接続、接続手段２０ｃと実行手段２０６との接続を遮断した状態としながら、削除保管手段２１０に、受信メールを移動させ、完全削除、または無力化する処置が施される。

[0171] 削除保管手段２１０で、受信メールが完全削除され、または無力化されると、実行手段２０６は、接続制御手段２０５の遮断状態を接続状態に切り替えてもよい場合もあるが、ウィルスプログラムがシステム領域に侵入してシステムを破壊する場合等が生じる場合は、制御手段２１２により、一時記録部２０６ｂおよびバッファメモリ等のすべての記録データを消去して、接続制御手段２０５を遮断状態から接続状態へ切り替えても良い。

[0172] この場合、制御手段２１２は、記憶手段２１１ａのプログラムデータを第２記憶手段２１１ｂへ移動コピーして、実行手段２０６がプログラムを実行可能な状態にすることが好ましい。

[0173] 判定手段２０９で、受信メールにウィルスが感染していないと判定された場合は、保管手段２０７に受信メールが移動保管され、接続制御手段２０５は、接続手段２０ｃと実行手段２０６との接続状態および記憶手段２１１ａ

と実行手段２０６の遮断状態を接続状態へ変更する。

[0174] 保管手段２０７に保管されたウィルスに感染していない受信メールのメール本文および添付ファイルは、制御手段２１２からの制御信号により、コンピュータ端末２０ａ内の送受信手段２０３で作成されるメールに添付、貼り付け等を可能となる状態を形成可能とする。

[0175] 本実施形態では、本体２０ｂのメール送受信手段等を省くことができるので、より簡素な本体を形成可能である。

[0176] なお、図１の実施形態と同様、メール関連データを表示する機能のみの場合は、制御手段２１２を残し、判定手段２０９、削除保管手段２１０、保管手段２０７は不要となる場合もある。

[0177] この場合、本体２０ｂは、受信メールの本文、添付ファイル等の受信メール関連データをメール表示手段２０８で表示し、使用者がウィルスプログラムによる感染の有無を調べ、ウィルス感染の無い場合は、コンピュータ端末２０ａが受信メールをメールサーバ２０１から再度受信できるようにしたり、ウィルス感染がある受信メールと思えるメールが、メール表示手段２０８で表示された場合は、メールサーバ２０１に一時的に記録された当該メールを削除する機能が、制御手段２１２またはコンピュータ端末２０ａから行われる様に設定されることが好ましい場合もある。この実施形態によれば、返信、転送メールの作成等の構成をコンピュータ端末２０ａに備えた分より簡素な構成を取ることができる。

[0178] 〔第５の実施形態〕

次に、図４を参照して本発明の第５の実施形態を説明する。なお、図４では、通常使用されるコンピュータ端末３０ａに接続して、より付属性の高い本体３０ｂを使用した形態を示す。

[0179] 図４の実施形態において、符号３０１はメールサーバであり、３０２はネットワークであり、いずれも図１～図３を参照して先に説明したものと同じ構成を有する。

[0180] 符号３０ａは、コンピュータ端末を示す。コンピュータ端末３０ａとして

は、例えば、キーボード、モニター、マウスを備えたデスクトップ型、ノート型のコンピュータ、携帯電話、スマートフォン等の形状を有するものが例示される。コンピュータ端末３０aには、予めメール作成、受信などを行うメーラー(プログラム)がインストールされている。

[0181] 符号３０ｄは、一時記録部を示す。一時記録部３０ｄは、受信メールを一時的に保存する記録部であり、ハードディスク、ＵＳＢメモリ、その他の記録部で構成されている。

[0182] 符号３０ｅは、入力部を示す。入力部３０ｅは、使用者が、コンピュータ端末に装着されたキーボード、仮想キーボード、マウス、タッチパッドを利用して信号を入力する入力部である。

[0183] 接続手段３０ｃは、図３を参照して先に説明したものと同様、無線、有線による接続状態を形成するものである。

[0184] 符号３０３は、接続制御手段を示す。接続制御手段３０３は、記憶手段３０８ａと実行手段３０４間の接続および接続手段３０ｃと接続制御手段３０３間の接続、遮断等を実行手段３０４の制御信号に基づいて行う。

[0185] 更に、接続制御手段３０３は、一時記憶部３０ｄに記録された受信メールを実行手段３０４の制御信号に基づいて消去したり、コンピュータ端末３０ａ側で、表示実行可能とする信号を出力する。

[0186] 実行手段３０４は、キーボード、タッチパッド等の使用者とのインタフェースを形成する制御入力部３０４ｃを備えており、図１及び図２で示した実施形態と同様の構成を持つものである。

[0187] 更に、実行手段３０４は、接続制御手段３０３を介して一時記録部３０ｄの受信メールを削除する操作や、コンピュータ端末３０ａ側で読み取り可能とする操作を行う。

[0188] また、実行手段３０４は、コンピュータ端末３０ａの表示モニターと接続し、受信メールが実行手段３０４上で実行された場合、コンピュータ端末３０ａのモニターに実行状態が表示されるように構成されている。

[0189] 実行手段３０４の出力をコンピュータ端末３０ａに表示する機能は、コン

ピュータ端末３０ａのモニターを利用して実行手段３０４で出力した受信メールの表示を行うだけであり、ウィルスプログラムの影響がない範囲で、画像表示用バッファメモリを共有する場合もある。

[0190] 符号３０４ａは、受信メールを一時的に記録する一時記録部を示す。一時記録部３０４ａは、ウィルス検査が終了した場合、メールの表示が終了した場合まで記録され、ウィルス感染がはっきりした場合は、完全に削除されることが好ましい。

[0191] 符号３０４ｂは、制御入力部を示す。制御入力部３０４ｂは、接続制御手段３０３の一時記憶部３０ｄと実行手段３０４の間、記憶手段３０８ａと第２記憶手段３０８ｂとの間の電気的接続等の遮断、接続を行うための信号を入力する部分である。

[0192] 符号３０５は保管手段、３０６は判定手段、３０７は削除保管手段、そして３０８ａは記憶手段であり、それぞれ、図１及び図３を参照して先に説明した実施形態と同様の構成動作を行うものである。なお、メール参照のみの場合、保管手段３０５等は、省略しても良い場合もある。

[0193] 符号３１２は、制御手段を示す。制御手段３１２は、ゲートアレイ、ロジックＩＣ、書き換えが制限されたコンピュータで構成され、記憶手段３０８ａ、判定手段３０６、削除保管手段３０７、実行手段３０４、一時記録部３０４ａ、第２記憶手段３０８ｂに接続して、各構成の動作の開始、停止、その他の動作を制御する。なお、制御手段３１２は、コンピュータ端末側に接続した一時記憶部３０ｄと端子３１２ｂを介して接続してもよい。

[0194] 制御手段３１２は、判定手段３０６でウィルスメールが検出された場合に、その旨の信号を入力し、第２記憶手段３０８ｂの記憶データ、その他関連する記憶素子のデータを消去するリセットする信号を出力する。また制御手段３１２は、接続制御手段３０３の制御入力部３０４ｂと接続しており、記憶手段３０８ａと第２記憶手段３０８ｂ間の遮断した状態から接続した状態へ切り替える為の信号を出力したり、記憶手段３０８ａの記録プログラム、その他の記録データを第２記憶手段３０８ｂへ移動コピーする機能を備えて

いる。

[0195] 制御手段３１２は、制御入力部３１２ａを備えており、使用者からのキーボード、タッチパッド、その他のマンマシンインタフェースを介した制御入力に基づいて制御信号の出力、制御機能を行ったり、あらかじめ設定された回路、プログラムに基づいて自動的な動作を行っても良い。

[0196] 符号３０８ａは記憶手段を示し、図３で示す記憶手段２１１ａと同様のデータを記憶する。また、符号３０８ｂは第２記憶手段であり、図３で示す第２記憶手段２１１ｂと同様のデータを記憶する。

[0197] 次に、図４で示す実施形態の動作の説明を行う。

[0198] メールサーバ３０１に記録された受信メールは、使用者の入力部３０ｅからの受信要請信号の入力または自動でネットワーク３０２を介してコンピュータ端末３０ａの一時記憶部３０ｄへ記録される。

[0199] コンピュータ端末３０ａ上では、例えば使用者のマウスポインタをメーラープログラム起動用アイコン、またはウィルスチェックアイコンに移動させ、ダブルクリック等の操作によりプログラムを起動させる。この起動により、コンピュータ３０ａのモニター上にウィルスチェック動作が開始するメッセージ（図示せず）が表示されてもよい。

[0200] 制御手段３１２から、接続する旨の制御信号が接続制御手段３０３の制御入力部３０４ｂに入力されると、接続制御手段３０３は、一時記憶部３０ｄおよび記憶手段３０８ａと実行手段３０４間のデータ伝送を含む接続動作を行う。

[0201] 実行手段３０４は、接続制御手段３０３を介して一時記憶部３０ｄに記録された受信メールを入力して一時記録部３０４ａに一時的に記録する。

[0202] 制御手段３１２から、遮断する旨の制御信号が接続制御手段３０３の制御入力部３０４ｂに入力されると、接続制御手段３０３は、一時記憶部３０ｄおよび記憶手段３０８ａと実行手段３０４間のデータ伝送を含む接続の遮断を行う。

[0203] 遮断状態で、一時記憶部３０ｄに記録された受信メールを実行して、コン

ピュータ端末３０ａのモニターへ表示出力する。

[0204] 実行手段３０４は、一時記録部３０４ａに記録した受信メールをコンピュータ端末３０ａのモニター上、または、その他の外部表示手段に表示する。

[0205] 判定手段３０６は、受信メールのウィルス検査を行い、ウィルスに感染していない場合は、保管手段３０５へ受信メールを移動させるか、接続制御手段３０３および制御手段３１２へ、接続手段３０ｃを介して一時記憶部３０ｄに記録された受信メールの開封禁止を解除する信号を出力する。

[0206] 制御手段３１２は、接続制御手段３０３の制御入力部３０４ｂへ、接続状態を示す信号を出力して、実行手段３０４と一時記憶部３０ｄを接続させる。

[0207] 判定手段３０６は、受信メールがウィルスに感染している場合は、これを削除保管手段３０７へ移動させる。移動させる際、完全削除または暗号化、圧縮化、改変して無効化する。

[0208] 更に、実行手段３０４は、接続制御手段３０３、接続手段３０ｃを介して一時記憶部３０ｄの受信メールがウィルスに感染していることをモニターなどに警告表示しても良い。

[0209] 制御手段３１２は、一時記憶部３０ｄの受信メールの完全削除、または無効化処理を行う。

[0210] 更に、判定手段３０６のウィルス感染を示す出力信号に基づいて、制御手段３１２は、第２記憶手段３０８ｂの記憶データを消去する信号を出力して、記憶データを消去し、更に接続制御手段３０３の制御入力部３０４ｂへ記憶手段３０８ａと第２記憶手段３０８ｂの遮断していた接続を再開する信号を出力して、記憶手段３０８ａの記憶するプログラムを第２記憶手段３０８ｂへ移動させて、実行手段３０４において、次の受信メールの実行が可能な状態にする。

[0211] 制御手段３１２は、一時記憶部３０ｄにウィルスが感染した受信メールの削除する信号を出力したり、ウィルスが感染した受信メールを特定するデータをコンピュータに警告的な情報として出力する場合もある。

[0212] 図４で示す実施形態は、本体３０ｂをより簡素にしながら、ウィルスの感染と削除処理を容易に行わせることを可能とする。

〔第６の実施形態〕

次に、図５を参照して本発明の第６の実施形態を説明する。

[0213] 図５の実施形態において、符号４０１は、メールサーバを示す。メールサーバ４０１としては、例えば、受信メールを一時的に記録し、端末からの要請に応じて端末へ送信したり、削除したりできる仕様を備えたものが例示される。メールサーバは、例えば実行手段４０７の命令により、メールの削除を可能とする。

[0214] 符号４０２は、入出力手段を示す。入出力手段４０２は、有線または無線で、インターネットルータ、モデム等と接続する手段である。入出力手段４０２としては、例えば、イーサネット（登録商標）接続、ＵＳＢ接続、アンテナ、変調・復調を司るフロントエンド回路、等が例示される。この手段は、少なくとも、メールサーバとの接続が可能なものであれば良い。その他に、入出力手段４０２は、必要に応じて、イントラネット、エクストラネット、公衆回線、携帯電話回線との接続が行われる構成であっても良い。

[0215] 符号４０３は、接続制御手段を示す。接続制御手段４０３は、２入力以上の入力端を備えたＮＡＮＤ、ＮＯＲ等を含むロジックＩＣ、リレー、スイッチングデバイス、スイッチング素子のアレイ等、外部入力信号により、電気的接続を切断したり、接続を行う部分である。

[0216] 接続制御手段４０３の電気的接続の遮断接続動作は、入出力手段４０２と実行手段４０７の接続、入出力手段４０２と第２記憶部４０６との接続、入出力手段４０２と制御手段４０９との接続、入出力手段４０２と判定手段４１０との接続をはじめ、記憶手段４０４と実行手段４０７との接続、記憶手段４０４と第２記憶部４０６との接続、登録手段４０５と実行手段４０７の接続、登録手段４０５と第２記憶部４０６との接続についても遮断接続を行う場合がある。なお、これらすべての接続の遮断接続動作を行うだけでなく、一部の遮断接続であっても良い場合もある。

[0217] 接続制御手段４０３の遮断接続動作は、例えば受信メールを受信完了の時点で遮断する動作が示される。第２記憶部４０６に記憶されたメールがすべて処理され、消去された時点で接続が開始されたり、制御手段４０９の動作により各記憶部のメールに関する記憶が、削除保管手段４１１以外消去された時点で接続が開始されても良い。また、例えば、一時記録部４０８に受信メールが記録された時点で、遮断してもよい。この遮断は、例えばソフトウェアによる場合は、あらかじめＲＯＭに記憶されたソフトウェアにより行われてもよい。

[0218] 符号４０４は、記憶手段を示す。記憶手段４０４は、ＲＡＭ、ＳＤメモリ、ＵＳＢメモリなどで構成される。記憶手段４０４は、メールを実行させたり、添付ファイルを開く動作をするメーラー（メール用プログラム）が記録されているとともに、ウィルス検出の為の判定用プログラム、等が記憶されている。記憶手段４０４は、メーラー（メール用プログラム）、判定用プログラムのバージョンアップを可能とさせる場合、外部との接続部を持つ場合もある。この接続部は、例えば、ＳＤメディア、ＵＳＢメモリ等のバージョンアップしたプログラムが記録されており、必要に応じて、プログラムごと入れ替える仕様や、ＵＳＢ接続、赤外線接続等を介して外部コンピュータからプログラムを入手する仕様であっても良い。

[0219] 符号４０５は、登録手段を示す。登録手段４０５には、メールアドレス、パスワード、アカウント、ＰＯＰアカウント、ＳＭＴＰアカウント等が登録されている。この登録も記憶手段４０４と同様、外部から入力可能とするが一度、登録手段４０５に登録された状態で、内部の実行手段４０７などに書き換え不可能に設定されていることが好ましい。

[0220] 符号４０７は、実行手段を示し、通常のコンピュータと同様のメーラーを起動させる程度の様式をもつコンピュータ仕様が好ましい。

[0221] 実行手段４０７は、ＲＡＭ、ＲＯＭおよびＣＰＵを備えたコンピュータ様式が好ましいが、ゲートアレイによる手段であってもよい。実行手段４０７は、マイクロソフト社のＯＵＴＬＯＯＫ（登録商標）、ＯＵＴＬＯＯＫ　Ｅ

