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

特許第5124119号
(P5124119)

(45)発行日　平成25年1月23日(2013.1.23)　(24)登録日　平成24年11月2日(2012.11.2)

(51)Int.Cl.　　F I
G06F 21/44 (2013.01)　　G06F 21/20 144C
H04L 12/66 (2006.01)　　H04L 12/66 B

請求項の数 11　(全 24 頁)

(21)出願番号　特願2006-258144(P2006-258144)
(22)出願日　平成18年9月23日(2006.9.23)
(65)公開番号　特開2008-77524(P2008-77524A)
(43)公開日　平成20年4月3日(2008.4.3)
審査請求日　平成21年9月10日(2009.9.10)

(73)特許権者　501440684
ソフトバンクモバイル株式会社
東京都港区東新橋一丁目９番１号
(74)代理人　100098626
弁理士　黒田　壽
(74)代理人　100128691
弁理士　中村　弘通
(72)発明者　生沼　茂朗
東京都港区東新橋一丁目９番１号　ボーダフォン株式会社内
(72)発明者　長谷川　徹
東京都港区東新橋一丁目９番１号　ボーダフォン株式会社内

最終頁に続く

(54)【発明の名称】通信端末装置、並びに通信端末装置とサーバとの間の通信方法及び通信システム

(57)【特許請求の範囲】
【請求項１】
汎用のコンピュータ装置を用いて構成され公衆の通信ネットワークを介してサーバと通信可能な通信端末装置であって、
前記コンピュータ装置の表示部を露出させるとともに該コンピュータ装置の操作部を覆うケーシング部材を備え、
前記サーバに接続して該サーバを利用するときの前記コンピュータ装置へのログオンに使用される特定のアカウントについて、前記通信ネットワークを介した外部への接続先が前記サーバに制限され、
前記コンピュータ装置の起動処理時に、前記特定のアカウントで自動ログオンされ、該自動ログオン時に該コンピュータ装置の汎用のデスクトップ画面及びメニュー画面に前記サーバの利用に不要なアイコンを表示せず、かつ、該コンピュータ装置に組み込まれている汎用のアプリケーションプログラムについて前記サーバの利用に不要な機能を制限するように設定され、前記通信ネットワークを介して前記サーバに自動接続され、ＰＫＩ認証及びＲＡＤＩＵＳ認証によりデジタル証明書によるクライアント認証及び暗号化通信を利用する仮想的なプライベートネットワークが前記サーバとの間の少なくとも公の通信ネットワーク部分に構築され、前記サーバとの間の仮想的なプライベートネットワーク上で前記サーバのサービスを利用するためのドメインユーザのアカウントが設定されたネットワークドメインが構築されている場合には、前記ドメインユーザのアカウントで自動ログオンされ、前記サーバを利用するときの初期画面が表示されることを特徴とする通信端末装

