

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4973912号
(P4973912)

(45) 発行日 平成24年7月11日(2012.7.11)

(24) 登録日 平成24年4月20日(2012.4.20)

(51) Int. Cl.		F I			
G06F 13/00	(2006.01)	G06F 13/00	610A		
H04M 1/00	(2006.01)	H04M 1/00	R		
G06F 17/30	(2006.01)	G06F 13/00	510A		
		G06F 17/30	340A		

請求項の数 9 (全 14 頁)

(21) 出願番号	特願2006-117397 (P2006-117397)	(73) 特許権者	000004237
(22) 出願日	平成18年4月21日(2006.4.21)		日本電気株式会社
(65) 公開番号	特開2007-293397 (P2007-293397A)		東京都港区芝五丁目7番1号
(43) 公開日	平成19年11月8日(2007.11.8)	(74) 代理人	100102864
審査請求日	平成21年3月11日(2009.3.11)		弁理士 工藤 実
		(72) 発明者	神田 俊之
			東京都港区芝五丁目7番1号 日本電気株式会社内
		審査官	小林 義晴

最終頁に続く

(54) 【発明の名称】 携帯端末、アクセス制限方法

(57) 【特許請求の範囲】

【請求項1】

送信しようとするデータの内容をメモリに一時保管する手段と、
前記データの宛先が既に送信履歴がある宛先か否か確認する手段と、
前記データの宛先が新たな宛先である場合、前記データの内容及び前記新たな宛先を所定の通知先に通知する手段と、
前記所定の通知先から送信可否の通知を受信する手段と、
前記送信可否の通知の内容が送信不可である場合、前記新たな宛先を送信不可リストに追加する手段と、
前記データの宛先が前記送信不可リスト上にあるか否か判定する手段と、
前記データの宛先が送信不可リスト上にある場合、前記データの送信が不可である旨を表示した上で送信を中止する手段と、
前記データの宛先が送信不可リスト上にない場合、前記データの内容及び宛先のうち少なくとも1つに、所定のキーワードが含まれているか確認する手段と、
前記所定のキーワードが含まれている場合、前記データの送信が不可である旨を表示した上で送信処理を中止する手段と、
前記所定のキーワードが含まれていない場合、前記データの送信を実行する手段とを具備する
携帯端末。

【請求項2】

請求項 1 に記載の携帯端末であって、
受信しようとするデータの内容をメモリに一時保管する手段と、
前記データの送信元が既に受信履歴がある送信元か否か確認する手段と、
前記データの送信元が新たな送信元である場合、前記データの内容及び前記新たな送信元を所定の通知先に通知する手段と、
前記所定の通知先から受信可否の通知を受信する手段と、
前記受信可否の通知の内容が受信不可である場合、前記新たな送信元を受信不可リストに追加する手段と、
前記データの送信元が前記受信不可リスト上にあるか否か判定する手段と、
前記データの送信元が受信不可リスト上にある場合、前記データの受信が不可である旨を表示した上で受信を中止する手段と、
前記データの送信元が受信不可リスト上にない場合、前記データの内容及び送信元のうち少なくとも1つに、所定のキーワードが含まれているか確認する手段と、
前記所定のキーワードが含まれている場合、前記データの受信が不可である旨を表示した上で受信処理を中止する手段と、
前記所定のキーワードが含まれていない場合、前記データの受信を実行する手段と
を更に具備する
携帯端末。

10

【請求項 3】

請求項 1 又は 2 に記載の携帯端末であって、
アクセスしようとする Web サイトの内容をメモリに一時保管する手段と、
前記 Web サイトの URL が既にアクセス履歴がある URL か否か確認する手段と、
前記 Web サイトの URL が新たな URL である場合、前記 Web サイトの内容及び前記新たな URL を所定の通知先に通知する手段と、
前記所定の通知先からアクセス可否の通知を受信する手段と、
前記アクセス可否の通知の内容がアクセス不可である場合、前記新たな URL をアクセス不可リストに追加する手段と、
前記 Web サイトの URL が前記アクセス不可リスト上にあるか否か判定する手段と、
前記 Web サイトの URL がアクセス不可リスト上にある場合、前記 Web サイトへのアクセスが不可である旨を表示した上でアクセスを中止する手段と、
前記 Web サイトの URL がアクセス不可リスト上にない場合、前記 Web サイトの内容及び URL のうち少なくとも1つに、所定のキーワードが含まれているか確認する手段と、
前記所定のキーワードが含まれている場合、前記 Web サイトへのアクセスが不可である旨を表示した上でアクセス処理を中止する手段と、
前記所定のキーワードが含まれていない場合、前記 Web サイトへのアクセスを実行する手段と
を更に具備する
携帯端末。

20

30

【請求項 4】

携帯端末により実施されるアクセス制限方法であって、
送信しようとするデータの内容をメモリに一時保管することと、
前記データの宛先が既に送信履歴がある宛先か否か確認することと、
前記データの宛先が新たな宛先である場合、前記データの内容及び前記新たな宛先を所定の通知先に通知することと、
前記所定の通知先から送信可否の通知を受信することと、
前記送信可否の通知の内容が送信不可である場合、前記新たな宛先を送信不可リストに追加することと、
前記データの宛先が前記送信不可リスト上にあるか否か判定することと、
前記データの宛先が送信不可リスト上にある場合、前記データの送信が不可である旨を