ＸＰＲＥＳＳ（登録商標）等、一般に使用されているメーラーソフトウェアを実行し、メールの送受信、サーバのメール削除、メールの表示等、汎用ソフトウェアの動作が行える環境を備えていることが好ましい。また、実行手段４０７は、ウィルスメールが実行可能な状況が好ましいが、必要に応じて、少なくともメールを上述したように実行可能であれば、ＲＯＭ（リードオンリーメモリー）にプログラムを記録させたり、ゲートアレイ等ハードウェアＩＣ等によって形成されても良い。

[0222] また、実行手段４０７は、判定手段４１０のウィルス感染メールが存在していると判定した場合は、メールサーバ４０１へ、メールの削除を行う信号を出力可能としてもよい。

[0223] また、実行手段４０７は、接続制御手段４０３の接続、遮断の制御を行う信号を出力する。

[0224] 符号４０６は、第２記憶部を示す。第２記憶部４０６としては、記憶手段４０４を実行手段４０７で実行させるべく一時的に記憶する、例えばＲＡＭ（ランダムアクセスメモリ）仕様のチップを例示することができる。

[0225] 符号４０８は、一時記録部を示す。一時記録部４０８は、入力された受信メールを一時的に記録するための記録部である。

[0226] 符号４０９は、制御手段を示す。制御手段４０９は、入出力手段４０２、記憶手段４０４、登録手段４０５、実行手段４０７、第２記憶部４０６、判定手段４１０と接続し、各構成の開始、停止、その他の制御を行う為の信号を出力する。制御手段４０９は、接続制御手段４０３の制御入力部４０３ａと接続し、接続制御手段４０３に接続されている各構成間を接続遮断させるための信号を出力する。また、接続制御手段４０３は、実行手段４０７、判定手段４１０の周辺の各セクションで記録されているデータを電気的に消去するための信号を出力する。制御手段４０９は、他の実施形態と同様、書き換え不可能に制御される記憶素子とＣＰＵの組み合わせや、ＡＳＩＣ、ロジックＩＣの組み合わせによって構成される。制御手段４０９は、一時記録部４０８等の記録または記憶内容を消去した後、接続制御手段４０３の制御入

力部４０３ａに接続状態を形成するための信号を出力する場合がある。

[0227] 制御手段４０９の制御入力部４０９ａは、使用者とのマンマシンインターフェースと接続する。しかし、本実施形態は、メールを表示することなく、ウィルス感染受信メールを検出し、メールサーバ４０１の受信メールを削除する動作を行う範囲でのインタフェース、例えば複数のボタンと、表示用ＬＥＤで足りる場合もある。また、実行手段４０７の制御入力部４０７ａも、同様のインターフェースで足りる場合もある。

[0228] 符号４１０は、判定手段を示す。判定手段４１０は、受信メールの本文や受信メールの添付ファイルを検査したり、開いて、その動作の異常な状態をチェックし、ウィルスが感染していると判断した受信メールを、削除保管手段４１１へ無力化を図った状態で移動し、場合によっては、削除を外部入力で行うものである。判定手段４１０がプログラムによって実行される場合は、実行手段４０７が代役を務めてもよい場合もある。

[0229] また、判定手段４１０は、ウィルス関連の定義ファイルを更新可能に記憶する場合もあるが、実行手段のＩ／Ｏ出力端の信号の状態を検出して、例えば、メール受信、添付ファイル開示動作に関係が無く、ネットワーク４０ｅ方向へデータを出力するかどうかを監視し、データの出力があった場合、ウィルス感染があった受信メールと特定する手段を更に備えることが好ましい場合もある。

[0230] 符号４１１は、削除保管手段を示す。削除保管手段４１１は、ウィルスに感染したメールを暗号化、圧縮化するなどして無力化して保存し、または削除する手段である。この手段は、外部入力により、外部へ移動して、復号化して表示するものであって良い。この動作は、少なくとも、実行手段４０７などに影響を与えることなく、制御手段４０９の制御信号に基づいた外部装置との接続手段との接続により、局所的な操作により行われる場合や、別途解読手段を備えた端末を用いて表示させても良い。これは、例えば、判定手段４１０が未知のウィルスプログラムデータを検出して、削除保管手段４１１へ、これを移動させた場合であって、これがウィルスプログラムであるか

確認する必要がある場合に生じる。

[0231] 符号４０ａは、コンピュータ端末を示す。コンピュータ端末４０ａは、通常の使用に足りるソフトウェアがインストールされており、通常の業務に使用できる状態で形成されていればよい。コンピュータ端末４０ａは、少なくとも、メーラープログラムが動作する状態であって、メールアドレス、アカウント、パスワード等は、本体４０ｄと同一のものが設定登録されていることが好ましい。

[0232] 符号４０ｂは、ネットワーク４０ｅとの接続手段を示す。接続手段４０ｅは、例えば、イーサネット（登録商標）、ＷＡＮ、ＬＡＮ等、無線あるいは有線での接続を行うための手段である。符号４０ｃも同様の接続手段であり、例えば、無線、有線手段によりネットワーク４０ｅと入出力手段４０２を接続する為の接続手段である。

[0233] 接続手段４０ｂ及び４０ｃは、ネットワーク４０ｅといずれも例えばルーター、モデム等を介して接続するものである。なお、これらの接続手段は、例えば携帯電話等では、アンテナおよび所望の周波数帯で、変調、復調、増幅を行うためのフロントエンド回路等を介して接続している。

[0234] 符号４０ｄは、本体を示す。本体４０ｄは、例えば、ネットワーク４０eとの接続状況を示すＬＥＤ、操作用スイッチ、ウィルス検出用インジケータ、動作オンオフスイッチ、ウィルス削除スイッチ等があれば足りる。なお、本体４０ｄは、必要に応じて、図１等に示した実施形態のように、液晶モニターを接続したものであっても良い。

[0235] 符号４０ｅは、ネットワークを示す。ネットワーク４０ｅは、インターネット、エクストラネット、社内専用回線、携帯電話回線、公衆電話回線等、メール送受信接続状態によって適宜選択されればよく、使用者の接続状況に対応したネットワークであれば良い。

[0236] 次に、図５で示す実施形態の動作の説明を行う。

[0237] 本体４０ｄには、使用者のメールアドレス、パスワード等をあらかじめ登録手段４０５に記録しておく。登録される使用者は、単数でもよく、複数で

あってもよい。

[0238] 登録手段４０５へのデータの記録は、例えば、制御手段４０９の制御入力部４０９ａを介して使用者が入力したもの、実行手段４０７の制御入力部４０７ａを介して入力したもの、または、登録手段４０５自体が、着脱自在なメモリユニットで形成されたものが例示される。

[0239] 本体４０ｄは、ネットワーク４０ｅと有線または無線よりなる接続手段４０ｃを介して接続した状態である。本体４０ｄは、コンピュータ端末４０ａと接続していない状態が好ましい場合もあるが、その他の目的に応じて付随的に接続する場合があってもよい。

[0240] この状態で、本体４０ｄの接続スイッチがオンの状態となっており、制御手段４０９が各構成に対し動作を開始させる信号を出力する。

[0241] また、記憶手段４０４に記憶された実行手段４０７で実行するプログラムを、第２記憶部４０６へ記憶させて、実行手段４０７がこのプログラムを実行可能な状態とする。

[0242] 接続制御手段４０３は、接続状態となっており、受信メールがメールサーバ４０１に受信記録されていると、入出力手段４０２、接続制御手段４０３を介して一時記録部４０８へ受信メールを取り込み記憶する。

[0243] メールサーバ４０１内の受信メールは、そのまま記録された状態としてもよいし、受信ごとに削除されても良い。なお、本実施形態では、メールサーバ４０１内に受信メールがそのまま記録された状態のもので説明する。

[0244] 受信メールの１乃至複数個を一時記録部４０８に記憶した状態となった時点で、接続制御手段４０３は、入出力手段４０２と実行手段４０７やその他、記憶手段４０４と実行手段４０７との接続を遮断する。遮断命令は、制御入力部４０３ａを介して実行手段４０７が信号を出力して行う。あるいは、必要に応じて、一時記録部４０８の記録内容を監視して、遮断信号を出力する制御信号出力部を設けて、この手段によって遮断命令を行っても良い。

[0245] 実行手段４０７は、第２記憶部４０６に記憶されたプログラムにもとづいて動作し、一時記録部４０８に記録された受信メールを開く動作、表示する

動作を行う。併せて、判定手段４１０で一時記録部４０８に記録された受信メールのウィルスプログラムが含まれているか、検査される。判定手段４１０は、既成のウィルスプログラムパターンと一致するか否かを検査してもよいが、実行手段４０７で受信メールの関連データが開いた時点での、実行手段４０７の動作を監視し、例えば、ネットワークへの信号を出力する入出力ポートから、メーラープログラムが動作している場合は、出力が生じることが無い一乃至複数のＩ／Ｏポートにロジック ＩＣ等で構成されるカウンタを接続し、カウンタの出力部に出力パルスを積分する積分回路を接続し、更にこの積分値を一端に入力し、他端で閾値電圧を設定したコンパレータを接続する構成を用いる。かかる構成として、実行手段４０７がメールの開示動作の際、そのカウンタの出力値を積分しコンパレータで設定した所定の閾値以上となったとき、ウィルス検出パルスがコンパレータから出力され、ウィルスプログラムであると判定して、制御手段４０９へ信号を出力する構成が例示される。

[0246] 判定手段４１０で、ウィルスが含まれたプログラムが検出された場合、これを削除保管手段４１１へ、暗号化または圧縮化する等して記録されることが好ましい。なお、メールの件名、日付など、ウィルスとは関係ない情報と対応して保存することが好ましい場合もある。

[0247] 判定手段４１０でウィルスが含まれているプログラムが検出され、削除保管手段４１１へ、そのウィルスメールが無力化して記録された時点で、制御手段４０９は、使用者へウィルス感染データありとの、例えばＬＥＤ表示を行うことが好ましい場合もある。

[0248] 更に、接続制御手段４０３が遮断状態を形成したまま制御手段４０９は、削除保管手段４１１以外の記憶を消去する。

[0249] 消去が完成した状態で、接続制御手段４０３の遮断状態を解除し、接続状態を形成する。この接続状態となった時点で、記憶手段４０４で記憶されたプログラム、登録手段４０５で記録されたアカウントデータが接続制御手段４０３を介して、第２記憶部４０６等へ移動コピーされ、実行手段４０７，

判定手段４１０等はメーラー（プログラム）の実行可能な状態を再度形成し、接続制御手段４０３が接続状態のまま次の受信メールをメールサーバ４０１から受信する状態を形成する。

[0250] 制御手段４０９の制御信号により接続制御手段４０３が接続状態を形成した状態において、削除保管手段４１１に無力化して保管されたウィルスプログラム付き受信メールのメール情報は、本体４０ｄの表示部（図示せず）に表示されてもよいが、このメール情報（メールの表題）にもとづいて、メールサーバ４０１内のウィルスメールを削除する操作を行ってもよい。

[0251] メールサーバ４０１内は、ウィルスプログラムが含まれるメールが削除された状態となっており、使用者は、コンピュータ端末４０ａで安心してメール受信開示操作が可能となる。なお、判定手段４１０の判定によっては、誤判定による非感染メールが削除保管手段４１１に記録される場合もあることから、また感染メールから、ウィルス阻止用のファイルを作成する場合、使用者は、ここに削除保管された受信メールを復号、再生して閲覧する手段を備えても良い場合もある。これは、異なる独立した端末によって、確認されることが好ましい場合もある。

[0252] 本実施形態は、受信メールの実行開示操作を行う際、外部との電気的接続を遮断することで、ウィルスメールの目的とする動作を遮断するとともに、メールサーバ上のメールを削除する操作を自動的に行うことで、使用者は、ウィルス感染を気にすることなく、メール開示作業をおこなうことを可能とする。このような操作は、コンピュータ端末４０ａと無関係に行うことを可能とすることから、常時本体４０ｄを接続しておけば良く、使用者の負担はより低減され、また、登録手段４０５に記録される使用者のメールアカウントを複数にすることで、複数のコンピュータ端末に対し、一つの本体で足りる場合もある。

[0253] 〔第７の実施形態〕

次に、図７を参照して本発明の第７の実施形態を説明する。

[0254] 図７の実施形態において、符号７０１は、中央処理手段を示し、ＣＰＵ、

ＭＰＵ、ＩＯバッファ等の組み合わせ構成よりなる。中央処理手段７０１は、一時記憶手段７０３に記憶されたＯＳ、メーラープログラム、ブラウザソフトウェア、ビューアープログラムに基づいて、ダウンロードしたメール本文の表示処理、添付ファイルの表示処理、ダウンロードしたプログラムの実行処理を行う部分である。

[0255] また、中央処理手段７０１は、ネットワークとの接続の為のプロトコルに基づいたパケット信号を出力する。

[0256] 符号７０２は、第１記憶部を示す。第１記憶部７０２は、例えば、図示されるように、記憶手段７０２１と、第１遮断接続手段７０２２の組み合わせからなり、制御手段７１１からの制御信号により、主に書き込み側の接続における接続と遮断を行う構成を採用している。

[0257] 記憶手段７０２１は、ハードディスク、フラッシュメモリ等、書き込み可能な記憶手段であり、ＯＳ、アプリケーションプログラム、メーラー、ビューアープログラム、ＨＴＭＬプログラム、等が記憶されている。

[0258] 第１記憶部７０２は、上述のように書き込みが制限された記憶装置を示したが、メーラー、ブラウザ専用機器の場合は、ＲＯＭ（Read Only Memory）の他、書き込み禁止したＵＳＢメモリ、ＳＤカード等のメディアなどに置き換えても良く、メール処理が主となる端末の場合は、ＲＯＭで十分な場合もある。

[0259] 第１遮断接続手段７０２２は、例えば図６Ｂで示すように、論理回路の組み合わせ構成をとる。図６Ｂは、ＡＮＤ回路列７０２ａで形成され、それぞれの一端が制御入力部ｂ２２３を形成する。更に、ＮＯＲ回路列７０２ｂのそれぞれの一端が制御入力部ｂ２２３と接続し、他端は、ＡＮＤ回路列７０２ａの入力部の他端ｂ２２１と接続する。

[0260] 制御入力部ｂ２２３には、デジタル信号「１」、「０」のいずれかが入力される。例えば、信号「１」を出力する場合は、入力部の他端ｂ２２１に入力されるデジタル信号は、そのまま、出力端ｂ２２２に出力され、接続状態を形成し、信号「０」が、制御入力部ｂ２２３へ入力されると、出力端ｂ２

２２の出力は、入力部の他端ｂ２２１の入力が「１」「０」と変化しても、常に「０」となり、伝送が遮断状態を形成する。

[0261] 他方、ＮＯＲ回路列７０２ｂは、制御入力部ｂ２２３からデジタル信号「１」が入力すると、他の入力端が「１」「０」のいずれでも、「０」となり、遮断状態を形成する。

[0262] 制御入力部ｂ２２３の入力が「０」となると、入力部の他端ｂ２２１と出力端ｂ２２２は、位相が９０度変化するが、接続状態を形成する。

[0263] 図６Ｂで示すＡＮＤ回路列の入力部の他端ｂ２２１は、中央処理手段７０１と接続し、出力端ｂ２２２は、記憶手段７０２１の入力端に接続する。

[0264] 記憶手段７０２１は、ハードディスク等の読み書き可能な記憶手段であるため、ウィルスプログラムの侵入を防ぐために第１遮断接続手段７０２２が設けられている。よって、データバスの数だけＡＮＤ回路７０２ａ及びＮＯＲ回路７０２ｂが設けられている。ＮＯＲ回路の出力端ｂ２２４は、検査手段７０９に接続している。