置。
【請求項２】
請求項１の通信端末装置において、
前記サーバへの接続時に通信が切断された場合には、前記サーバに再接続され、前記仮想的なプライベートネットワークが再構築されることを特徴とする通信端末装置。
【請求項３】
請求項１又は２の通信端末装置において、
複数の移動体通信端末間のデータ転送に使用されるデータ転送装置であることを特徴とする通信端末装置。
【請求項４】
請求項３の通信端末装置において、
当該通信端末装置に接続された移動体通信端末の端末識別番号のデータと該移動体通信端末に保存されている送信先のメールアドレスのデータとを読み出すメールアドレスデータ読み出し手段と、
前記移動体通信端末から読み出した前記端末識別番号のデータを、移動体通信ネットワークを介してメッセージ配信支援サーバに送信する端末識別番号データ送信手段と、
前記メッセージ配信支援サーバから受信したメールアドレスを送信元とし、前記移動体通信端末から読み出した複数のメールアドレスを送信先とし、利用者が指定した配信対象のメッセージをメール本文とした、電子メールのデータを生成する電子メールデータ生成手段と、
前記電子メールのデータを前記メッセージ配信支援サーバに送信する電子メールデータ送信手段と、
前記電子メールのデータを生成した後、前記移動体通信端末から読み出したデータを削除するデータ削除手段と、
を備えたことを特徴とする通信端末装置。
【請求項５】
汎用のコンピュータ装置を用いて構成された複数の通信端末装置と、該複数の通信端末装置と公衆の通信ネットワークを介して通信可能なサーバとを備えた通信システムであって、
各通信端末装置は、
前記コンピュータ装置の表示部を露出させるとともに該コンピュータ装置の操作部を覆うケーシング部材を備え、
前記サーバに接続して該サーバを利用するときの前記コンピュータ装置へのログオンに使用される特定のアカウントについて、前記通信ネットワークを介した外部への接続先が前記サーバに制限され、
前記コンピュータ装置の電源をオンした起動処理時に、前記特定のアカウントで自動ログオンされ、該自動ログオン時に該コンピュータ装置の汎用のデスクトップ画面及びメニュー画面に前記サーバの利用に不要なアイコンを表示せず、かつ、該コンピュータ装置に組み込まれている汎用のアプリケーションプログラムについて前記サーバの利用に不要な機能を制限するように設定され、前記通信ネットワークを介して前記サーバに自動接続され、ＰＫＩ認証及びＲＡＤＩＵＳ認証によりデジタル証明書によるクライアント認証及び暗号化通信を利用する仮想的なプライベートネットワークが前記サーバとの間の少なくとも公の通信ネットワーク部分に構築され、前記サーバとの間の仮想的なプライベートネットワーク上で前記サーバのサービスを利用するためのドメインユーザのアカウントが設定されたネットワークドメインが構築されている場合には、前記ドメインユーザのアカウントで自動ログオンされ、前記サーバに接続してサービスを受けるときの初期画面が表示されることを特徴とする通信システム。
【請求項６】
請求項５の通信システムにおいて、
前記通信端末装置は、複数の移動体通信端末間のデータ転送に使用されるデータ転送装

置であることを特徴とする通信システム。
【請求項７】
請求項６の通信システムにおいて、
前記通信端末装置は、
当該通信端末装置に接続された移動体通信端末の端末識別番号のデータと該移動体通信端末に保存されている送信先のメールアドレスのデータとを読み出すメールアドレスデータ読み出し手段と、
前記移動体通信端末から読み出した前記端末識別番号のデータを、移動体通信ネットワークを介してメッセージ配信支援サーバに送信する端末識別番号データ送信手段と、
前記メッセージ配信支援サーバから受信したメールアドレスを送信元とし、前記移動体通信端末から読み出した複数のメールアドレスを送信先とし、利用者が指定した配信対象のメッセージをメール本文とした、電子メールのデータを生成する電子メールデータ生成手段と、
前記電子メールのデータを前記メッセージ配信支援サーバに送信する電子メールデータ送信手段と、
前記電子メールのデータを生成した後、前記移動体通信端末から読み出したデータを削除するデータ削除手段と、
を備えたことを特徴とする通信システム。
【請求項８】
請求項５、６又は７の通信システムにおいて、
前記通信端末装置のコンピュータ装置に組み込まれている基本ＯＳプログラムの更新情報を取得し、前記基本ＯＳプログラムが更新されたときにその基本ＯＳプログラムの更新プログラムを前記複数の通信端末装置に適用するように一括配信するプログラム更新サーバを備えたことを特徴とする通信システム。
【請求項９】
請求項５、６又は７の通信システムにおいて、
前記通信端末装置から前記サーバを利用するときに使用する新規プログラム又は修正プログラムを前記複数の通信端末装置に一括配信するプログラム管理サーバを備えたことを特徴とする通信システム。
【請求項１０】
請求項５、６又は７の通信システムにおいて、
前記通信端末装置のハードウェア及びソフトウェアに関する情報を前記複数の通信端末装置から収集する端末管理サーバを備えたことを特徴とする通信システム。
【請求項１１】
汎用のコンピュータ装置を用いて構成され前記コンピュータ装置の表示部を露出させるとともに該コンピュータ装置の操作部を覆うケーシング部材を備えた通信端末装置から、公衆の通信ネットワークを介してサーバに接続して該サーバを利用する通信方法であって、
前記サーバに接続して該サーバを利用するときの前記コンピュータ装置へのログオンに使用されるアカウントとして、前記通信ネットワークを介した外部への接続先が前記サーバに制限された特定のアカウントを前記通信端末装置に予め設定しておくステップと、
前記通信端末装置が、前記コンピュータ装置の電源をオンした起動処理時に前記特定のアカウントで自動ログオンされるステップと、
前記自動ログオン時に前記コンピュータ装置の汎用のデスクトップ画面及びメニュー画面に前記サーバの利用に不要なアイコンを表示せず、かつ、該コンピュータ装置に組み込まれている汎用のアプリケーションプログラムについて前記サーバの利用に不要な機能を制限するように設定するステップと、
前記通信端末装置が、前記通信ネットワークを介して前記サーバに自動接続されるステップと、ＰＫＩ認証及びＲＡＤＩＵＳ認証によりデジタル証明書によるクライアント認証及び暗号化通信を利用する仮想的なプライベートネットワークが前記サーバとの間の少な