40

50

表示した上で送信を中止することと、

前記データの宛先が送信不可リスト上にない場合、前記データの内容及び宛先のうち少なくとも1つに、所定のキーワードが含まれているか確認することと、

前記所定のキーワードが含まれている場合、前記データの送信が不可である旨を表示した上で送信処理を中止することと、

前記所定のキーワードが含まれていない場合、前記データの送信を実行することとを含む

アクセス制限方法。

【請求項5】

請求項4に記載のアクセス制限方法であって、

受信しようとするデータの内容をメモリに一時保管することと、

前記データの送信元が既に受信履歴がある送信元か否か確認することと、

前記データの送信元が新たな送信元である場合、前記データの内容及び前記新たな送信元を所定の通知先に通知することと、

前記所定の通知先から受信可否の通知を受信することと、

前記受信可否の通知の内容が受信不可である場合、前記新たな送信元を受信不可リストに追加することと、

前記データの送信元が前記受信不可リスト上にあるか否か判定することと、

前記データの送信元が受信不可リスト上にある場合、前記データの受信が不可である旨を表示した上で受信を中止することと、

前記データの送信元が受信不可リスト上にない場合、前記データの内容及び送信元のうち少なくとも1つに、所定のキーワードが含まれているか確認することと、

前記所定のキーワードが含まれている場合、前記データの受信が不可である旨を表示した上で受信処理を中止することと、

前記所定のキーワードが含まれていない場合、前記データの受信を実行することとを更に含む

アクセス制限方法。

【請求項6】

請求項4又は5に記載のアクセス制限方法であって、

アクセスしようとするWebサイトの内容をメモリに一時保管することと、

前記WebサイトのURLが既にアクセス履歴があるURLか否か確認することと、

前記WebサイトのURLが新たなURLである場合、前記Webサイトの内容及び前記新たなURLを所定の通知先に通知することと、

前記所定の通知先からアクセス可否の通知を受信することと、

前記アクセス可否の通知の内容がアクセス不可である場合、前記新たなURLをアクセス不可リストに追加することと、

前記WebサイトのURLが前記アクセス不可リスト上にあるか否か判定することと、

前記WebサイトのURLがアクセス不可リスト上にある場合、前記Webサイトへのアクセスが不可である旨を表示した上でアクセスを中止することと、

前記WebサイトのURLがアクセス不可リスト上にない場合、前記Webサイトの内容及びURLのうち少なくとも1つに、所定のキーワードが含まれているか確認することと、

前記所定のキーワードが含まれている場合、前記Webサイトへのアクセスが不可である旨を表示した上でアクセス処理を中止することと、

前記所定のキーワードが含まれていない場合、前記Webサイトへのアクセスを実行することと

を更に含む

アクセス制限方法。

【請求項7】

送信しようとするデータの内容をメモリに一時保管するステップと、

10

20

30

40

50

前記データの宛先が既に送信履歴がある宛先か否か確認するステップと、
前記データの宛先が新たな宛先である場合、前記データの内容及び前記新たな宛先を所定の通知先に通知するステップと、
前記所定の通知先から送信可否の通知を受信するステップと、
前記送信可否の通知の内容が送信不可である場合、前記新たな宛先を送信不可リストに追加するステップと、
前記データの宛先が前記送信不可リスト上にあるか否か判定するステップと、
前記データの宛先が送信不可リスト上にある場合、前記データの送信が不可である旨を表示した上で送信を中止するステップと、
前記データの宛先が送信不可リスト上にない場合、前記データの内容及び宛先のうち少なくとも1つに、所定のキーワードが含まれているか確認するステップと、
前記所定のキーワードが含まれている場合、前記データの送信が不可である旨を表示した上で送信処理を中止するステップと、
前記所定のキーワードが含まれていない場合、前記データの送信を実行するステップとを携帯端末に実行させるためのプログラム。

【請求項 8】

請求項 7 に記載のプログラムであって、
受信しようとするデータの内容をメモリに一時保管するステップと、
前記データの送信元が既に受信履歴がある送信元か否か確認するステップと、
前記データの送信元が新たな送信元である場合、前記データの内容及び前記新たな送信元を所定の通知先に通知するステップと、
前記所定の通知先から受信可否の通知を受信するステップと、
前記受信可否の通知の内容が受信不可である場合、前記新たな送信元を受信不可リストに追加するステップと、
前記データの送信元が前記受信不可リスト上にあるか否か判定するステップと、
前記データの送信元が受信不可リスト上にある場合、前記データの受信が不可である旨を表示した上で受信を中止するステップと、
前記データの送信元が受信不可リスト上にない場合、前記データの内容及び送信元のうち少なくとも1つに、所定のキーワードが含まれているか確認するステップと、
前記所定のキーワードが含まれている場合、前記データの受信が不可である旨を表示した上で受信処理を中止するステップと、
前記所定のキーワードが含まれていない場合、前記データの受信を実行するステップとを更に携帯端末に実行させるためのプログラム。