[0265] 記憶手段７０２１へデータを直接書き込む信号が検査手段７０９に接続している。よって、ＲＡＭ起動にもかかわらず、通常書き込まないタイミングでデータ信号が出力する場合、検査手段７０９は、このデータ信号に対応した点滅を行って、ウィルスプログラムの発生を予測可能とする。第１遮断接続手段７０２２は、ＡＮＤ回路とＮＯＲ回路の組み合わせを示したが、その他の論理回路を組み合わせて用いても良い。

[0266] 図６Ａにおいて、符号７０７は、第２遮断接続手段を示す。第２遮断接続手段７０７は、複数の２入力のＡＮＤ回路７０７ａ、７０７ｂ及び複数のＮＯＲ回路７０７ｃのアレイであるので、入出力端を示す記号は、図７で示すものと同一とした。ＡＮＤ回路及びＮＯＲ回路は、それぞれ、一つに７０７ａ、７０７ｂ及び７０７ｃの符号を示している。

[0267] 符号ｂ７０は、すべての入力端の一つと接続する制御信号入力部であり、制御手段７１１の制御信号出力部と接続している。

[0268] ＡＮＤ回路７０７ｂの出力端ｂ７１は、ネットワーク接続手段７０６の入

力部と接続し、ＡＮＤ回路７０７ｂの入力部の他端ｂ７２は、中央処理手段７０１の出力ポートと接続する。

[0269] ＡＮＤ回路７０７ａの入力部の他端ｂ７３は、ネットワーク接続手段７０６の出力端と接続し、ＡＮＤ回路７０７ａの出力端ｂ７４は、中央処理手段７０１の入力ポートと接続する。

[0270] ＡＮＤ回路の場合、制御信号入力部ｂ７０の入力信号が「０」の時、他の入力部の他端ｂ７３、ｂ７２が「１」，「０」のいずれであっても「０」であり入出力間で遮断状態を形成する。

[0271] 制御信号入力部ｂ７０の入力信号が「１」の場合、他の入力端に入力される信号が「１」のとき、ＡＮＤ回路の出力は「１」、他の入力端の入力信号が「０」のときは、「０」となって、入出力間で接続状態を形成する。

[0272] ＮＯＲ回路の場合、制御信号入力部ｂ７０の入力が「０」のとき、他の入力部の他端ｂ７２の入力信号が「１」の場合、出力端ｂ７５の出力は、「０」で、他の入力部の他端ｂ７２の入力信号が「０」の場合、出力端ｂ７５の出力は、「１」の出力となって、位相が１８０度ずれるが接続状態を形成し、制御信号入力部ｂ７０の入力信号が「１」となると、他の入力端b72等の入力信号が「１」、「０」に変化しても、出力端ｂ７５は、常に「０」であり、遮断状態を形成する。

[0273] 符号７０３は、一時記憶手段を示す。一時記憶手段７０３は、ＲＡＭ（Random Access Memory）等で形成され、揮発性を備えており、一時的に記録するものであって、電源のオフまたはリセット信号により、記憶内容は消去される。一時記憶手段７０３は、制御手段７１１と接続しており、制御手段７１１からのリセット信号により、記憶内容が消去される。消去は、リセット端子にリセット信号を出力したり、一時記憶手段７０３の電源を切っても可能である。

[0274] また、本実施形態は、メーラー用、ブラウザ用と特定の目的用に形成された端末の場合などは、特に中央処理手段７０１は、一時記憶手段７０３に記憶されたプログラムでブート起動可能になっていることが好ましい。しかし

、本実施形態はこの形態に限定されるものではない。

[0275] 符号７０４は、表示手段を示す。表示手段７０４としては、例えば、モニターディスプレイ、各種プリンタ、携帯電話画面等が例示される。スマートフォンのように表示手段とタッチパッドのように指を接触させて入力するような仕様の場合は、入力手段７１０と一体化している場合もあり得る。

[0276] 符号７０５は、データ用一時記憶手段を示し、一時的に記録するＲＡＭで構成されている。データ用一時記憶手段７０５は、一つのドライブとして認識できるようなＲＡＭディスク仕様が好ましい。データ用一時記憶手段７０５は、ダウンロードしたアプリケーション、メール、及び添付ファイルが記録されるところとして用いることが好ましい。

[0277] なお、本実施形態において、データ用一時記憶手段７０５は、説明のために独立した構成として図示したけれども、必要に応じて、一時記憶手段７０３がデータ用一時記憶手段７０５の記憶領域を備えている場合は、省略しても良い。

[0278] また、データ用一時記憶手段７０５は、一時記憶手段７０３と同様、制御手段７１１からのリセット信号によって、内容が消去されるような接続構成を有する。

[0279] 符号７０６は、ネットワーク接続手段を示し、ＬＡＮ接続コネクタ、無線ＬＡＮ用の無線電波、光等の変調、復調を行うフロントエンド回路等で構成されている。

[0280] 符号７０７は、第２遮断接続手段を示す。第２遮断接続手段７０７は、例えば図６Ａで示す回路で形成され、制御回路７１１の信号により、遮断と接続を繰り返すものである。図６Ａにおいて、第２遮断接続手段７０７は、複数のＡＮＤ回路及びＯＲ回路のアレイであって、少なくともデータバスの本数だけ配列されている。

[0281] ＡＮＤ回路列７０７ａの入力部の一端は、制御信号入力部ｂ７６に接続され、入力部の他端ｂ７３は、ネットワーク接続手段７０６の出力端と接続する。制御信号入力部ｂ７６は、制御手段７１１の制御信号出力部と接続する

。

[0282] ＡＮＤ回路列７０７ａの出力端ｂ７４は、中央処理手段７０１の入力ポートに接続する。

[0283] ＡＮＤ回路列７０７ｂの入力部の一端は、制御信号入力部ｂ７０と接続し、入力部の他端ｂ７２は、中央制御手段７０１の出力ポートと接続する。ＡＮＤ回路列７０７ｂの出力端ｂ７１は、ネットワーク接続手段７０６の入力部と接続している。ＮＯＲ回路列７０７ｃの入力端は、同じく制御信号入力部ｂ７０と接続し、入力部の他端ｂ７２は、中央処理手段７０１の出力部に接続する。

[0284] ＮＯＲ回路列７０７ｃの出力端ｂ７５は、検査手段７０９の入力部に接続する。

[0285] 図６Ａの第２遮断接続手段７０７も、他の論理回路によって、形成されてもよい。

[0286] 符号７０８は、第３遮断接続手段を示す。第３遮断接続手段７０８としては、例えば、図６Ｃで示す回路構成が例示される。

[0287] 図６Ｃに具体的に示す回路例において、符号７０８ａは、複数のＡＮＤ回路の配列である。符号ｂ８２は、入力部の他端であり、中央処理手段７０１の出力ポートと接続する。符号ｂ８４は、ＡＮＤ回路７０８ａの出力端であり、データ記録手段７０１２の入力部に接続する。

[0288] 符号ｂ８１ｂは、制御入力部を示し、制御手段ｂ１１の制御出力部と接続する。

[0289] 符号７０８ｂは、複数のＡＮＤ回路の配列であり、入力部の他端ｂ８５は、データ記録手段７０１２のデータ出力部と接続している。ＡＮＤ回路列７０８ｂの出力端ｂ８３は、中央処理手段７０１の入力ポートと接続している。

[0290] 符号ｂ８１ａは、制御入力部であり、制御手段７１１の制御信号出力端と接続している。

[0291] 例えば、制御手段７１１から出力されるデジタル信号が「０」の状態の時

、ＡＮＤ回路列７０８ｂの入力部の他端ｂ８５からの信号が変化しても、出力端ｂ８３の出力が「０」となり、データの伝送を遮断している。ＡＮＤ回路列７０８ａも、制御入力部ｂ８１ｂの制御デジタル信号「０」と「１」で、入力部の他端ｂ８２と、出力端ｂ８４間で伝送される信号の遮断と接続を行う。

[0292] 図６Ｃは、制御手段７１１から２つの異なる制御信号を出力しているが、少なくとも、中央処理手段７０１から、データ記録手段７０１２へのデータの遮断と接続を行うＡＮＤ回路列７０８ａがあれば足りる場合もある。また、図６Ｃのようにデータ記録手段７０１２の入力と出力のそれぞれに、遮断接続手段を設けることで、例えばデータ記録手段７０１２が外部から提供されたＵＳＢメモリ等、内部にウィルスプログラムが存在する可能性があり、携帯されるメディア内のプログラム、データを検証する場合も本実施形態は、好適に利用可能である。

[0293] 例えば、ＡＮＤ回路列７０８ｂを配置して中央処理手段７０１へデータ記録手段７０１２のデータの流入を遮断しておき、データ記録用として使用する際、ＡＮＤ回路列７０８ｂを接続状態としてデータ用一時記憶手段７０５へデータをコピーした後、データ記録手段７０１２内の記録をフォーマットするなどして完全消去し、データ用一時記憶手段７０５内のプログラムを実行して、ウィルスプログラムを検証した後、ウィルスプログラムでなく、保存が必要なプログラム、又はデータを再度データ記録手段７０１２へ記録する。その際、制御手段７１１は、ＡＮＤ回路列７０８ａを接続状態とするデジタル信号「１」を制御入力部ｂ８１ｂへ出力する。

[0294] ＡＮＤ回路列７０８ａが接続状態となった後、保存が必要なプログラムをデータ記録手段７０１２に記録する。図６Ｃで示すように、制御入力部を２つ別々にすることで、ＵＳＢ内のプログラムの検証等を可能とする場合もある。なお、図６Ｃは、その他の論理回路によって形成されてもよい。

[0295] 符号７０９は、検査手段を示す。検査手段７０９は、信号の伝送遮断時の中央処理手段７０１から記憶手段７０２１への信号出力信号、及び中央処理

手段７０１からネットワーク接続手段７０６への伝送用信号を入力し、ウィルスプログラムによって生じた、データの伝送を検出し、ＬＥＤ等で表示したり、ウィルスの発生を示す信号を制御手段７１１へ出力するものである。

[0296] 検査手段７０９として、例えば、ＩＰパケット中の相手ＩＰアドレスを検出して、ウィルスの有無を確認したり、パケットを出力するタイミングを検出してウィルスの存在を検出する手段を用いても良い。

[0297] 検査手段７０９によるウィルスの検出は、出力内容を分析しなくても、通常、出力が無い状況であるにもかかわらずパケットを送信している状態が検出できればよい場合もある。例えば、シフトレジスタにより、データを直列から並列に変換して更にＬＥＤドライバ回路とＬＥＤを接続して、ＬＥＤの点滅の具合などを目視観察する手段でも良い場合もある。

[0298] すなわち、ウィルスプログラムの目的は、外部サーバへ情報を送信させたり、コンピュータ内部のハードディスク等の記録手段に時限プログラム、異常な動作を生じさせるプログラムを記憶させたり、破壊するためのプログラムを記憶させたり、感染したコンピュータの外部との接続を勝手に行い、外部から遠隔操作を可能としたり、パスワード、その他の個人情報を外部へ送信したり、メーラー等の特定のアプリケーションの実行時では、通常は、行わない不自然なデータの伝送を行うことから、これを信号の出力頻度で判定検出するものである。この手法は、ウィルス用のテーブルの更新等を不要とし、未知のウィルスへの防御も可能となる。

[0299] 符号７１０は、入力手段を示す。入力手段７１０は、キーボード、マウス、タッチパッド等のユーザインタフェースで構成されており、本実施形態の大きさ、用途などのファクターに応じて、適宜選択使用される。

[0300] 符号７１１は、制御手段を示す。制御手段７１１は、例えば、各遮断接続手段の接続、遮断を制御するパルスを出力したり、一時記憶手段の記憶をリセットする信号を出力したりする。

[0301] 制御手段７１１は、内部に別途コンピュータを備えても良いが、一定の動作の決まりがある場合や使用者の手動操作による場合は、論理素子等の組み

合わせによって構成されても良い。

[0302] また、制御手段７１１は、中央処理手段７０１と接続しており、中央処理手段７０１が、ダウンロードしたプログラム、添付ファイル、ＵＳＢメモリ等の外部メディアにあらかじめ含まれるプログラムを実行する際の入力手段７１０の入力信号を受信して、それぞれの遮断接続手段に、遮断信号、接続信号を出力する場合もある。

[0303] また、制御手段７１１は、中央処理手段７０１で実行されるＯＳ又はアプリケーション、プログラムに対し、調整可能な時間信号を出力し、実行しているプログラムの時間データを変更する手段を有する。これは、ＯＳの時間データを自動的に変化させるデータを制御手段７１１が出力することで、いわゆるトロイの木馬のように所定の日時で起動するウィルスプログラムを検証することを可能とするものである。

[0304] 必要に応じて、制御手段７１１は、プログラム等を消去するスイッチ、記憶メモリをリセットするスイッチ、通信機能を送信、受信のそれぞれを遮断接続させるスイッチ類を備えた使用者によるマニュアル操作可能な構成であっても良い。

[0305] 符号７０１２は、データ記録手段を示す。データ記録手段７０１２は、ＵＳＢメモリ、ＳＤメモリ、フラッシュメモリチップ、その他のメディアであって、場合によっては、着脱可能な状態のものが使用される。データ記録手段７０１２は、ダウンロードしたプログラム、添付ファイル、メール本文であって、ウィルスプログラムでないことが判明したものを記録する記録メディアである。

[0306] 次に、図６及び図７で示す実施形態の動作を説明する。

[0307] 図示の実施形態は、例えば、メーラープログラム、ブラウザソフトウェア等、外部からウィルスプログラムが侵入する経路にあるプログラムを起動する為の構成を有し、その際の動作の一例を示すものである。

[0308] メールまたはアプリケーションプログラムをダウンロードしていない状態で本実施形態を起動すると、第１遮断接続手段７０２２、第２遮断接続手段

７０７、及び第３遮断接続手段７０８が接続状態となるよう、制御手段７１１は、制御信号を出力する。この出力は、デフォルト状態で例えば、”１”か”０”の信号を継続的に出力している状態が示される。

[0309] 例えば、第１遮断接続手段７０２２を示す図６Ａにおける制御信号入力部ｂ７０に、「１」の信号を継続的に出力する。

[0310] ＡＮＤ回路列７０２ａは、いずれも接続状態となり、入力部の他端ｂ２２１に入力されたデジタル信号は、そのまま出力端ｂ２２２へと伝送される。

[0311] 記憶手段７０２１は、第1遮断接続手段７０２２を介して一時記憶手段７０３にＯＳ、メーラー等をコピーして、中央処理手段７０１は、この一時記憶手段７０３の記憶内容に基づいて起動する。ＲＡＭ起動形式をとることで、実行時、ウィルスプログラムに一時記憶手段７０３が感染したとしても、制御手段７１１からの制御信号により、容易にデータが消去でき、再度、記憶手段７０２１からＯＳ等を一時記憶手段７０３にコピーして現状回復が可能となる。なお、情報流出防止のみを防止する場合等は、一時記憶手段７０３を用いず、第１遮断接続手段７０２２を介した記憶手段７０２１による起動でもよい場合もある。

[0312] 表示手段７０４は、ＯＳの表示が現れ、目的とするソフトウェアを、入力手段７１０を操作して選択する。すると、プログラムをダウンロードするブラウザ表示が現れる。使用者は、入力部７１０を操作して、アプリケーションプログラムを受信する操作を行う。

[0313] 中央処理手段７０１は、例えば、ネットワーク接続手段７０６を介して外部のＷＥＢサーバからアプリケーションプログラムをダウンロードする。ダウンロードしたアプリケーションプログラムは、ネットワーク接続手段７０６、第２遮断接続手段７０７、中央処理手段７０１を介してデータ用一時記憶手段７０５へ記憶される。