くとも公の通信ネットワーク部分に構築されるステップと、
前記サーバとの間の仮想的なプライベートネットワーク上で前記サーバのサービスを利用するためのドメインユーザのアカウントが設定されたネットワークドメインが構築されている場合には、前記ドメインユーザのアカウントで自動ログオンされるステップと、
前記起動が完了した前記通信端末装置が、前記サーバに接続して該サーバを利用するときの初期画面を表示するステップと、
を含むことを特徴とする通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、不特定の利用者が操作可能な状態で設置される通信端末装置、並びにかかる通信端末装置とサーバとの間で公衆の通信ネットワークを介した通信を行う通信方法及び通信システムに関するものである。
【背景技術】
【０００２】
従来、この種の通信端末装置として、例えば、携帯電話機の販売店や電化製品の量販店に設置されるデータ転送装置が知られている。このデータ転送装置は、販売店のオペレータや携帯電話機の不特定の利用者によって操作され、携帯電話機から読み出したアドレス帳に保存されているメールアドレス等のデータを、他の携帯電話機に書き出すことにより、２つの携帯電話機間でデータを転送することができる。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
上記販売店や量販店に複数のデータ転送装置を設置した場合、通信ネットワークを介して各データ転送装置とサーバとを接続し、そのサーバで各データ転送装置を管理したり、サーバが提供するサービスを各データ転送装置から利用したりすることが考えられる。
ところが、上記通信端末装置としてのデータ転送装置が汎用のパーソナルコンピュータ（コンピュータ装置）で構成され、不特定の利用者が操作可能な状態で設置されていると、利用者の誤操作や意図的な不正操作によってサーバが不正に利用されたり、一般のネットワークサイトへアクセスされてスパイウェアやワームなどが取り込まれてしまったりすることにより、セキュリティが低下するおそれがある。また、データ転送装置とサーバとの間でインターネットなどの公衆の通信ネットワークを利用する場合には、通信が盗聴されたり通信内容が改ざんされたりすることによりセキュリティが低下するおそれもある。
【０００４】
本発明は以上の問題点に鑑みなされたものであり、その目的は、汎用のコンピュータ装置を用いて構成された通信端末装置が不特定の利用者によって操作可能な状態で設置される場合でも、利用者の利便性を確保しつつ、通信端末装置から公衆の通信ネットワークを介してサーバを利用するときのセキュリティを高めることができる通信端末装置、通信システム及び通信方法を提供することである。
【課題を解決するための手段】
【０００５】
本発明に係る通信端末装置は、汎用のコンピュータ装置を用いて構成され公衆の通信ネットワークを介してサーバと通信可能な通信端末装置であって、前記コンピュータ装置の表示部を露出させるとともに該コンピュータ装置の操作部を覆うケーシング部材を備え、前記サーバに接続して該サーバを利用するときの前記コンピュータ装置へのログオンに使用される特定のアカウントについて、前記通信ネットワークを介した外部への接続先が前記サーバに制限され、前記コンピュータ装置の電源をオンした起動処理時に、前記特定のアカウントで自動ログオンされ、該自動ログオン時に該コンピュータ装置の汎用のデスクトップ画面及びメニュー画面に前記サーバの利用に不要なアイコンを表示せず、かつ、該コンピュータ装置に組み込まれている汎用のアプリケーションプログラムについて前記サ