【請求項 9】

請求項 7 又は 8 に記載のプログラムであって、
アクセスしようとする Web サイトの内容をメモリに一時保管するステップと、
前記 Web サイトの URL が既にアクセス履歴がある URL か否か確認するステップと、
前記 Web サイトの URL が新たな URL である場合、前記 Web サイトの内容及び前記新たな URL を所定の通知先に通知するステップと、
前記所定の通知先からアクセス可否の通知を受信するステップと、
前記アクセス可否の通知の内容がアクセス不可である場合、前記新たな URL をアクセス不可リストに追加するステップと、
前記 Web サイトの URL が前記アクセス不可リスト上にあるか否か判定するステップと、
前記 Web サイトの URL がアクセス不可リスト上にある場合、前記 Web サイトへのアクセスが不可である旨を表示した上でアクセスを中止するステップと、
前記 Web サイトの URL がアクセス不可リスト上にない場合、前記 Web サイトの内

10

20

30

40

50

容及びURLのうち少なくとも1つに、所定のキーワードが含まれているか確認するステップと、

前記所定のキーワードが含まれている場合、前記Webサイトへのアクセスが不可である旨を表示した上でアクセス処理を中止するステップと、

前記所定のキーワードが含まれていない場合、前記Webサイトへのアクセスを実行するステップと

を更に携帯端末に実行させるための

プログラム。

【発明の詳細な説明】

【技術分野】

10

【0001】

本発明は、携帯端末に関し、特に子供向け携帯端末に関する。

【背景技術】

【0002】

携帯電話に代表される携帯端末は低価格化が進むにつれ、業務利用だけでなくホームユースにまで利用が拡大している。同時に、その利用者は大人だけでなく、小学生を含む子供にまで広がりつつある。

【0003】

それは、非常時の通報や、位置のリアルタイム確認や、多忙な親子におけるコミュニケーション手段として有益である一方、子供による有害サイトへのWebアクセスや、逆に匿名性を利用した有害なメール受信の機会を与えてしまいかねない。

20

【0004】

これに対して、これまでも、パソコンにおける有害サイトへの自動ブロック機能としてWebブラウザにコンテンツアダプタが搭載されるなど、多くのアクセス制限方法が提案されている。

【0005】

しかし、その設定は利用者本人が行う必要があったり、設定される閾値はある程度想定される集団に対する一律なものであったりと、生育段階に応じて個別の保護判定を要する子供向けのものとは言えなかった。

【0006】

30

関連する技術として、特開2005-202700号公報(特許文献1)に移動通信端末が開示されている。

この移動通信端末は、特定キーワードを記憶するキーワード記憶手段と、外部端末との間でデータ通信を行う際、前記外部端末からの受信データ若しくは前記外部端末への送信データに前記特定キーワードが含まれているか否かを判断する判断手段と、前記受信データ若しくは前記送信データに前記特定キーワードが含まれている場合には、該特定キーワードを含むログデータを生成する生成手段と、前記生成手段によって生成されたログデータを保存する保存手段とを具備することを特徴とする。

【0007】

また、特開2005-311482号公報(特許文献2)に携帯電話装置が開示されている。

40

この携帯電話装置は、電波を送受信するアンテナと、上記アンテナで受信した電波を変換するRF部と、上記RF部とデータを送受信する送受信制御部と、特定の電話番号を記憶する電話番号記憶部と、上記特定の電話番号と受信した電話番号とを比較して一致検出を行う電話番号比較部と、書き換え可能な情報/ソフトウェアを記憶する記憶部と、上記記憶部の情報/ソフトウェアに基づき通話や各種サービスを実行する通話/サービス実行部とを備える。また、上記電話番号比較部での一致信号により接続中の相手方電話装置から通信回線を通じて上記記憶部をアクセスして上記通話/サービス実行部で実行される機能の一部又は全部を制限することが可能とされてなることを特徴とする。

【0008】

50

特開 2006-4213 号公報 (特許文献 3) に通信管理システムが開示されている。

この通信管理システムは、通信の宛先を通知してこの宛先への接続の許可を要求する接続許可要求手段を備えた被保護者側通信端末と、この被保護者側通信端末の管理を依頼した管理側通信端末と、前記被保護者側通信端末ごとに宛先と接続の可否の結果を対応付けた通信可否データベースと、前記被保護者側通信端末から接続要求があったときその宛先への接続の可否をこの通信可否データベースを用いて検索する検索手段と、この検索手段の検索の結果、接続を否とするとき前記接続要求の宛先への接続を拒否する接続拒否手段と、前記検索手段の検索の結果、接続を可とする時、或いは前記通信可否データベースに該当する宛先が存在しない時接続を実行する接続実行手段と、前記通信可否データベースに該当する宛先が存在しない時その宛先を前記被保護者側通信端末と対応付けて新規宛先としてその被保護者側通信端末の管理を依頼した前記管理側通信端末に通知して以後の接続の可否を問う新通信先通知手段とを備えた管理サーバとを具備することを特徴とする。

10

【0009】

【特許文献 1】特開 2005-202700 号公報

【特許文献 2】特開 2005-311482 号公報

【特許文献 3】特開 2006-4213 号公報

【発明の開示】

【発明が解決しようとする課題】

【0010】

本発明の目的は、携帯端末上で送受信される電子メールや、閲覧される Web サイトのコンテンツに、子供にとって有害な情報を遮断すると共に、保護者にその旨が自動的に通知することを可能とする携帯端末を提供することである。

20

【課題を解決するための手段】

【0011】

以下に、[発明を実施するための最良の形態] で使用される番号を括弧付きで用いて、課題を解決するための手段を説明する。これらの番号は、[特許請求の範囲] の記載と [発明を実施するための最良の形態] との対応関係を明らかにするために付加されたものである。但し、それらの番号を、[特許請求の範囲] に記載されている発明の技術的範囲の解釈に用いてはならない。