[0314] データ用一時記憶手段７０５に記憶されたプログラムは、入力手段７１０の入力操作により、任意に実行される。中央処理手段７０１には、図示していないがバッファメモリがあり、個々に一時的にプログラムがコピーされて

実行するといった一般的な構成を取り入れても良い場合もある。

[0315] ダウンロードしたプログラム、メールの添付ファイル等の実行開始時、制御手段７１１は、それぞれの遮断接続手段に遮断信号を出力する。

[0316] なお、ＨＴＭＬメールのように実行時、外部サーバからデータを送信する場合の為、図６Ａで示すＡＮＤ回路列７０７ａの制御入力部ｂ７６に制御手段７１１から、デジタル信号「１」を出力して、入力部の他端ｂ７３と出力端ｂ７４間に接続状態を形成する。

[0317] 制御手段７１１は、例えば入力手段７１０から出力されるデータに連動して自動的に動作を行うことが好ましい。

[0318] この遮断により、ウィルスが含まれている場合は、感染しようとする媒体との接続が遮断されているため、記録できず、また、外部へ、データを送ることができない状態となっていることから、ウィルスプログラムが実行しても、周囲への影響は無い状況である。

[0319] 検査手段７０９は、この実行しているプログラムの動作を監視し、無用な相手へのデータの送信等があるかないか確認する。

[0320] また、実行状態で、目的に対応した内容かどうかを目視等で確認する。

[0321] ウィルスメール、ダウンロードしたウィルスプログラムは、タイトル等に、偽装があるだけであり、実行または開くことで、要不要が判断できる場合が多いからである。

[0322] 本発明は、プログラム、データを表示することで、タイトルと内容の関係において明らかに偽装的又は不明な関係等があるものは、これをウィルスプログラムとして、削除対象とすることができ、ウィルスリストを含むテーブルなどを要しないで、ウィルス検査が可能となる。

[0323] 検査手段７０９は、遮断後、ダウンロードしたプログラム、添付ファイル、メーラー等が実行時、プログラムの内容等から必要でないとわかるネットワークとの接続を可能とするプロトコル信号を受信している状態を検出表示することで、ウィルスプログラムが実行状態であることが、ある程度認識できることから、中央処理手段７０１で実行しているプログラム等を削除する

。

[0324] 次に受信したメール、プログラムを、データ用一時記憶手段７０５から呼び出して中央制御手段７０１で実行する。

[0325] プログラム、メールの処理が終了した後、一度、一時記憶手段７０３の記録部をリセットする。なお、途中で更にメールをダウンロードしたい場合は、中央処理手段７０１で、アプリケーションプログラム等が実行していない状態として、第２遮断接続手段７０７の遮断を解除して接続状態とする信号を出力する。

[0326] 検査手段７０９の出力が異常であった場合は、制御手段７１１上に異常を示すＬＥＤ表示等が行われ、この表示に基づくか、プログラムの内容が目的とずれていると認識した場合、制御手段７１１上のスイッチを使用者が押すことで、そのプログラムを消去する。

[0327] ウィルスプログラムに感染していない状態で消去した後、中央処理手段７０１は、データ記憶手段のプログラムを、データ記録手段７０１２に記録するが、制御手段７１１は、第３遮断接続手段７０８の遮断状態を接続状態へ切り換える。この切り換えも、使用者の手動でよい場合もある。また、切り換えるタイミングは、プログラムを閉じた状態で、データ用一時記録手段７０５からデータ記録手段７０１２へコピーすることが好ましい。

[0328] ウィルスプログラムに感染している場合は、ＲＡＭ及びＣＰＵ上で実行されているプログラム及びＯＳを削除して、新たに中央処理手段７０１へ記憶手段７０２１に記憶されたＯＳ及びメーラー、閲覧用プログラムを起動させた状態で、コピーすることが好ましい。

[0329] なお、データ記録手段７０１２の記録データの内容の完全消去を制御手段７１１が行う場合もあってもよい。制御手段７１１は、表示されるダウンロードプログラム、添付ファイル、ＨＴＭＬメール、さらには、ＵＳＢ等の携帯可能なメディアに記録されていたプログラムをウィルスの有無に関係なく表示させることができ、消去も簡単に行うことができるものである。

[0330] 〔第８の実施形態〕

次に、図８を参照して本発明の第８の実施形態を説明する。

[0331] 図８の実施形態は、ウィルスプログラム等の検査用プログラムを隔離実行する実行部９２と、この構成を挙動信号に基づいて制御する制御部９１の組み合わせからなる。

[0332] 実行部９２において、符号８０１は、中央処理手段を示す。中央処理手段８０１は、ＣＰＵ、ＭＰＵ等よりなり、ＯＳ及びプログラムを実行し、モニターに表示をしたり、データの移動、削除、変更、の処理を行うものである。

[0333] 符号８０２a、８０２ｂ、８０２ｃ及び８０２ｄは、挙動出力を行う部分を示す。これらの部分では、データの移動を、光、電磁波、赤外線その他の物理的な信号に変換して出力することができ、また、ＲＡＭ、ＲＯＭ、ハードディスク、ＵＳＢメモリへの書き込み、読み出しを表示することができる。

[0334] 挙動出力は、上述したデータの移動に伴う物理的信号を出力するものであり、ＬＥＤや音声等で出力する他、フォトカプラ等の変換器を配置して再度電気信号に置き換えて、外部制御信号として使用する場合もある。更に信号処理の目的に応じ他の物理的信号への変換をしてもよい。

[0335] 符号８０７１は、受信出力表示部を示す。受信出力表示部８０７１は、ネットワーク接続手段８０６から中央処理手段８０１へデータが移動する場合の挙動を表示するものである。符号８０７２は、送信出力表示部を示す。送信出力表示部８０７２は、中央処理手段８０１からネットワーク接続手段８０６方向へデータが移動する時の挙動を出力するものである。このような送信及び受信の際のデータの移動は、データを光、電磁波、赤外線その他の物理的な信号に変換して行う。

[0336] 符号８０２ａ１は、第１読出出力部を示し、記憶手段８０２１からデータを読み出した際のデータの移動を表示するものである。第１読出出力部８０２ａ１で、例えば、記憶ＩＣチップであれば、ＲＥ（リードイネーブル）端子、ＣＳ（チップセレクト）又は、ＣＥ(チップイネーブル)のそれぞれ端子から出力されている信号をＬＥＤで発光させたり、フォトカプラによって、

電光→光電変換して電気信号に変換したりするものである。

[0337] 第２読出出力部８０２ｂ１、第３読出出力部８０２ｃ１、及び第４読出出力部８０２ｄ１も、第１読出出力部８０２ａ１と同様の構成と動作を行うものである。但し、第２読出出力部８０２ｂ１及び第２書込出力部８０２ｂ２は、一時記憶手段８０３のＯＳが書き込まれた領域に相当するシステム記憶部８０３１に接続されている。

[0338] システム記憶部８０３１は、いわゆるＲＡＭボードの一部のＲＡＭとしたり、データが読み書きされるＲＡＭと別々に構成しても良い。

[0339] 符号８０２ａ２は、第１書込出力部を示す。第１書込出力部８０２ａ２は、記憶手段８０２１にデータを書き込む際の書き込み信号であって、記憶ＩＣチップのＷＥ（ライトイネーブル）端子の信号、ＣＳ（チップセレクト）端子から出力される読み出し信号と書き込み信号の混在信号から、読出信号を論理的減算により得られた信号を読出信号として用いてもよい。

[0340] 第２書込出力部８０２ｂ２、第３書込出力部８０２ｃ２、及び第４書込出力部８０２ｄ２も、第１書込出力部８０２ａ２と同様の構成と動作を行うものである。

[0341] 符号８０２１は、記憶手段であり、ＯＳ、アプリケーションが記憶されており、例えば、ポータブルアプリケーション、ＫＮＯＰＰＩＸ（商標）、ＡＮＤＲＯＩＤ（商標）、ＷＩＮＤＯＷＳ　ＰＥ（商標）、ＷＩＮＤＯＷＳ　ＣＥ（商標）などの小容量ＯＳ、その他通常のＯＳ、アプリケーションが記憶されている。

[0342] 符号８０２２は、第1遮断接続手段を示し、記憶手段８０２１と中央処理手段８０１間のデータ移動信号を制御手段８１１からの電気リード線８１１ｂを介して伝達される制御信号でオンオフ動作を行う。

[0343] 符号８０３は、一時記憶手段を示し、ＲＡＭメモリ等、一時的に記憶する為の手段であり、例えば電源を切ることで、内容が消去されるようなＩＣチップを有する。一時記憶手段８０３は、ＯＳを起動する為にＯＳがシステム記憶部８０３１にコピーされて使用されることが好ましい。

[0344] 符号８０４は、表示手段を示す。表示手段８０４は、プログラムが実行された際のデータ表示、メニュー表示等の表示部であり、例えば液晶モニタが例示される。表示手段８０４は、好ましくは、中央処理手段８０１と、制御手段８１１の双方に表示可能に接続しており、例えば、１画面に個々の手段に関する表示がされた複数のウィンドウとすることが好ましいが、場合によっては、２以上のモニタで構成されても良い。

[0345] 上述の表示は、入力手段８０９ａ、８０９ｂと組み合わせることで、ＧＵＩ（グラフィカルユーザインターフェース）を形成しても良く、タッチパッド構成でも良い。

[0346] 表示手段８０４は、中央処理手段８０１と、制御手段８１１の両方に接続してもよく、それぞれの表示を同時に又は異なるタイミングで表示しても良い。

[0347] 符号８０５は、検査データ記憶手段を示す。検査データ記憶手段８０５は、メールデータ、添付ファイルデータ、その他、検査用のデータ（プログラムデータ等を含む）を一時的に記録するためのものであり、ＲＡＷ、フラッシュメモリ、ＥＥＰＲＯＭ等で構成されても良いが、ウィルスプログラムによる感染状態を解消させる為に、ＲＡＭが好ましい。

[0348] 符号８０６は、ネットワーク接続手段を示し、有線ＬＡＮ、無線ＬＡＮ仕様を形成する。ネットワーク接続手段８０６は、インターネット、エクストラネット等の外部ネットワークと接続する入出力端８Ｉと接続する。

[0349] ネットワーク接続手段８０６と制御手段８１１は、受信側として電気リード線８１１ｋを介して接続し、送信側として電気リード線８１１Ｉを介して接続される。なお、この例は、全二重方式に係る場合で、半二重方式の場合は、一本であっても良い場合もある。

[0350] 符号８０７は、第２遮断接続手段を示す。第２遮断接続手段８０７は、ネットワーク接続手段８０６と、中央処理手段８０１間のデータの移動を遮断したり、接続したりする為のものであって、制御手段８１１と電気リード線８１１ｅと接続し、制御手段８１１の制御信号によってオンオフ駆動する。

[0351] 符号８０１２は、データ記録手段を示す。データ記録手段８０１２は、例えば、ＵＳＢメモリ、ＳＤカード等のメデイアなどの継続的な記憶ができるメモリで構成され、好ましくは、着脱可能な構成を有する。

[0352] データ記録手段８０１２は、例えば、検査が必要なデータが記録されているメデイアであり、ＵＳＢソケット等、メデイア接続コネクタを含むものである。

[0353] 符号８０８は、第３遮断接続手段を示す。第３遮断接続手段８０８は、中央処理手段８０１とデータ記録手段８０１２とのデータの移動を遮断したり接続したりするものであって、制御手段８１１から電気リード線８１１ｄを介して伝達される制御信号によりオンオフ駆動を行うものである。

[0354] 符号８０９ａは、入力手段を示す。入力手段８０９ａは、キーボード、マウス、タッチパネル等からなり、制御手段８１１に接続する。入力手段８０９ａは、上述したように表示手段８０４と一体的に形成されても良い。

[0355] 符号８０９ｂは、入力手段を示す。入力手段８０９ｂは、動作命令、データ入力の為に中央処理手段８０１と接続するものである。入力手段８０９ｂは、キーボード、マウスなどで形成されても良いが、入力手段８０９ａと共有化されることが好ましい場合もある。

[0356] 符号８１０は、メールデータ記憶手段を示す。メールデータ記憶手段８１０は、ＲＡＭ、フラッシュメモリ、ＥＥＰＲＯＭ等の記憶素子によって構成されており、インターネットを介してメールサーバからのメールデータ、添付データを一時的又は継続的に記録するものである。

[0357] メールデータ記憶手段８１０に記憶されるデータは、少なくともコンピュータ上で実行不可能な状態で記憶されることが好ましく、暗号化、圧縮化、その他の変換、変更のプロテクトが行われた状態が好ましい。

[0358] メールデータ記憶手段８１０から、データが読み出され、検査データ記憶手段８０５へ移動する際、プロテクトがかかったデータをプロテクト解除された状態にすることが好ましい。当該プロテクトは、処理時間を短縮する為、バーナム暗号系などのストリーム暗号が好適に利用されることが好ましい

。

[0359] 符号８０１３は、切換手段を示す。切換手段８０１３は、マルチプレクサ、切り換えスイッチなどで形成され、中央処理手段８０１と検査データ記憶手段８０５の接続と、検査データ記憶手段８０５とメールデータ記憶手段８１０との接続の両者を、制御手段８１１の制御信号により切り換えるものである。

[0360] 符号８１１は、制御手段を示す。制御手段８１１は、好ましくはコンピュータによって構成され、ハードディスク等の継続的記憶装置を装着し、マウス等、使用者が操作を行う入力手段８０９ａを備えている。

[0361] 制御手段８１１は、各挙動情報表示部と、電気リード線によって接続状態を形成し、更に、第１遮断接続手段８０２２、第２遮断接続手段８０７及び切換手段８０１３の各切り換え、オンオフ制御を行う部分と電気リード線を介して接続状態が形成されている。

[0362] 第１読出出力部８０２ａ１及び第１書込出力部８０２ａ２の出力信号は、複数の電気リード線８１１ｆを介して制御手段８１１に入力するように接続し、

受信表示出力部８０７１及び送信表示出力部８０７２の出力信号は、複数の電気リード線８１１ｈを介して制御手段８１１が入力するように接続し、

第２読出出力部８０２ｂ１及び第２書込出力部８０２ｂ２の出力信号は、複数の電気リード線８１１ｇを介して制御手段８１１が入力するように接続し、

第３読出出力部８０２ｃ１及び第３書込出力部８０２ｃ２の出力信号は、複数の電気リード線８１１ｉを介して制御手段８１１へ入力するように接続し、

第４読出出力部８０２ｄ１及び第４書込部８０２ｄ２の出力信号は、複数の電気リード線８１１ｊを介して制御手段８１１に入力するように接続し、

制御手段８１１と切換手段８０１３は、制御手段８１１の出力信号が、切換手段８０１３の切り換え動作をさせるべく電気リード線８１１ｅを介して

接続し、制御手段８１１の制御信号が、第１遮断接続手段８０２２をオンオフ駆動させる為に、電気リード線８１１ｂを介して接続し、

制御手段８１１の制御信号は、第２遮断接続手段８０７をオンオフ駆動させる為に、電気リード線８１１ｃを介して接続する。

[0363] 制御手段８１１と中央処理手段８０１は、複数の電気リード線８１１ａを介して接続し、制御手段８１１の動作開始停止、及びリセット信号を中央処理手段８０１へ出力するものであって、一方向の信号のみ伝達するものである。

[0364] これら電気リード線は、必ずしも線状でなく、基板上のパターン化された電気回路で形成されても良い。また、このリード線であって、制御手段８１１から制御信号が出力する電気リード線には、フォトカプラ等の電気的に分離した手段が接続しても良い。当該フォトカプラは、当該信号の目的が、オンオフ程度の１ビット信号又は、数ビット信号の情報量を持つ程度であれば良く、仮に情報量が大きいデータが入力された場合でも、フィルタ動作を行って、情報量を少なくするような伝送形態が好ましい。