ーバの利用に不要な機能を制限するように設定され、前記通信ネットワークを介して前記サーバに自動接続され、ＰＫＩ認証及びＲＡＤＩＵＳ認証によりデジタル証明書によるクライアント認証及び暗号化通信を利用する仮想的なプライベートネットワークが前記サーバとの間の少なくとも公の通信ネットワーク部分に構築され、前記サーバとの間の仮想的なプライベートネットワーク上で前記サーバのサービスを利用するためのドメインユーザのアカウントが設定されたネットワークドメインが構築されている場合には、前記ドメインユーザのアカウントで自動ログオンされ、前記サーバを利用するときの初期画面が表示される。

この通信端末装置では、コンピュータ装置の起動を開始すると、その起動処理時に、予め設定された特定のアカウントで自動ログオンされ、通信ネットワークを介してサーバに自動接続されるので、ログオンのためのパスワード入力やサーバへの接続操作が不要になるとともに、そのパスワード入力等を利用者に意識させることがない。しかも、上記自動ログオンした特定のアカウントでは、通信ネットワークを介した外部への接続先が前記サーバに制限されているので、上記自動ログオン後、利用者が前記サーバ以外の外部接続先に通信ネットワークを介して接続するのを制限でき、一般のネットワークサイトへのアクセスを抑止してスパイウェアやワーム等が取り込まれてしまうのを防止できる。更に、前記サーバに接続された後、デジタル証明書によるクライアント認証及び暗号化通信を利用する仮想的なプライベートネットワークがサーバとの間に構築されるので、その仮想的なプライベートネットワークを介して前記サーバと通信できる。また、前記通信端末装置のコンピュータ装置の起動処理が終了すると、前記サーバとの通信を伴うサービスを利用するときの初期画面が表示されるので、初期画面を表示するための利用者の個別操作が不要となる。また、サーバの利用に不要なアイコンに対する利用者の誤操作や意識的な不正操作を防止し、利用者の不正使用を抑止することにより、更にセキュリティを高めることができる。また、汎用のアプリケーションプログラムの機能のうちサーバ利用に不要な機能が利用者の誤操作又は意識的な操作によって利用されるのを回避することにより、更にセキュリティを高めることができる。また、前記プライベートネットワーク上に構築されたネットワークドメインへログオンするための利用者の操作が不要になるとともに、かかるネットワークドメインへのログオン処理を利用者に意識させることもない。

【０００６】

前記通信端末装置において、前記サーバへの接続時に通信が切断された場合には、前記サーバに再接続され、前記仮想的なプライベートネットワークが再構築されるようにしてもよい。この場合には、サーバとの通信切断時におけるサーバへの再接続及び仮想的なプライベートネットワークの再構築のための利用者による操作が不要となるとともに、かかる再接続及び再構築の処理を利用者に意識させることもない。