【0012】

30

本発明の携帯端末は、送受信されるコンテンツ内容を一時保管するメモリ (1) と、所定のキーワードを保持する単語データベース (2) と、前記コンテンツ内容に前記所定のキーワードが含まれているか確認する判定コントローラ (3) と、前記コンテンツ内容に前記所定のキーワードが含まれている場合、前記所定のキーワードを含むコンテンツ内容へのアクセスが行われる旨を、外部へ通知する警告通知部 (4) と、前記コンテンツ内容に対するアクセス可否判断を受信する許可情報受信部 (5) と、前記アクセス可否判断の結果、前記コンテンツ内容がアクセス不可とされた場合、前記コンテンツ内容の送信又は受信に用いられる宛先情報を保持する宛先データベース (6) と、前記コンテンツ内容の表示可否を判定する表示コントローラ (7) とを具備する。

【0013】

40

前記メモリ (1) は、電子メールの内容を保管するメモリ作業領域を一時的に共有する形で確保されている。

【0014】

前記単語データベース (2) は、外部から前記所定のキーワードが送信されてきた時、前記所定のキーワードを保持する。

【0015】

前記警告通知部 (4) は、携帯端末の契約者の通信端末に電子メールで通知する。

【0016】

前記宛先データベース (6) は、携帯端末の電話帳データベースに送信可否のフラグを追加する形で確保されている。

50

【0017】

前記表示コントローラ(7)は、前記コンテンツ内容の送信又は受信に用いられる宛先情報が前記宛先データベース(6)に格納されていなければ、前記コンテンツ内容を表示画面に表示するように制御する。

【0018】

本発明のアクセス制限方法は、(a1)作成された電子メールの宛先、表題、本文をメモリ(1)に保管するステップと、(a2)前記宛先が送信履歴にある宛先か否かについて確認するステップと、(a3)前記宛先が新たな宛先である場合、携帯端末から設定された通知相手に、前記電子メールの内容と共に新たな宛先である旨を通知するステップと、(a4)前記通知相手から前記電子メールの送信可否を示す情報を受信し、送信不可であれば前記電子メールの宛先をアクセス不可リストに登録するステップと、(a5)前記携帯端末は、前記電子メールの宛先が前記アクセス不可リスト上にあるか否かを判断し、ある場合は前記携帯端末は送信が不可であることを表示した上で本プロセスを中断し、ない場合は表題、本文に含まれる単語に所定のキーワードがあるか否かを検索するステップと、(a6)前記携帯端末は、前記所定のキーワードが含まれている場合は、前記携帯端末は送信不可であることを表示した上で本プロセスを中断し、前記所定のキーワードが含まれていない場合は前記電子メールを送信するステップとを具備する。

10

【0019】

本発明のアクセス制限方法は、(b1)受信した電子メールの宛先、表題、本文をメモリ(1)に保管するステップと、(b2)前記宛先が受信履歴にある宛先か否かについて確認するステップと、(b3)前記宛先が新たな宛先である場合、携帯端末から設定された通知相手に、新たな宛先である旨を通知するステップと、(b4)前記通知相手から前記電子メールの受信可否を示す情報を受信し、受信不可であれば前記電子メールの宛先をアクセス不可リストに登録するステップと、(b5)前記携帯端末は、前記電子メールの宛先が前記アクセス不可リスト上にあるか否かを判断し、ある場合は前記携帯端末は受信が不可であることを表示した上で本プロセスを中断し、ない場合は表題、本文に含まれる単語に所定のキーワードがあるか否かを検索するステップと、(b6)前記携帯端末は、前記所定のキーワードが含まれている場合は、前記携帯端末は受信不可であることを表示した上で本プロセスを中断し、前記所定のキーワードが含まれていない場合は前記電子メールを表示するステップとを具備する。

20

30

【0020】

本発明のアクセス制限方法は、(c1)アクセスしたWebサイトのURL、表題、本文をメモリ(1)に保管するステップと、(c2)前記URLがアクセス履歴にあるURLか否かについて確認するステップと、(c3)前記URLが新たなURLである場合、携帯端末から設定された通知相手に、新たなURLである旨を通知するステップと、(c4)前記通知相手から前記Webサイトのアクセス可否を示す情報をアクセスし、アクセス不可であれば前記WebサイトのURLをアクセス不可リストに登録するステップと、(c5)前記携帯端末は、前記WebサイトのURLが前記アクセス不可リスト上にあるか否かを判断し、ある場合は前記携帯端末はアクセスが不可であることを表示した上で本プロセスを中断し、ない場合は表題、本文に含まれる単語に所定のキーワードがあるか否かを検索するステップと、(c6)前記携帯端末は、前記所定のキーワードが含まれている場合は、前記携帯端末はアクセス不可であることを表示した上で本プロセスを中断し、前記所定のキーワードが含まれていない場合は前記Webサイトを表示するステップとを具備する。