[0365] 実行部９２と制御部９１は、同一の起動を行うように起動スイッチが形成されていることが好ましいが、別々に起動させても良い場合もある。

[0366] 次に、図８で示す実施形態の動作を説明する。

[0367] 起動時、第１遮断接続手段８０２２を接続状態、第２遮断接続手段８０７は遮断状態、第３遮断接続手段８０８は遮断状態、切換手段８０１３は、中央処理手段８０１と検査データ記憶手段８０５を接続する状態となっている（デフォルト）。

[0368] 電源スイッチを入れると、実行部９２、制御部９１が動作を開始する。

[0369] 中央処理手段８０１は、記憶手段８０２１に記憶されたＯＳ、アプリケーションを一時記憶手段のシステム記憶部８０３１に展開記憶させ、実行状態とする。その際、第１読出出力部８０２ａ１は、データの移動を挙動情報（例えばＬＥＤの点滅）で出力し、その挙動情報が終了すると、制御手段８１１は、第１遮断接続手段８０２２をオフするような信号を出力する。

[0370] この制御手段８１１から、電気リード線８１１ｂを介して伝達されたオフ信号は、第１遮断接続手段８０２２を遮断（オフ）状態とさせる。

[0371] 中央処理手段８０１は、データ処理が可能な状態となっている。

[0372] 制御手段８１１は、ネットワーク接続手段８０６を介してインターネット上のメールサーバと接続し、メールサーバ上のメールを全て、ダウンロードして、メールデータ記憶手段８１０へ記憶する。この制御手段８１１の動作は、使用者の入力手段８０９ａの入力操作によって実現されてもよく、自動で行われても良い。

[0373] その際、メールサーバ（図示せず）上のメールは、消去されることが好ましいが、消去されずに、後で、ウィルス感染メールデータをピックアップするためのデータとして利用する等、残しておいても良い。

[0374] 制御手段８１１は、メールデータ記憶手段８１０で記憶されたメールデータの内の一つを、検査データ記憶手段８０５へ移動するよう切換手段８０１３に切り換え信号を出力し、切り換え完了後、検査データ記憶手段８０５へ、メールデータが移動させる。

[0375] メールデータは、メール本文と、添付ファイル、メール本文に貼り付けられた画像データの３つのパターンで、任意に一つずつ移動される。

[0376] 一つのメールデータが検査データ記憶手段８０５へ移動した後、すなわち、第３読出出力部８０２ｃ１の点滅が消えた後、制御手段８１１は、切換手段８０１３を切り換える信号を出力して、中央処理手段８０１と検査データ記憶手段８０５を接続する。

[0377] 中央処理手段８０１は、検査データ記憶手段８０５にメールデータが存在していることを確認すると、このメールデータを実行する。実行は、データの種類が、例えば、テキストデータであれば、ＮＯＴＥＰＡＤ（商標）等のテキスト表示プログラム、ＨＴＭＬであれば、ＦＩＲＥＦＯＸ（商標）等のブラウザソフトウェアが、連動して起動する。

[0378] この実行プログラムは、実行部起動時に、一時記憶手段８０３のシステム記憶部８０３１にＯＳなどがコピーされた後、初期実行プログラムとして起

動している。

[0379] 制御手段８１１は、第２読出出力部８０２ｂ１、第２書込出力部８０２ｂ２、第３読出出力部８０２ｃ１、第３書込出力部８０２ｃ２及び第４読出出力部８０２ｄ１、第４書込出力部８０２ｄ２の挙動、又は、この挙動を変換した電気信号として入力しながら、データの移動、消去、書き換えを監視する。

[0380] これらの挙動状態で、例えば、メールを表示するだけの動作にもかかわらず一時記憶手段８０３内のシステム記憶部８０３１へ書き込みがあった場合、制御手段８１１は、この信号を信号線８１１ｇを介してウィルスの感染の可能性を示す信号を受け取り、リセット信号を電気リード線８１１ａを介して出力し、リセット信号は、中央処理手段８０１にリセット動作を行うか、ウィルス感染の可能性の表示を表示手段８０４へ表示し、使用者の意志を尋ねる状態を形成した後、使用者の操作によりリセット起動がされる。

[0381] このため、一時記憶手段８０３、検査データ記憶手段８０５のデータが消滅することから、ウィルスプログラムも当然消滅する。

[0382] 第１遮断接続信号８０２２は、リセット信号の出力と併せて制御手段８１１からの信号により、記憶手段８０２１と中央処理手段８０１との接続を行い。記憶手段８０２１のＯＳ、アプリケーションは一時記憶手段８０３内のシステム記憶部８０３１に記憶して、ブート状態を形成する。

[0383] これは、図示しないが、中央処理手段８０１にＢＩＯＳプログラムを記録したＲＯＭ（Read Only Memory）が接続されており、このＢＩＯＳプログラムに基づいて起動する。

[0384] リセット信号により、中央処理手段８０１は、リセット状態となって、検査データ記憶手段８０５の内容も消滅し、最初の状態に戻る。

[0385] 制御手段８１１が、実行部９２が最初の状態に戻ったかどうかを判定するのは、所定時間後であっても良く、第１遮断接続手段８０２２に遮断する信号を出力した時でも良い。

[0386] メール実行後、各挙動出力手段に異常な挙動が無い場合は、所定の時間後

、制御手段８１１は、切換手段８０１３に、メールデータ記憶手段８１０と検査データ記憶手段８０５の接続を行い、検査データ記憶手段８０５のメールデータを再度戻すと共に、正常な状態であることの記号を付ける。

[0387] なお、所定時間の間、中央処理手段８０１は、内蔵クロックを変更したりして、ウィルスのプログラムが実行状態でないかを確認してもよい。

[0388] このように、メールデータ記憶手段８１０には、正常なメールデータが、正常であるとの表示と共に残留する。

[0389] 表示手段８０４は、検査データ記憶手段８０５に記憶されたデータが実行されると、その内容を表示することで、目視で、正常なメールを読むことができ、また、挙動情報に基づいて、リセット信号が出力される前に、挙動情報に対応したメール又は添付ファイルが、表示され、ウィルス感染のおそれを示すメッセージを表示してもよい。

[0390] メールデータ記憶手段８１０に記憶されたメールが、検査データ記憶手段に移動する際、データを消去しながら、正常なデータのみを残しても良い。また、場合によっては、メールデータ記憶手段８１０のデータを消去せず、正常とウィルス感染データを区別した表示を伴う状態を形成しても良い。

[0391] 制御手段８１１は、メールデータ記憶手段８１０内のメールの検査が終了した後、内部のメールデータを他の記憶領域へ移動させて、通常のメール処理を行っても良い。

[0392] 図８で示す構成は、実行部９２から電気信号を入力することなく、挙動情報を示す書込出力、読出出力を検出して、それにもとづいて制御を行っている。このように構成することで、実行部で活動するウィルスプログラムが形成する信号の影響を受けることなく、未知のウィルスプログラムの検出消去を行うことができる。

[0393] 次いで、メールデータのうち、ＨＴＭＬメールの場合の実行部９２の動作を説明する。

[0394] 制御手段８１１は、メールデータを検査データ記憶手段８０５へ移動させる際、データの識別子を判定して、ＨＴＭＬ形式である場合、第２遮断接続

手段８０７を接続する。

[0395] 検査データ記憶手段８０５が、切換手段８０１３を介して中央処理手段８０１と接続して、中央処理手段８０１が、検査データ記憶手段８０５のＨＴＭＬデータを実行すると、送信表示出力部８０７２及び受信表示出力部８０７１が、データの移動を示す挙動を表示出力する。

[0396] その間、第２読出出力部８０２ｂ１、第３読出出力部８０２ｃ１、第２書込出力部８０２ｂ２、第３書込出力部８０２ｃ２の出力表示において、書き込みがされないタイミングであるにも関わらず、書き込みがされる挙動があるかどうかが監視される。

[0397] 書き込みがあった場合は、制御手段８１１は、この表示出力データに基づいて、リセット信号を電気リード線８１１ａを介して出力し、一時記憶手段８０３及び検査データ記憶手段８０５のデータを消去する。

[0398] 以上の動作説明は、メールデータの操作の説明であるが、その他、ＵＳＢメモリのウィルス感染の検査を行う動作を説明する。

[0399] ＵＳＢメモリからなるデータ記録手段８０１２を装着する。このとき、中央処理手段８０１は、オートラン機能等、挿入しただけで起動しない状態となっているか、第３遮断接続手段８０８がオフの状態となっている。第３遮断接続手段８０８は、通常、遮断状態となっており、制御手段８１１の入力手段８０９ａのユーザの入力により開始されることが好ましい。

[0400] 入力手段８０９ａからの入力により、制御手段８１１は、第３遮断接続手段８０８を接続状態とすると共に、一時記憶手段８０３に記録されているＵＳＢデータ検査プログラムが実行状態となる。

[0401] データ記録手段８０１２内のＵＳＢデータの一覧を表示手段８０４に表示する。

[0402] 入力手段８０９ｂからデータを選択し、又は、全部自動実行を選択する。

[0403] データ記録手段８０１２のデータの一つが検査データ記憶手段８０５に移動する。

[0404] 制御手段８１１は、８０２ｅ１の挙動と第４読出出力部８０２ｄ１の挙動

により、第３遮断接続手段８０８を遮断する。

[0405] 検査データ記憶手段８０５に記憶されたデータは、中央処理手段８０１で実行され、内容が表示手段８０４に出力表示される。

[0406] 内容が表示され、所定時間経過後であって、第３書込出力部８０２ｃ２、第４読出出力部８０２ｄ１、及び第２読出出力部８０２ｂ１の挙動に異常が無い場合は、制御手段８１１が、第３遮断接続手段８０８を接続状態として、このデータに検査結果データを付加して上書き又は書き込みを行う。

[0407] この動作は、中央処理手段８０１の動作に基づき、次のデータをデータ記録手段８０１２から読み取り、検査データ記憶手段８０５へ記憶する。このとき、制御手段８１１は、８０２ｅ１及び第４読出出力部８０２ｄ１の挙動により、第３遮断接続手段８０８を遮断状態にする信号を出力する。

[0408] 検査データ記憶手段８０５に記憶されたデータは、実行される。その際、第３読出出力部８０２ｃ１、データが送信される挙動を表示する第２書込出力部８０２ｂ２、第４読出出力部８０２ｄ１の挙動に異常がある場合は、制御手段８１１は、中央処理手段８０１へリセット信号を出力する。その際、制御手段８１１は、表示手段８０４に異常を示すメッセージを表示し、その表示による、使用者の入力手段８０９ａを介した入力を待って、リセット出力を行っても良い。

[0409] 中央処理手段８０１は、このリセット信号を受けてリセットされ、また、制御手段８１１は、第１遮断接続手段８０２２を接続状態とする。

[0410] 中央処理手段８０１は、記憶手段８０２１に記憶されたＯＳ等のプログラムがブートされ、一時記憶手段８０３のシステム記憶部８０３１にＯＳなどが展開記憶される。

[0411] このリセット操作により、感染したＯＳ、プログラムは消去され、制御手段８１１は、リセット後の第１読出出力部８０２ａ１、第３書込出力部８０２ｃ２の挙動状態が終了した時、第１遮断接続手段８０２２の接続を遮断する。

[0412] データ記録手段８０１２のデータは、そのまま検査ログが無い状態で保存

されるか、消去される。

[0413] 本実施形態においても、ネットワーク接続手段８０６から得られたメール関連データは、一度、プロテクト手段（暗号化、符号化等、再現可能な変換手段）で変換して、メールデータ記憶手段８１０に記憶させ、検査データ記憶手段８０５へ入力される時点で、復号変換手段で、再現してもよい。

[0414] 不正プログラムの実行について、不正プログラムは、個人情報やパスワードの流出を行ったり、不正にデータの書き換え、破壊を行うプログラムを指し示すことが多いが、不正プログラムもウィルスプログラムと同様の挙動をとると言い得るのであり、その際、図８の送信出力表示部８０７２の発光状態、メールアドレスが蓄積されたメモリーの発光状態で示される挙動が、プログラム実行から所定の期間、多い場合、不正プログラムの可能性が大きいというメッセージを表示手段に表示したり、消去しますのメッセージを表示し、リセット実行をしてもよい。

[0415] また、検査データ記憶手段８０５のデータを実行表示させ、ウィルス感染の可能性があって、リセットをかける必要があるデータを保存する場合は、データ記録手段８０１２へデータを記録する場合、符号化変換を行って、実行不可能な状態にしてもよい。

産業上の利用可能性

[0416] 以上に説明したように、本発明によれば、スピア型の目的を明確にしたウィルスプログラムの感染、プログラムダウンロードによるウィルスデータの流入やＵＳＢメモリ等の既存メディアに含まれるウィルスプログラムその他のウィルスの感染を気にすることなく、安定したメール通信、インターネット接続、データ閲覧が可能であると共に、ウィルスの検出を可能とすると共に、アクセス攻撃によるサーバ機能低下を防止もできることから、ＢtoＢ（Business to Business）、ＢtoＣ（Business to Consumer)等の電子商取引、電子政府、メールを用いた社内手続き等、現在利用されているメールを使用した様々な分野で大いに利用可能とする。

請求の範囲

［請求項1］ 外部データを入力する入力手段、前記入力手段で入力した外部データを所定の領域で実行する実行手段、前記実行時、前記実行領域をその他の領域から遮断する遮断制御手段を含んでなる安全ボックス。

［請求項2］ 前記実行手段で実行された外部データの挙動を表示する表示手段、

前記表示手段で表示された挙動に基づいて、前記外部データが正常データか否かを判定する判定手段、前記判定手段で正常データでないと判定されたデータ及び／又は実行手段の全部のデータを消去する消去手段を更にさらに含む、請求項１に記載の安全ボックス。

［請求項3］ 前記外部データの挙動が、実行手段で、データが実行される前記実行領域内のデータの移動に対応して外部で認識可能な情報である、請求項２に記載の安全ボックス。

［請求項4］ 前記外部データの挙動が、光信号、超音波信号、音波信号、磁気信号、電磁気信号及び熱信号から群から選ばれる１乃至複数の信号を組み合わせた情報である、請求項２に記載の安全ボックス。

［請求項5］ 前記外部データの挙動が、記憶部のデータの書込及び／又は読出、前記入力手段のデータの出力及び／又は入力動作に対応した情報である、請求項２に記載の安全ボックス。

［請求項6］ 前記外部データが、プログラム、メール関連データ、ダウンロードアプリケーション又は記録メディア既存データである、請求項１に記載の安全ボックス。

［請求項7］ 前記遮断制御手段が、データをデジタル記憶する領域とデジタルデータを処理する中央処理領域との間のデータ伝送及び／又はデータを処理する中央処理領域と外部ネットワークの接続を行うネットワーク接続領域との間のデータ伝送を遮断及び接続をする、請求項１に記載の安全ボックス。

［請求項8］ 前記実行手段は、ＯＳプログラム、メーラープログラム、ブラウザプログラム、アプリケーションプログラム又はビューアープログラム

を、ＲＡＭ又はその他の一時記憶手段に記憶し、前記一時記憶手段の記憶データに基づいて起動するコンピュータプロセッサを備え、前記遮断制御手段は、前記一時記憶手段の記録内容を消去可能とする、請求項１に記載の安全ボックス。