【０００７】

前記通信端末装置は、複数の移動体通信端末間のデータ転送に使用されるデータ転送装置であってもよい。この場合は、かかるデータ転送装置が汎用のコンピュータ装置を用いて構成され不特定の利用者によって操作可能な状態で設置される場合でも、利用者の利便性を確保しつつ、データ転送装置から公衆の通信ネットワークを介してサーバを利用するときのセキュリティを高めることができる。

特に、この通信端末装置においては、当該通信端末装置に接続された移動体通信端末の端末識別番号のデータと該移動体通信端末に保存されている送信先のメールアドレスのデータとを読み出すメールアドレスデータ読み出し手段と、前記移動体通信端末から読み出した前記端末識別番号のデータを、移動体通信ネットワークを介してメッセージ配信支援サーバに送信する端末識別番号データ送信手段と、前記メッセージ配信支援サーバから受信したメールアドレスを送信元とし、前記移動体通信端末から読み出した複数のメールアドレスを送信先とし、利用者が指定した配信対象のメッセージをメール本文とした、電子メールのデータを生成する電子メールデータ生成手段と、前記電子メールのデータを前記メッセージ配信支援サーバに送信する電子メールデータ送信手段と、前記電子メールのデータを生成した後、前記移動体通信端末から読み出したデータを削除するデータ削除手段

と、を備えてもよい。

この場合は、データ転送装置に接続された移動体通信端末の端末識別番号のデータと移動体通信端末に保存されている送信先のメールアドレスのデータが読み出される。このデータ転送装置が、移動体通信端末から読み出した端末識別番号のデータをメッセージ配信支援サーバに送信すると、メッセージ配信支援サーバは、データ転送装置から受信した端末識別番号に基づいて、前記移動体通信端末の利用者に割り当てられている移動体通信ネットワークの加入者用のメールアドレスを、利用者の最新メールアドレスとして取得し、そのメールアドレスをデータ転送装置に送信する。データ転送装置は、利用者が指定した配信対象のメッセージをメール本文とした電子メールのデータを生成し、その電子メールのデータをメッセージ配信支援サーバに送信する。この電子メールの送信元には、メッセージ配信支援サーバから受信した利用者の最新メールアドレスが設定され、同電子メールの送信先には、前記移動体通信端末から読み出した複数のメールアドレスが設定される。メッセージ配信支援サーバは、データ転送装置から受信した電子メールを、インターネットに公開された移動体通信ネットワークの加入者用の送信メールサーバに送信する。このように利用者の最新メールアドレスと同じドメイン名が登録された送信メールサーバを介して前記電子メールが送信されるので、ドメイン名が異なる送信メールサーバを介して送信されるスパムメール（迷惑メール）として電子メールが拒否されることがない。

しかも、前記配信対象のメッセージを含む電子メールが何らかの理由で配達されなかったときには、その不達通知が前記移動体通信端末の利用者の最新メールアドレス宛に届くので、電子メールの配達状況を利用者が容易に把握できる。また、データ転送装置が、電子メールのデータを作成した後、データ転送装置での処理が終了する前に、移動体通信端末から読み出した個人情報であるメールアドレス等のデータを削除する。従って、かかるメールアドレス等の個人情報を通信ネットーク上のサーバに保存してパソコン等の端末装置からアクセスできるようにした場合とは異なり、個人情報保護の点で優れている。