40

【発明の効果】

【0021】

第1の効果は、親などの、子供の携帯端末の契約者となっている第三者が、有害情報へのアクセスをリアルタイムにかつ半自動的に防止できることにある。

第2の効果は、同様に、親などが、有害情報へのアクセスを、子供の成長過程に応じて個別に設定することができることにある。

50

【発明を実施するための最良の形態】

【0022】

以下に本発明の第1実施形態について添付図面を参照して説明する。

図1は、本発明の携帯端末としてのコンテンツを送受信可否判断を制御実行するためのシステム構成を表したものである。図1において、本発明の携帯端末は、メモリ1と、DB2と、判定コントローラ3と、メール送信部4と、メール受信部5と、DB6と、表示コントローラ7を具備する。なお、DBは、データベースを示す。

【0023】

メモリ1は、送受信するコンテンツ内容を一時保管する。DB2は、有害とされるキーワードを保持する。判定コントローラ3は、コンテンツ内容から有害とされるキーワード有無を確認する。メール送信部4は、有害情報へのアクセスがされることを通知する。メール受信部5は、アクセス可否判断を受信する。DB6は、その結果有害と認定された電子メールアドレスとWebサイトのURL(Uniform Resource Locator)を保持する。表示コントローラ7は、有害情報の表示可否を判定する。

【0024】

本発明の携帯端末において、送受信するコンテンツ内容を一時保管するメモリ1は通常送信する電子メールの内容を保管するメモリ作業領域と一時的に共有させる形で確保しても良い。或いは、有害と判断されたメール宛先を保持するDBは携帯端末に通常保持されている電話帳DBに送信可否のフラグなどのプロパティを追加する形で確保しても良い。

【0025】

すなわち、メモリ1は、携帯端末が受信した電子メール又はWebサイトの情報(コンテンツ内容)を格納する。この時、メモリ1は、外部から電子メール又はWebサイトの情報を取得する通信部(図示されず)と接続されている。通信部は、携帯端末が備えている通信用インタフェース、アンテナ、送受信データ変換回路のいずれか又は全てを含む。但し、前述の例に限定されない。なお、メモリ1は、メール受信部5と接続されている場合もある。

【0026】

DB2において保持されるキーワードは、予め登録しておく。或いは、メモリ1が電子メール又はWebサイトの情報を取得した時点で、無条件でメール送信部4を介して該当する電子メールアドレス又はWebサイトのURLを通知対象に通知する。通知に対しメール受信部5で受信したアクセス可否判断にてアクセス拒否されていた場合、当該電子メール又はWebサイトのタイトル(件名)や本文、電子メールアドレス、URLに含まれている所定の単語又は全単語を自動的に抽出し、抽出した単語をキーワードとしてDB2に格納する。単語の抽出は、単語抽出処理のプログラムをCPU(図示されず)が実行することにより実施する。この単語抽出処理は、公知技術、周知技術でも実現可能である。例えば、予想されるキーワードが含まれていたら抽出する。又は、構文を単語に分解して単語を取り出す。なお、所定の単語については、アクセス可否判断と共に受信するようにしても良い。

【0027】

判定コントローラ3は、メモリ1を監視し、メモリ1に何らかのデータが格納された時点で、DB2に保持されているキーワードを参照し、メモリ1に一時保管されているデータに、キーワードに該当する内容が含まれていないか確認する。含まれていたら、メール送信部4に通知を依頼する。

【0028】

メール送信部4が通知を行う対象は、携帯端末の契約者となっている第三者の携帯電話やパソコン、又は、その他電子メールを受信可能な通信端末である。通知を受け取る相手は、基本的に携帯端末の契約者が望ましいが、設定により、他の相手に通知するように変更することも考えられる。なお、通知手段は、電子メールに限らず、ショートメッセージサービス(SMS)、又は、これに準ずる他の通知手段でも良い。また、メール送信部4からの通知により、携帯端末の契約者となっている第三者の通信端末の画面に「OK(ア

10

20

30

40

50

クセス許可)」「NG(アクセス拒否)」を示す選択肢又はボタンを表示するようにしても良い。この場合、「OK(アクセス許可)」又は「NG(アクセス拒否)」を、携帯端末の契約者となっている第三者に選択させ、その選択結果をアクセス可否判断としてメール受信部5が受信する。構造化文書(例えばHTML文書)を用いたメールで通知を行えば実現可能である。

【0029】

また、メール受信部5が受信するアクセス可否判断の他の例として、メール送信部4による通知を受けた者が、通知に対する返信メールにアクセス可否判断を示す情報を記載して送信することが考えられる。或いは、メール送信部4による通知に対してメール受信部5が返信メールを受信した場合、返信メールの内容に関係なくアクセス拒否を示すものと判断するようにする。この場合、返信メールは空メール(件名・本文無しのメール)でも良い。なお、アクセス可否判断の結果、アクセス不可とされた場合、CPU(図示されず)がメモリ1に一時保管されているコンテンツ内容を削除するようにしても良い。

10

【0030】

DB6に格納される電子メールアドレスやWebサイトのURLは、完全な形(全文)でなく、電子メールアドレスやURLの一部を用いることも可能である。例えば、電子メールアドレスのドメイン部分、すなわちアットマーク(@)以降の部分のみ使用する。逆に、アカウント部分、すなわちアットマーク(@)以前の部分を使用しても良い。同様に、URLの場合も、ドメイン部分(例:「http://www. .com/」の「.com/」部分)のみ使用する。又は、アカウント/ディレクトリ部分(例:「http://www. .com/xxx/」の「xxx/」部分)のみ使用する。電子メールアドレスやWebサイトのURLは、特徴的な部分以外は共通している場合も多く、特徴的な部分のデータのみ保持し、他の一般的な部分は無視する。このようにすることで、DB6に保持するデータ量を減少させることが可能である。