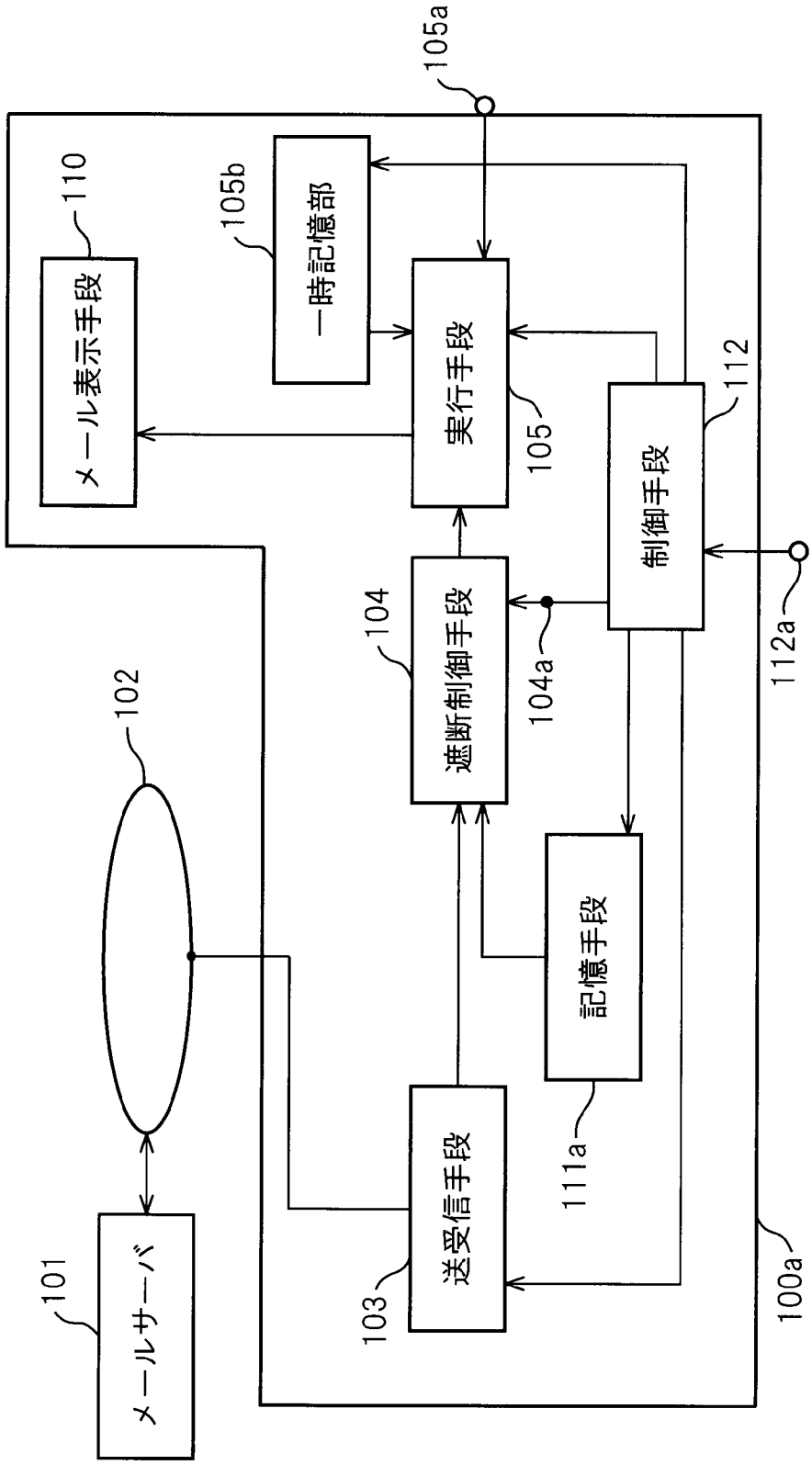
［請求項9］ 前記判定手段で、ウィルス感染状態が検出された場合であって少なくとも受信したメールを送信する場合に警告を出力する、請求項２に記載の安全ボックス。

［請求項10］ 前記正常でないデータが、コンピュータウィルスプログラム、ワームプログラム、トロイの木馬タイプのプログラム、実行エラー又はコンピュータがハングアップを起こすプログラム又は外部から正常でないデータを呼び込むプログラムである、請求項２に示す安全ボックス。

［請求項11］ 外部データの供給頻度を検出して所定の頻度を超えた時、前記外部データと、データ処理部とのデータ伝送路を遮断する遮断手段、前記遮断手段で、遮断された外部データから、送信元の送信頻度を計測し、送信頻度が所定値より超えたとき、攻撃データとして削除又は整理して、前記データ処理部へ送信する削除制御手段を備える安全ボックス。

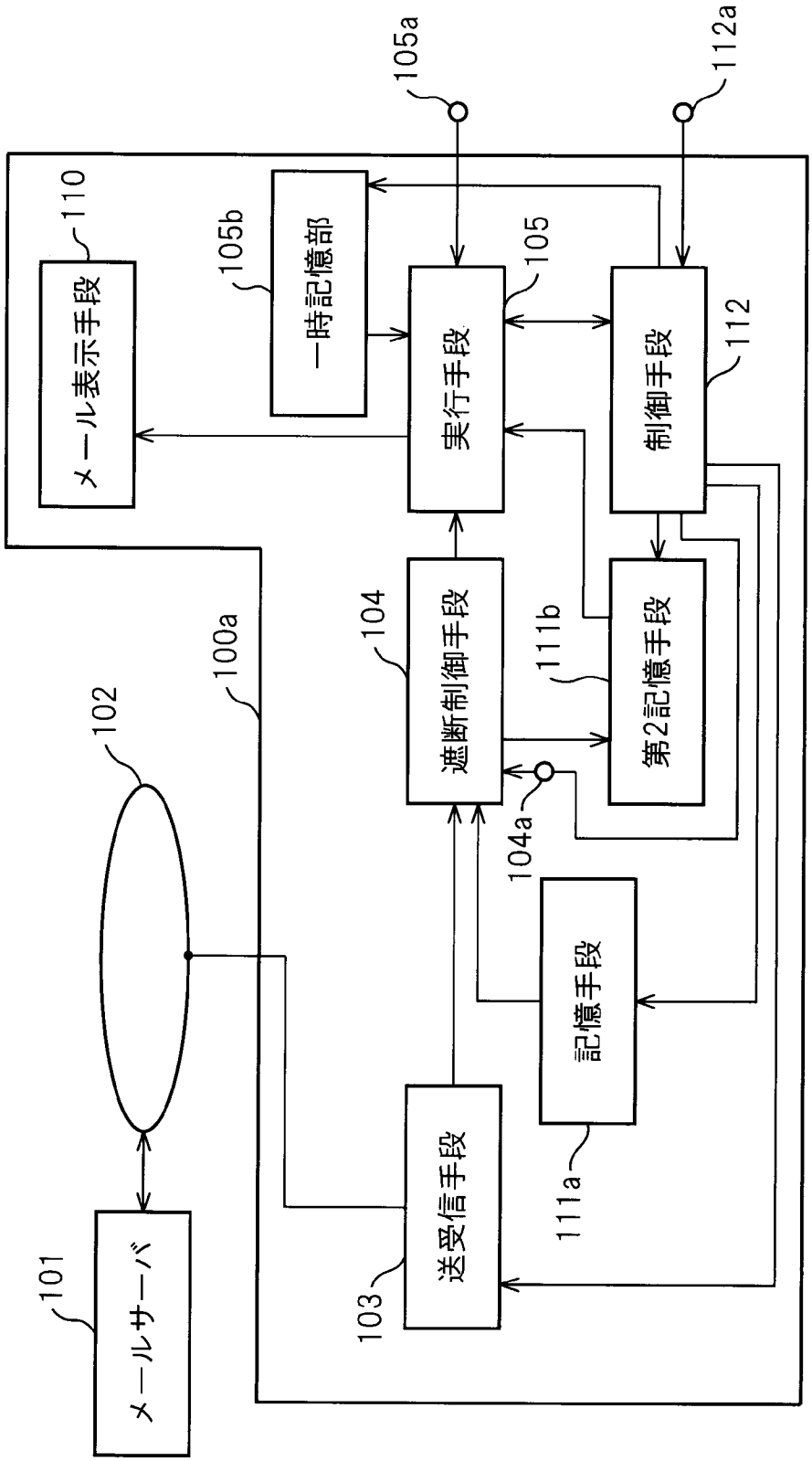
[図1A]

図1A


105a
110
メール表示手段
105b
一時記憶部
実行手段
105
112
制御手段
112a
104
遮断制御手段
104a
102
記憶手段
111a
送受信手段
103
101
メールサーバ
100a

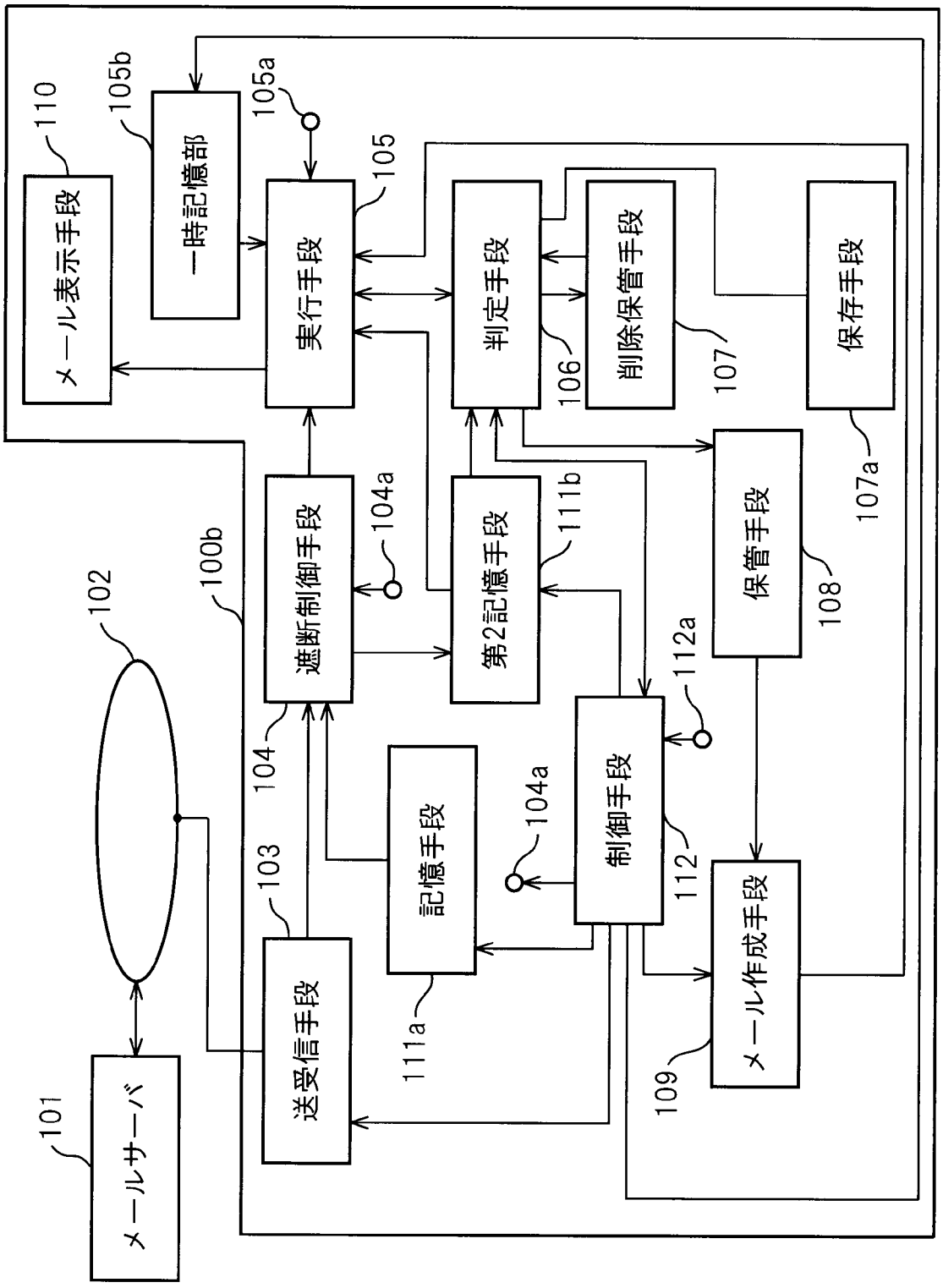
[図1B]

図1B


105a
112a
110
メール表示手段
105b
一時記憶部
実行手段
105
制御手段
112
100a
104
遮断制御手段
111b
第2記憶手段
102
104a
記憶手段
111a
送受信手段
103
101
メールサーバ

[図2]

図2


メールサーバ
101
送受信手段
103
遮断制御手段
104
104a
実行手段
105
105a
一時記憶部
105b
メール表示手段
110
判定手段
106
削除保管手段
107
保存手段
107a
第2記憶手段
111b
記憶手段
111a
制御手段
112
112a
保管手段
108
メール作成手段
109
102
100b

[図3]