【０００８】

本発明に係る通信システムは、汎用のコンピュータ装置を用いて構成された複数の通信端末装置と、該複数の通信端末装置と公衆の通信ネットワークを介して通信可能なサーバとを備えた通信システムであって、各通信端末装置は、前記コンピュータ装置の表示部を露出させるとともに該コンピュータ装置の操作部を覆うケーシング部材を備え、前記サーバに接続して該サーバを利用するときの前記コンピュータ装置へのログオンに使用される特定のアカウントについて、前記通信ネットワークを介した外部への接続先が前記サーバに制限され、前記コンピュータ装置の電源をオンした起動処理時に、前記特定のアカウントで自動ログオンされ、該自動ログオン時に該コンピュータ装置の汎用のデスクトップ画面及びメニュー画面に前記サーバの利用に不要なアイコンを表示せず、かつ、該コンピュータ装置に組み込まれている汎用のアプリケーションプログラムについて前記サーバの利用に不要な機能を制限するように設定され、前記通信ネットワークを介して前記サーバに自動接続され、ＰＫＩ認証及びＲＡＤＩＵＳ認証によりデジタル証明書によるクライアント認証及び暗号化通信を利用する仮想的なプライベートネットワークが前記サーバとの間の少なくとも公の通信ネットワーク部分に構築され、前記サーバとの間の仮想的なプライベートネットワーク上で前記サーバのサービスを利用するためのドメインユーザのアカウントが設定されたネットワークドメインが構築されている場合には、前記ドメインユーザのアカウントで自動ログオンされ、前記サーバに接続してサービスを受けるときの初期画面が表示される。

前記通信システムにおいて、前記通信端末装置は、前記サーバへの接続時に通信が切断された場合には、前記サーバに再接続され、前記仮想的なプライベートネットワークが再構築されるように構成してもよい。

前記通信システムにおいて、前記通信端末装置は、複数の移動体通信端末間のデータ転送に使用されるデータ転送装置であってもよい。

前記通信システムにおいて、前記通信端末装置は、当該通信端末装置に接続された移動体通信端末の端末識別番号のデータと該移動体通信端末に保存されている送信先のメール

アドレスのデータとを読み出すメールアドレスデータ読み出し手段と、前記移動体通信端末から読み出した前記端末識別番号のデータを、移動体通信ネットワークを介してメッセージ配信支援サーバに送信する端末識別番号データ送信手段と、前記メッセージ配信支援サーバから受信したメールアドレスを送信元とし、前記移動体通信端末から読み出した複数のメールアドレスを送信先とし、利用者が指定した配信対象のメッセージをメール本文とした、電子メールのデータを生成する電子メールデータ生成手段と、前記電子メールのデータを前記メッセージ配信支援サーバに送信する電子メールデータ送信手段と、前記電子メールのデータを生成した後、前記移動体通信端末から読み出したデータを削除するデータ削除手段と、を備えてもよい。

前記通信システムにおいて、前記通信端末装置のコンピュータ装置に組み込まれている基本ＯＳプログラムの更新情報を取得し、前記基本ＯＳプログラムが更新されたときにその基本ＯＳプログラムの更新プログラムを前記複数の通信端末装置に適用するように一括配信するプログラム更新サーバを備えてもよい。この場合には、各通信端末装置で個別に更新操作を行うことなく、プログラム更新サーバから各通信端末装置に対して基本ＯＳプログラムの更新プログラムを一括配信することにより、各通信端末装置における基本ＯＳプログラムを遠隔的に一括更新することができる。

前記通信システムにおいて、前記通信端末装置から前記サーバを利用するときに使用する新規プログラム又は修正プログラムを前記複数の通信端末装置に一括配信するプログラム管理サーバを備えてもよい。この場合には、各通信端末装置で個別に新規プログラム又は修正プログラムをダウンロードする操作を行うことなく、プログラム管理サーバから各通信端末装置に対して新規プログラム又は修正プログラムを一括配信することにより、各通信端末装置における新規プログラム等のダウンロード及びそのインストールが容易になる。

前記通信システムにおいて、前記通信端末装置のハードウェア及びソフトウェアに関する情報を前記複数の通信端末装置から収集する端末管理サーバを備えてもよい。この場合には、端末管理サーバが各通信端末装置から収集したハードウェア及びソフトウェアに関する情報に基づいて各通信端末装置を一元管理できる。

なお、上記各サーバはそれぞれ個別のコンピュータ装置で構成してもいいし、上記各サーバの機能の少なくとも２以上の機能を合わせ持つように構成されたコンピュータ装置を用いて構成してもよい。