20

【0031】

表示コントローラ7は、携帯端末の表示画面を制御する。従って、有害情報の表示可否を判定した後、表示許可の電子メール又はWebサイトを表示画面に表示する。表示不可の電子メール又はWebサイトについては、表示しない。或いは、非表示である旨の表示又はエラー表示を表示する。なお、ここでは、表示許可の電子メール又はWebサイトとは、DB6に保持されているデータに該当しない電子メール又はWebサイトである。逆に、表示不可の電子メール又はWebサイトとは、DB6に保持されているデータに該当する電子メール又はWebサイトである。

30

【0032】

次に、図2のフローチャートを参照して本発明の実施例の動作について詳細に説明する。図2は子供が作成した電子メールの送信制御を行う際に取り上げた、実施例のフローチャートである。

(1)ステップS101

送信しようとするメール、すなわち、作成された電子メールの、宛先、表題、本文をメモリに一時保管する。

(2)ステップS102

作成された電子メールの宛先が、これまでに送信履歴がある宛先か否かについてDB6の登録情報を利用して確認する。

40

(3)ステップS103

新たな宛先である場合は、携帯端末から親又は契約者に電子メールなどを利用して、そのメール内容と一緒にその旨が通知される。

(4)ステップS104

親は携帯端末から送られた情報に基づいて送信可否を判断し、その可否を携帯端末に通知する。通知の方法は、携帯端末が保有する機能に合わせて、電子メールでも、Web連携アプリケーションのような自動化した方法でも、或いは親子で音声通話の上で可否判定を子ども自身が入力する手順方法を取っても良い。

50

(5) ステップ S105

送信不可であれば、この新たな宛先を DB6 にあるアクセス不可リストに追加する。

(6) ステップ S106

その後、携帯端末は、作成された電子メールの宛先が DB6 にあるアクセス不可リスト上にあるか否かを判断する。

(7) ステップ S107

宛先がアクセス不可リスト上にある場合、携帯端末は送信が不可であることを表示した上で本プロセスは中断する。

(8) ステップ S108

宛先がアクセス不可リスト上にない場合は、表題・本文に含まれる単語に DB2 にある有害キーワードがあるか否かを検索する。場合によっては、宛先に含まれる単語に DB2 にある有害キーワードがあるか否かについても検索する。

(9) ステップ S109

有害キーワードが含まれている場合は、携帯端末は送信不可であることを表示した上で本プロセスは中断する。この時、有害情報が含まれるメールである旨の通知と共に、送信内容を親又は契約者に通知するようにしても良い。通知は、電子メール、ショートメッセージサービス (SMS)、その他、携帯電話機やパソコンに対して通常考え得る通知方法のいずれか又は組み合わせにより行う。

(10) ステップ S110

有害キーワードが含まれていない場合は、メールが送信される。

【0033】

有害キーワードの DB2 は、親又は契約者による新規宛先のフィルタリングプロセスと逆の方法で、有害キーワードとして DB2 に登録されているをキーワードを削除したり、他の一般的に行われている日本語変換辞書の更新方法で採用されているような手法でメンテナンスをしても良い。

【0034】

次に、図3のフローチャートを参照して本発明の他の実施例の動作について詳細に説明する。図3は子供の携帯端末に対して送信されてきた電子メールの受信制御を行う際を取り上げた、実施例のフローチャートである。

(1) ステップ S201

受信しようとするメールの、送信元、表題、本文をメモリに一時保管する。

(2) ステップ S202

電子メールの送信元が、これまでに受信履歴がある送信元か否かについて DB6 の登録情報を利用して確認する。

(3) ステップ S203

新たな送信元である場合は、携帯端末から親又は契約者に電子メールなどを利用して、そのメール内容と一緒にその旨が通知される。

(4) ステップ S204

親は携帯端末から送られた情報に基づいて受信可否を判断し、その可否を携帯端末に通知する。通知の方法は、携帯端末が保有する機能に合わせて、電子メールでも、Web 連携アプリケーションのような自動化した方法でも、或いは親子で音声通話の上で可否判定を子ども自身が入力する手順方法を取っても良い。

(5) ステップ S205

受信不可であれば、この新たな送信元を DB6 にあるアクセス不可リストに追加する。

(6) ステップ S206

その後、携帯端末は、受信した電子メールの送信元が DB6 にあるアクセス不可リスト上にあるか否かを判断する。

(7) ステップ S207

送信元がアクセス不可リスト上にある場合、携帯端末は受信が不可であることを表示した上で本プロセスは中断する。

10

20

30

40

50

(8) ステップ S 2 0 8

送信元がアクセス不可リスト上にない場合は、表題・本文に含まれる単語に DB 2 にある有害キーワードがあるか否かを検索する。場合によっては、送信元に含まれる単語に DB 2 にある有害キーワードがあるか否かについても検索する。

(9) ステップ S 2 0 9

有害キーワードが含まれている場合は、携帯端末は受信不可であることを表示した上で本プロセスは中断する。この時、有害情報が含まれるメールである旨の通知と共に、受信内容を親又は契約者に通知するようにしても良い。通知は、電子メール、ショートメッセージサービス (SMS)、その他、携帯電話機やパソコンに対して通常考え得る通知方法のいずれか又は組み合わせにより行う。