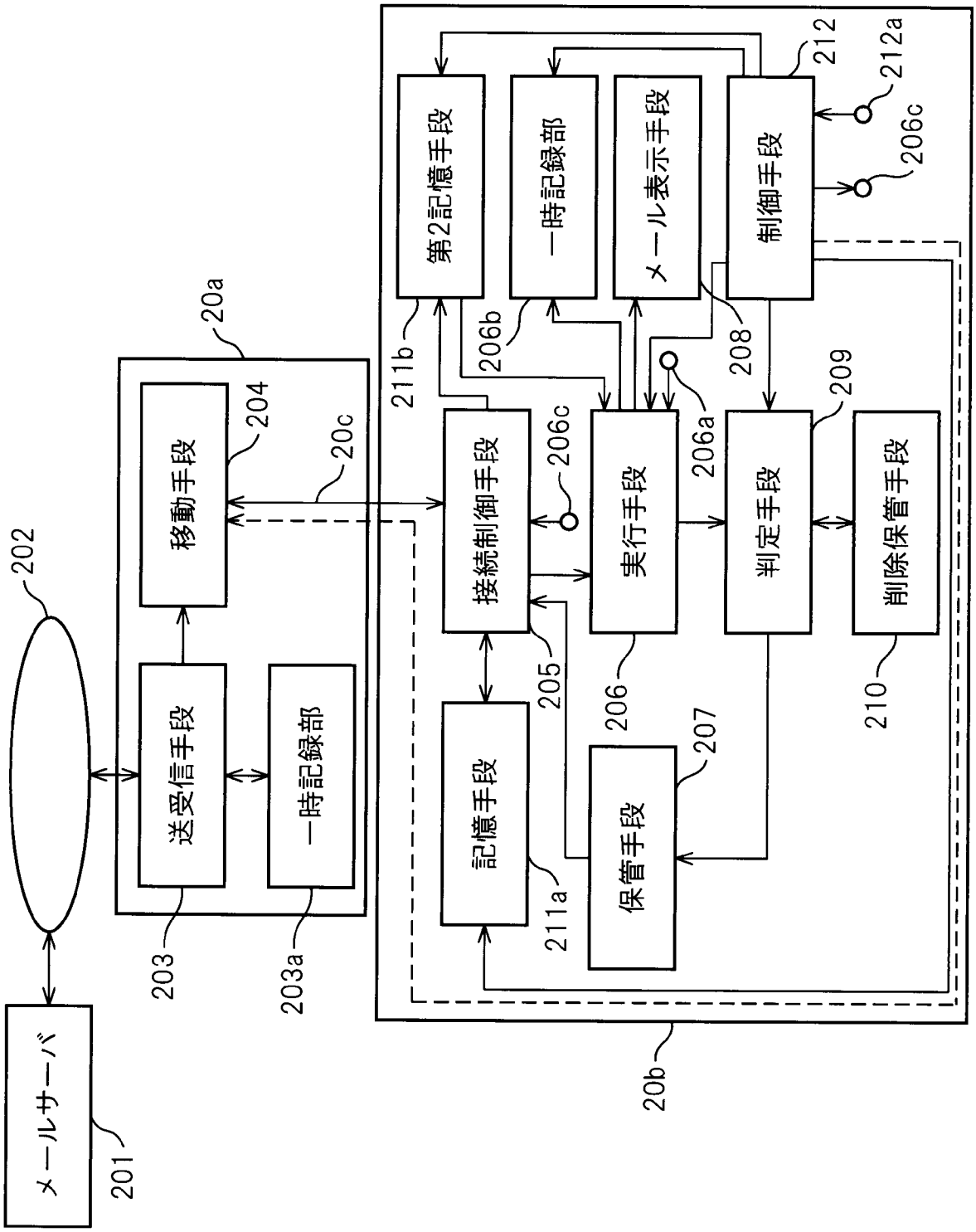
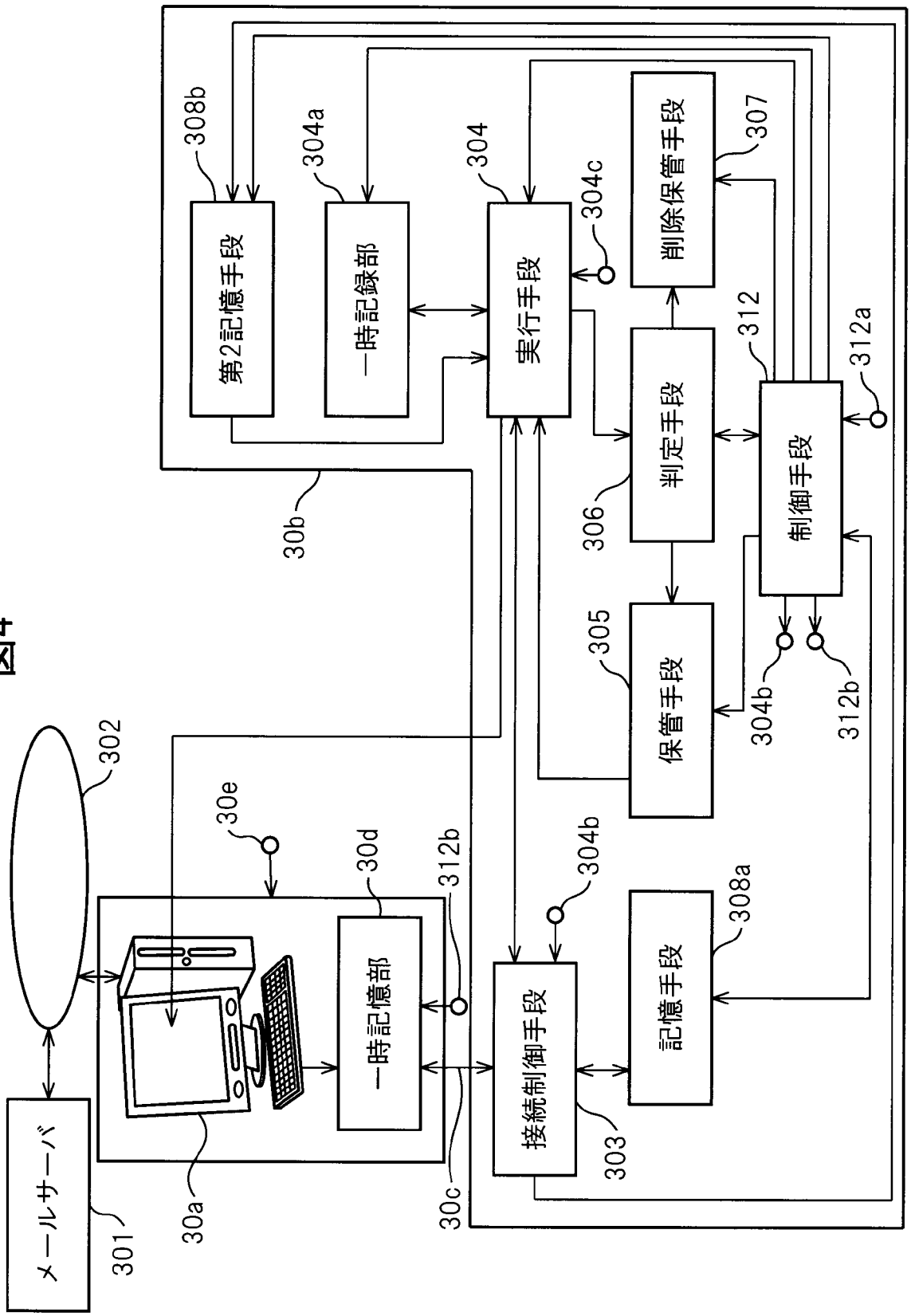

メールサーバ
201
202
送受信手段
203
一時記録部
203a
移動手段
204
20a
20c
接続制御手段
205
206c
記憶手段
211a
実行手段
206
206a
保管手段
207
判定手段
209
削除保管手段
210
20b
第2記憶手段
211b
一時記録部
206b
メール表示手段
208
制御手段
212
212a
206c

図3

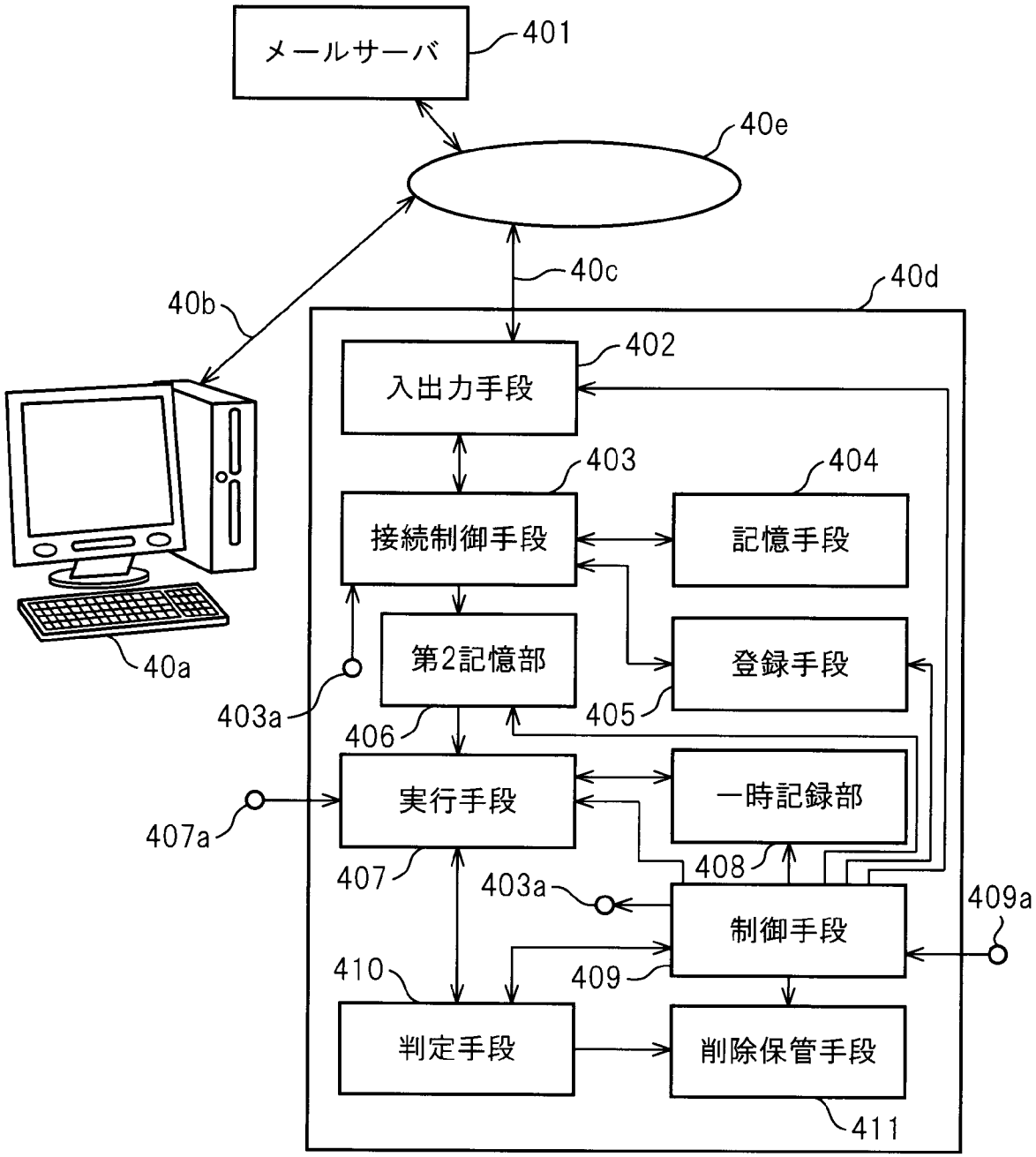
[図4]

図4


メールサーバ
301
302
30a
30b
30c
30d
30e
一時記憶部
312b
304b
接続制御手段
303
記憶手段
308a
保管手段
305
306
判定手段
312
制御手段
312a
304b
312b
実行手段
304c
304
削除保管手段
307
一時記録部
304a
第2記憶手段
308b

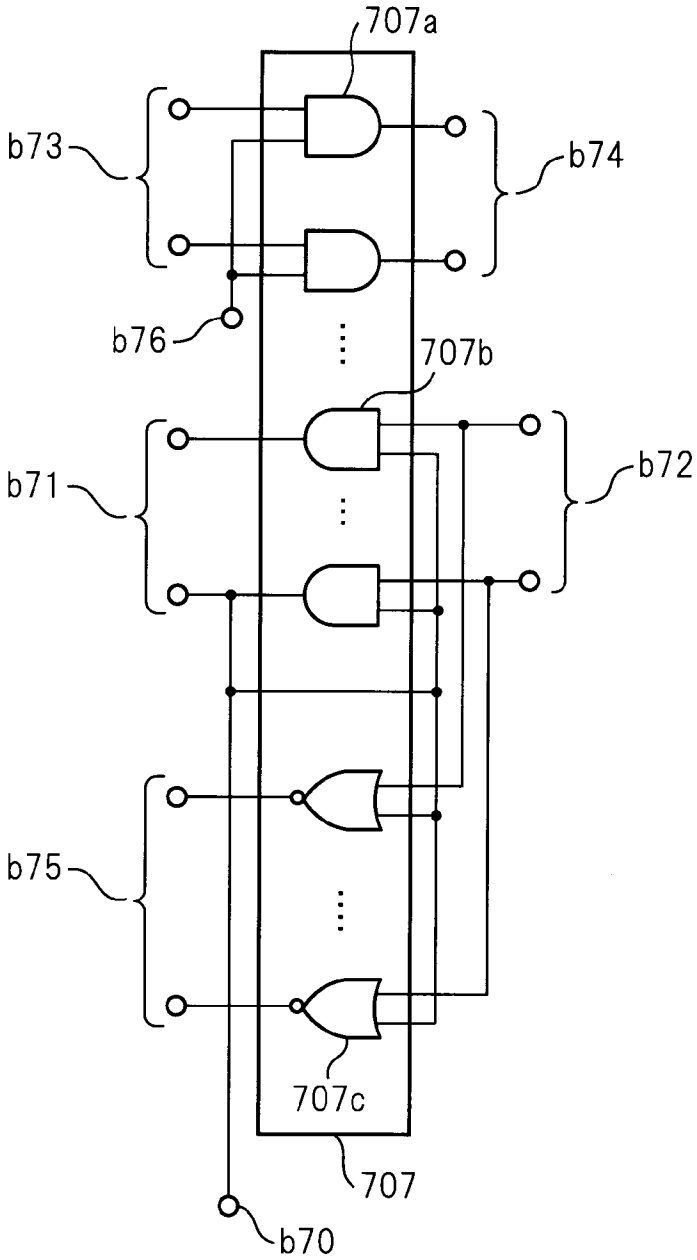
[図5]

図5


メールサーバ
401
40e
40c
40d
40b
402
入出力手段
403
404
接続制御手段
記憶手段
第2記憶部
登録手段
40a
403a
405
406
実行手段
一時記録部
407a
407
408
403a
409a
制御手段
410
409
判定手段
削除保管手段
411

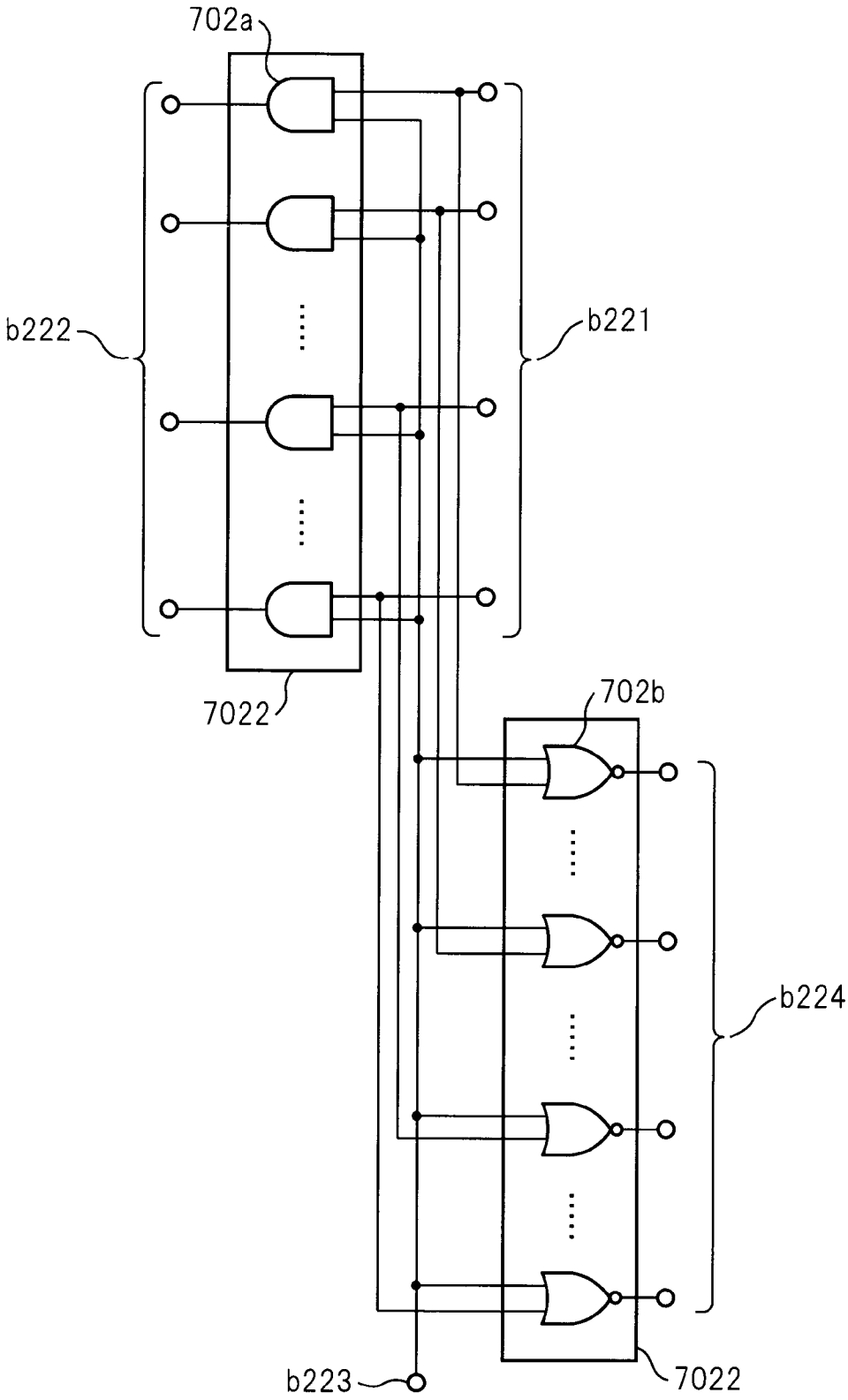
[図6A]