【０００９】

本発明に係る通信方法は、汎用のコンピュータ装置を用いて構成され前記コンピュータ装置の表示部を露出させるとともに該コンピュータ装置の操作部を覆うケーシング部材を備えた通信端末装置から、公衆の通信ネットワークを介してサーバに接続して該サーバを利用する通信方法であって、前記サーバに接続して該サーバを利用するときの前記コンピュータ装置へのログオンに使用されるアカウントとして、前記通信ネットワークを介した外部への接続先が前記サーバに制限された特定のアカウントを設定しておくステップと、前記コンピュータ装置の電源をオンした起動処理時に前記特定のアカウントで自動ログオンされるステップと、前記自動ログオン時に前記コンピュータ装置の汎用のデスクトップ画面及びメニュー画面に前記サーバの利用に不要なアイコンを表示せず、かつ、該コンピュータ装置に組み込まれている汎用のアプリケーションプログラムについて前記サーバの利用に不要な機能を制限するように設定するステップと、前記コンピュータ装置が前記通信ネットワークを介して前記サーバに自動接続されるステップと、ＰＫＩ認証及びＲＡＤＩＵＳ認証によりデジタル証明書によるクライアント認証及び暗号化通信を利用する仮想的なプライベートネットワークが前記サーバとの間の少なくとも公の通信ネットワーク部分に構築されるステップと、前記サーバとの間の仮想的なプライベートネットワーク上で前記サーバのサービスを利用するためのドメインユーザのアカウントが設定されたネットワークドメインが構築されている場合には、前記ドメインユーザのアカウントで自動ログオンされるステップと、前記コンピュータ装置の画面に前記サーバに接続して該サーバを利用するときの初期画面が表示されるステップと、を含む。

前記通信方法において、前記サーバへの接続時に通信が切断された場合には、前記通信端末装置が前記サーバに再接続され、前記仮想的なプライベートネットワークが再構築されるステップを、更に含んでもよい。

前記通信方法において、前記通信端末装置は、複数の移動体通信端末間のデータ転送に使用されるデータ転送装置であってもよい。

前記通信方法において、前記データ転送装置を用いて、移動体通信端末の電子メール送信先の候補として保存されている複数のメールアドレス宛に同じメッセージを一斉に送信してもよい。この通信方法（メッセージ配信方法）は、前記データ転送装置が、そのデータ転送装置に接続された移動体通信端末の端末識別番号のデータと該移動体通信端末に保存されている送信先のメールアドレスのデータとを読み出すステップと、前記データ転送装置が、前記移動体通信端末から読み出した前記端末識別番号のデータを、移動体通信ネットワーク上に設けられたメッセージ配信支援サーバに送信するステップと、前記メッセージ配信支援サーバが、前記データ転送装置から受信した前記端末識別番号に基づいて、前記移動体通信端末の利用者に割り当てられている前記移動体通信ネットワークの加入者用のメールアドレスを取得し、そのメールアドレスを前記データ転送装置に送信するステップと、前記データ転送装置が、前記メッセージ配信支援サーバから受信したメールアドレスを送信元とし、前記移動体通信端末から読み出した複数のメールアドレスを送信先とし、利用者が指定した配信対象のメッセージをメール本文とした電子メールのデータを生成し、その電子メールのデータを前記メッセージ配信支援サーバに送信するステップと、前記メッセージ配信支援サーバが、前記データ転送装置から受信した電子メールを、インターネットに公開された前記移動体通信ネットワークの加入者用の送信メールサーバを介して送信するステップと、前記データ転送装置が、前記電子メールのデータを作成した後、前記移動体通信端末から読み出したデータを削除するステップと、を更に含んでもよい。