10

(1 0) ステップ S 2 1 0

有害キーワードが含まれていない場合は、メールが受信され、携帯端末の画面に表示される。

【 0 0 3 5 】

更に、図 4 のフローチャートを参照して本発明の実施例の動作について詳細に説明する。図 4 は子供がアクセスしようとする Web サイトのアクセス制御を行う際を取り上げた、実施例のフローチャートである。

(1) ステップ S 3 0 1

アクセスしようとする Web サイトの、URL、表題、本文をメモリに一時保管する。

(2) ステップ S 3 0 2

Web サイトの URL が、これまでにアクセス履歴がある URL か否かについて DB 6 の登録情報を利用して確認する。

20

(3) ステップ S 3 0 3

新たな URL である場合は、携帯端末から親又は契約者に電子メールなどを利用して、その Web サイト内容と一緒にその旨が通知される。

(4) ステップ S 3 0 4

親は携帯端末から送られた情報に基づいてアクセス可否を判断し、その可否を携帯端末に通知する。通知の方法は、携帯端末が保有する機能に合わせて、電子メールでも、Web 連携アプリケーションのような自動化した方法でも、或いは親子で音声通話の上で可否判定を子ども自身が入力する手順方法を取っても良い。

30

(5) ステップ S 3 0 5

アクセス不可であれば、この新たな URL を DB 6 にあるアクセス不可リストに追加する。

(6) ステップ S 3 0 6

その後、携帯端末は、アクセスしようとする Web サイトの URL が DB 6 にあるアクセス不可リスト上にあるか否かを判断する。

(7) ステップ S 3 0 7

URL がアクセス不可リスト上にある場合、携帯端末はアクセス不可であることを表示した上で本プロセスは中断する。

(8) ステップ S 3 0 8

URL がアクセス不可リスト上にない場合は、表題・本文に含まれる単語に DB 2 にある有害キーワードがあるか否かを検索する。場合によっては、URL に含まれる単語に DB 2 にある有害キーワードがあるか否かについても検索する。

40

(9) ステップ S 3 0 9

有害キーワードが含まれている場合は、携帯端末はアクセス不可であることを表示した上で本プロセスは中断する。この時、有害情報が含まれる Web サイトである旨の通知と共に、Web サイトの内容又は URL を親又は契約者に通知するようにしても良い。通知は、電子メール、ショートメッセージサービス (SMS)、その他、携帯電話機やパソコンに対して通常考え得る通知方法のいずれか又は組み合わせにより行う。

(1 0) ステップ S 3 1 0

50

有害キーワードが含まれていない場合は、Webサイトにアクセスする。

【0036】

本発明の携帯端末は、図2～図4に示す、電子メールの送信制御、電子メールの受信制御、Webサイトのアクセス制御のうち、少なくとも1つを実施する。基本的には、全て実施することが望ましい。

【0037】

なお、本発明の携帯端末は、子供向けの携帯端末に限らず、社用の携帯端末に使用することも考えられる。例えば、会社が通信事業者（キャリア）と契約した携帯端末を該会社の従業員に持たせる場合、本発明の携帯端末であれば、従業員が有害とされるキーワードを含むコンテンツ内容の送受信を実施することを制限することが可能となる。

10

また、他の実施例として、業務内容に関するキーワードを登録しておけば、従業員が業務内容に関するキーワードを含むコンテンツ内容の送受信を実施した場合、業務内容に関するコンテンツ内容の送受信が行われた旨を第三者（例えば上司・上長）に通知することが可能になる。この時、コンテンツ内容についても共に通知するようにしても良い。これにより、従業員からの報告を待つことなく、従業員が実施した業務内容に関するメールの送受信を会社側が把握することが可能となる。また、意図しない相手に対して業務内容に関するメールの送受信が行われることを防止することが可能になる。

【0038】

以上のように、本発明の携帯端末は、有害とされるキーワード（電子メールアドレスやURLを含む）を保持するDBを有する。また、有害とされるキーワードを端末外から更新する機能を有する。また、送受信するコンテンツ内容から有害とされるキーワード有無を確認する判定コントローラを有する。更に、有害情報の送受信が行われることを、端末外に（事前に）通知する機能を有する。