図6A



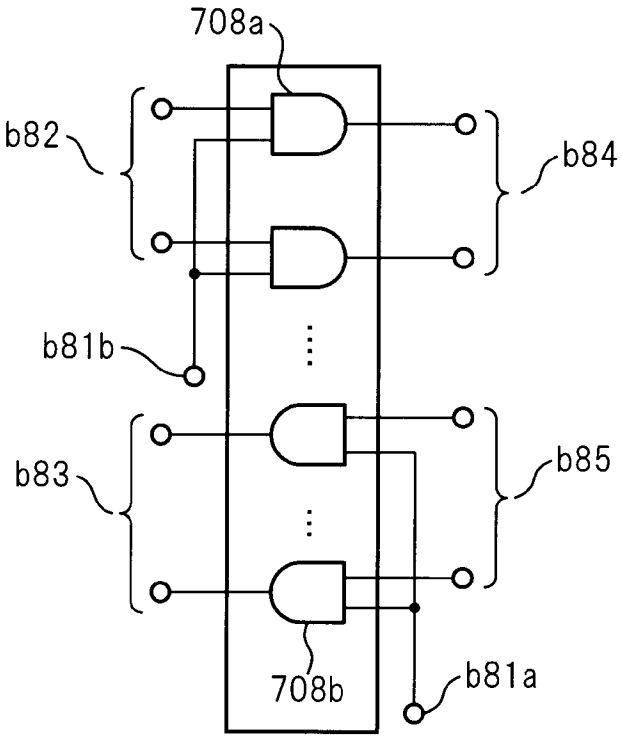
[図6B]

図6B



[図6C]

図6C



[図7]

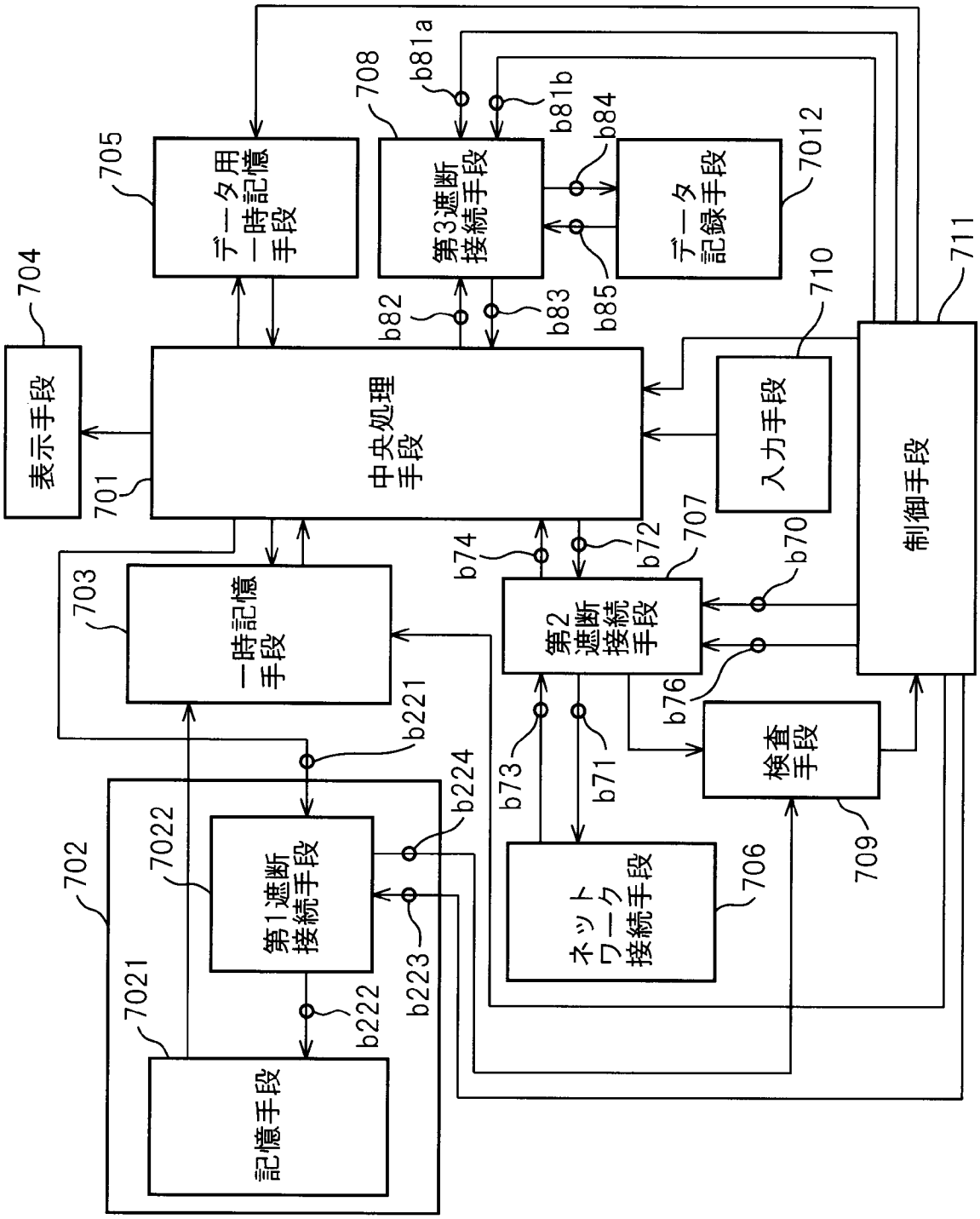

表示手段
704
中央処理手段
701
データ用一時記憶手段
705
第3遮断接続手段
708
データ記録手段
7012
入力手段
710
制御手段
711
一時記憶手段
703
第2遮断接続手段
707
検査手段
709
ネットワーク接続手段
706
第1遮断接続手段
7022
記憶手段
7021
702
b81a
b81b
b84
b85
b83
b82
b74
b72
b70
b76
b73
b71
b221
b224
b223
b222

図7

[図8]

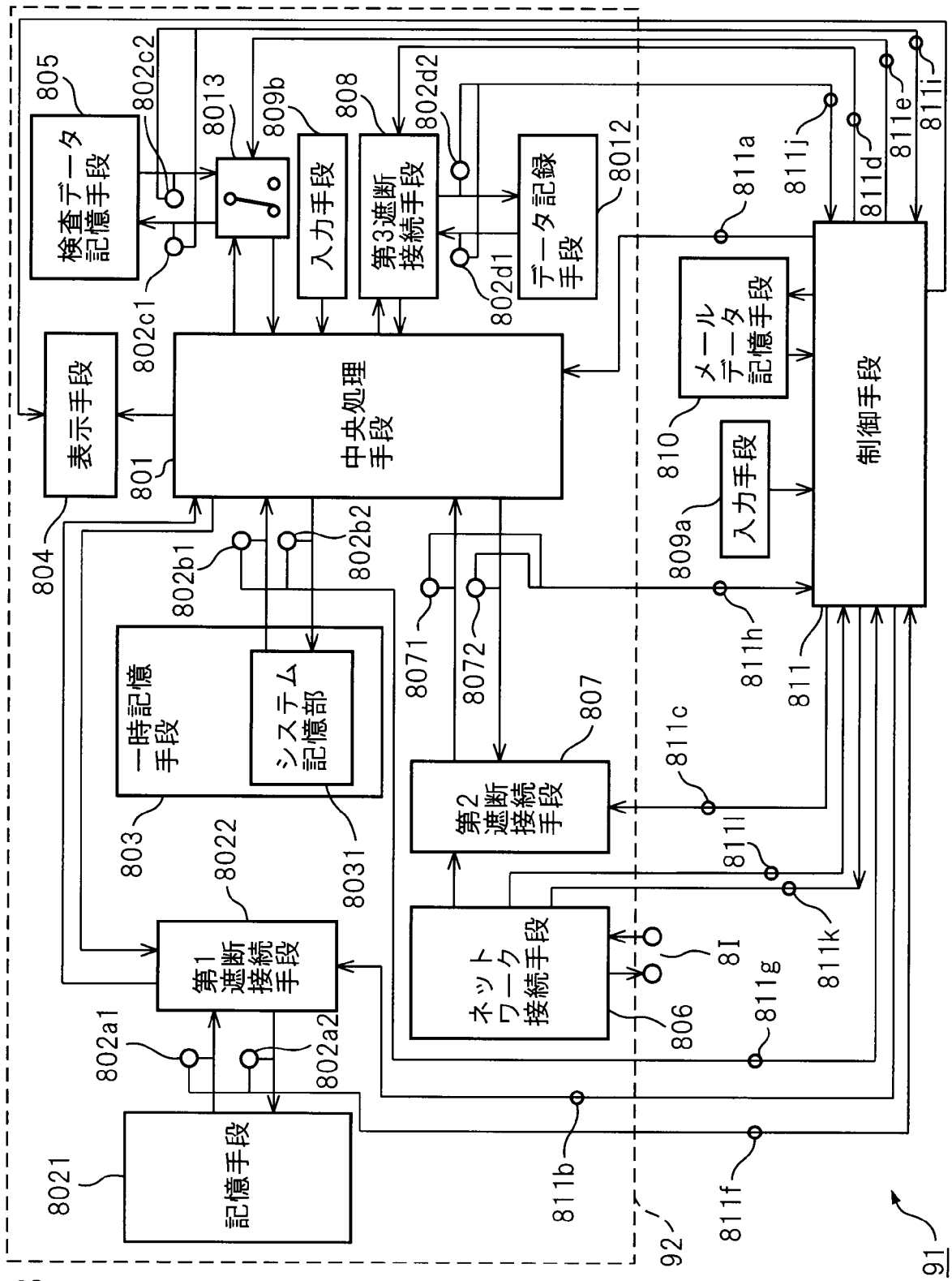

検査データ記憶手段
805
802c2
8013
809b
入力手段
808
第3遮断接続手段
802d2
802d1
データ記録手段
8012
811a
811j
811d
811e
811i
表示手段
804
802c1
801
中央処理手段
メールデータ記憶手段
810
制御手段
入力手段
809a
802b1
802b2
8071
8072
811h
811
一時記憶手段
システム記憶部
803
8031
807
811c
第2遮断接続手段
8022
811l
第1遮断接続手段
802a1
802a2
ネットワーク接続手段
8I
806
811g
811k
8021
記憶手段
811b
811f
92
91

図8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/078868

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/56(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2013
Kokai Jitsuyo Shinan Koho	1971-2013	Toroku Jitsuyo Shinan Koho	1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2004-104739 A (Hironori WAKAYAMA et al.), 02 April 2004 (02.04.2004), paragraphs [0026] to [0035]; fig. 1, 2 (Family: none)	1,6-8 2-5,9,10
Y A	JP 2008-500653 A (Intel Corp.), 10 January 2008 (10.01.2008), paragraphs [0027] to [0029] & US 2006/0021029 A1 & WO 2006/012197 A2 & CN 1961272 A	1,6-8 2-5,9,10
A	WO 1998/008163 A1 (APM LTD.), 26 February 1998 (26.02.1998), fig. 4 & US 6065118 A & JP 2000-516740 A	1-10

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 January, 2013 (28.01.13)	05 February, 2013 (05.02.13)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2012/078868

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
See extra sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-10

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Continuation of Box No.III of continuation of first sheet(2)

The technical feature common to the invention of claim 1 and the invention of claim 11 is a security box for securely performing blocking for external data.

The technical feature, however, cannot be considered as a special technical feature since it does not define a contribution over the prior art in view of the disclosure of document 1 (JP 2004-104739 A (Hironori WAKAYAMA et al.), 02 April 2004 (02.04.2004), paragraphs [0026] to [0035]; fig. 1, 2) in which data is read from an information processing apparatus (1) as an external apparatus, and an information processing apparatus (2) performs blocking by turning off all the switches SW 1 through 3 and then executes packet filtering and content filtering.

Further, there is no other same or corresponding special technical feature between these inventions.

Accordingly, the following two inventions (invention groups) are involved in claims.

(Invention 1) the inventions of claims 1-10

A security box for executing an external data in a predetermined area.

(Invention 2) the invention of claim 11

A security box comprising: a blocking means for blocking a data transmission path between external data and a data processing unit when the frequency of supply of the external data is detected and exceeds a predetermined frequency; and a deletion controlling means which measures the frequency of transmission from a source based on the external data blocked by the blocking means, and transmits to the data processing unit by deleting or organizing as attack data when the frequency of transmission exceeds a predetermined value.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１２／０７８８６８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/56(2013.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/56

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１３年
日本国実用新案登録公報	１９９６－２０１３年
日本国登録実用新案公報	１９９４－２０１３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y A	JP 2004-104739 A（若山裕典他）2004.04.02, 【0026】-【0035】, 図1,図2（ファミリーなし）	1,6-8 2-5,9,10
Y A	JP 2008-500653 A（インテル・コーポレーション）2008.01.10, 【0027】-【0029】 & US 2006/0021029 A1 & WO 2006/012197 A2 & CN 1961272 A	1,6-8 2-5,9,10
A	WO 1998/008163 A1 (APM LIMITED) 1998.02.26, Fig.4 & US 6065118 A & JP 2000-516740 A	1-10

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ２８．０１．２０１３	国際調査報告の発送日 ０５．０２．２０１３
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　９５５５ 宮司　卓佳 電話番号　０３－３５８１－１１０１　内線　３５４６

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１２／０７８８６８

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

１．☐ 請求項 ＿＿＿＿＿＿＿＿ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

２．☐ 請求項 ＿＿＿＿＿＿＿＿ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

３．☐ 請求項 ＿＿＿＿＿＿＿＿ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

特別ページ参照

１．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求項について作成した。

２．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求項について調査することができたので、追加調査手数料の納付を求めなかった。

３．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求項のみについて作成した。

４．☑ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求項について作成した。

請求項１－１０

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。

☐ 追加調査手数料の納付はあったが、異議申立てはなかった。

請求項１に係る発明と、請求項１１に係る発明とは、外部データに係る遮断を安全に行う安全ボックスであるという共通の技術的特徴を有している。

しかしながら、当該技術的特徴は、文献 1(JP 2004-104739 A (若山裕典他) 2004.04.02, 【0026】-【0035】,図 1,図 2)に開示された内容である、外部装置である情報処理装置（１）からデータを読み込み、スイッチＳＷ１－３をすべてオフとする遮断を行った上でパケットフィルタリング及びコンテンツフィルタリングを実行する情報処理装置（２）に照らして、先行技術に対する貢献をもたらすものではないから、当該技術的特徴は、特別な技術的特徴であるとはいえない。

また、これらの発明の間には、他に同一の又は対応する特別な技術的特徴は存在しない。

そして、請求の範囲には、以下に示す２群の発明（群）が含まれる。

（発明１）請求項１－１０に係る発明
所定の領域で外部データを実行する安全ボックス。

（発明２）請求項１１に係る発明
外部データの供給頻度を検出して所定の頻度を超えた時、外部データと、データ処理部とのデータ伝送路を遮断する遮断手段、遮断手段で、遮断された外部データから、送信元の送信頻度を計測し、送信頻度が所定値より超えたとき、攻撃データとして削除又は整理して、データ処理部へ送信する削除制御手段を備える安全ボックス。