20

【図面の簡単な説明】

【0039】

【図1】図1は、本発明の構成例を示すブロック図である。

【図2】図2は、電子メールの送信制御のフローチャートである。

【図3】図3は、電子メールの受信制御のフローチャートである。

【図4】図4は、Webサイトのアクセス制御のフローチャートである。

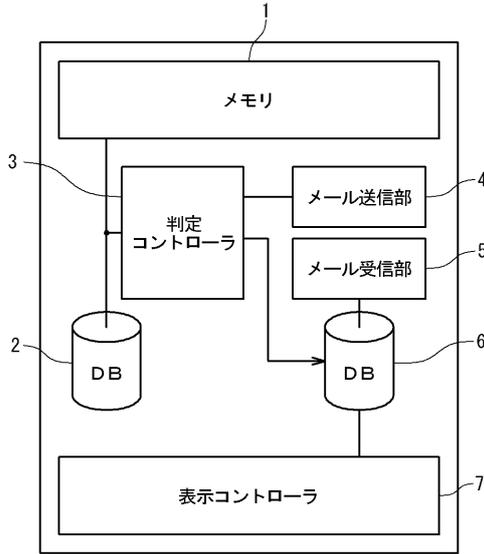
【符号の説明】

30

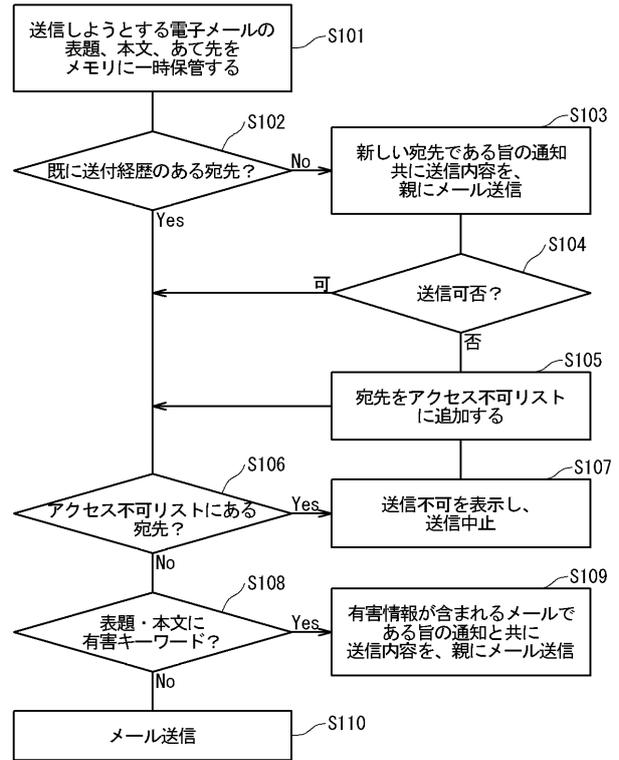
【0040】

- 1 ... メモリ
- 2 ... DB（データベース）
- 3 ... 判定コントローラ
- 4 ... メール送信部
- 5 ... メール受信部
- 6 ... DB（データベース）
- 7 ... 表示コントローラ

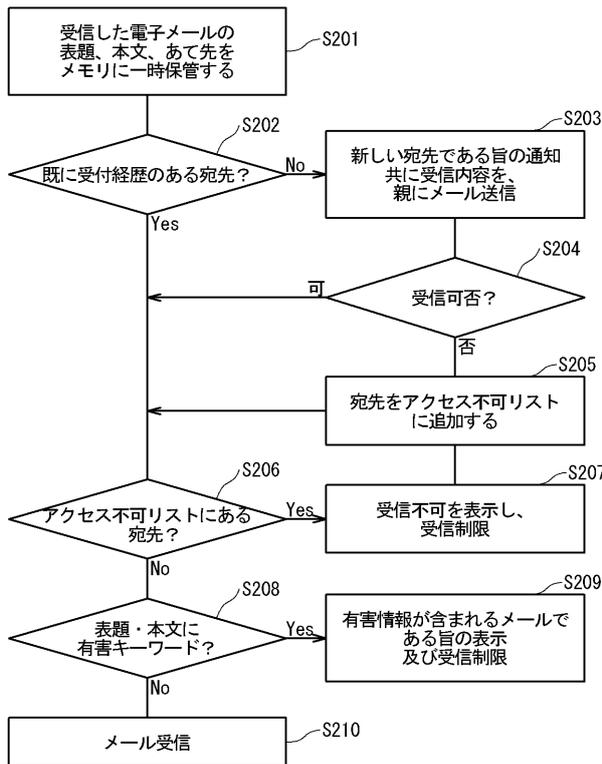
【図1】



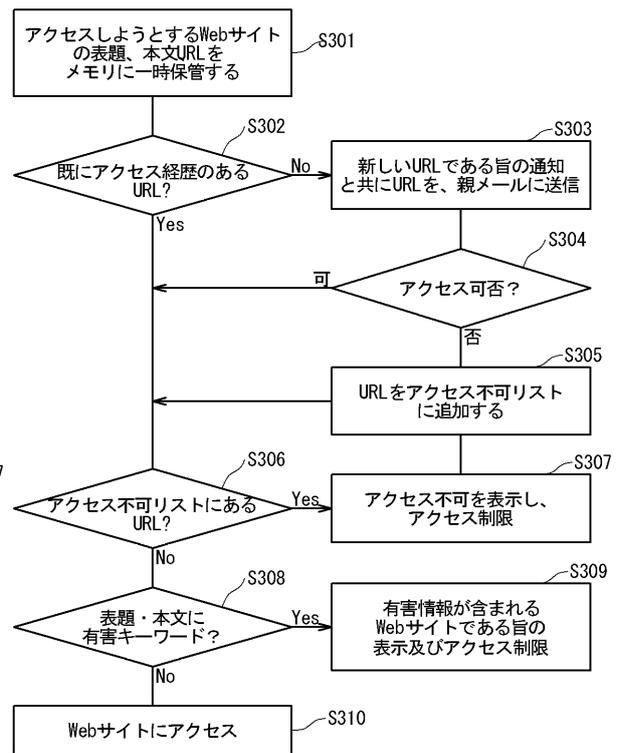
【図2】



【図3】



【図4】



フロントページの続き

(56)参考文献 特開2006-004213(JP,A)
特開2004-227056(JP,A)
特開2003-338879(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F	13/00
G06F	17/30
H04M	1/00