前記通信方法において、プログラム更新サーバが、前記通信端末装置のコンピュータ装置に組み込まれている基本ＯＳプログラムの更新情報を取得するステップと、前記プログラム更新サーバが、前記基本ＯＳプログラムが更新されたときにその基本ＯＳプログラムの更新プログラムを前記複数の通信端末装置に適用するように一括配信するステップと、を更に含んでもよい。

前記通信方法において、プログラム管理サーバが、前記通信端末装置から前記サーバを利用するときに使用する新規プログラム又は修正プログラムを前記複数の通信端末装置に一括配信するステップを、更に含んでもよい。

前記通信方法において、プログラム管理サーバが、前記通信端末装置のハードウェア及びソフトウェアに関する情報を前記複数の通信端末装置から収集するステップを更に含んでもよい。

【発明の効果】

【００１０】

本発明によれば、通信端末装置のコンピュータ装置の電源をオンして起動を開始すると、その起動処理時に、予め設定された特定のアカウントで自動ログオンされ、通信ネットワークを介してサーバに自動接続されるので、ログオンのためのパスワード入力やサーバへの接続操作が不要になってセキュリティが高まるとともに、そのパスワード入力等を利用者に意識させることがないので利用者の利便性も高まる。しかも、上記自動ログオンした特定のアカウントでは、通信ネットワークを介した外部への接続先が前記サーバに制限されているので、上記自動ログオン後、利用者が前記サーバ以外の外部接続先に通信ネットワークを介して接続するのを制限でき、一般のネットワークサイトへのアクセスを抑止してスパイウェアやワーム等が取り込まれてしまうのを防止できるので、セキュリティを更に高めることができる。更に、前記サーバに接続された後、デジタル証明書によるクライアント認証及び暗号化通信を利用する仮想的なプライベートネットワークがサーバとの間に構築されるので、その仮想的なプライベートネットワークを介して前記サーバと通信できる。この仮想的なプライベートネットワークを介した通信により、サーバとの通信の

盗聴や通信内容の改ざんの危険性を低減できるので、更にセキュリティを高めることができる。また、前記通信端末装置のコンピュータ装置の起動処理が終了すると、前記サーバとの通信を伴うサービスを利用するときの初期画面が表示されるので、初期画面を表示するための利用者の個別操作が不要となり、利用者の利便性を更に高めることができる。以上により、前記通信端末装置が不特定の利用者によって操作可能な状態で設置される場合でも、利用者の利便性を確保しつつ、その通信端末装置から公衆の通信ネットワークを介してサーバとの通信を伴うサービスを利用するときのセキュリティを高めることができるという効果を奏する。

【発明を実施するための最良の形態】

【００１１】

以下、本発明を複数の携帯電話機（移動体通信端末）間のデータ転送に使用される通信端末装置としてのデータ転送装置、並びにそのデータ転送装置を用いた通信方法及び通信システムに適用した実施形態について説明する。

図１は本実施形態に係る通信システムの全体構成の一例を示す説明図である。この通信システムは、各データ転送装置１０をサーバから管理する管理システムや、各データ転送装置１０に接続されている携帯電話機から読み出した情報に基づいて他の携帯電話機等にメッセージを配信するメッセージ配信システムとしても機能する。図１において、本実施形態の通信システムは、携帯電話機を販売するショップや代理店（以下「ショップ等」という。）６００に設置されたデータ転送装置１０と、電化製品の量販店６１０に設置されたデータ転送装置１０と、通信事業者内の通信ネットワーク（以下「事業者ネットワーク」という。）４００に設けられた各種サーバ４２０、４３０、４６０～４８０、７００～７８０とを用いて構成されている。

【００１２】

上記ショップ等６００のデータ転送装置１０は、例えばショップ・ネットワークを構成している専用回線５００及びルータ４１０、５２０を介して事業者ネットワーク４００に接続され、事業者ネットワーク４００内の各種サーバと通信できる。一方、上記量販店６１０のデータ転送装置１０は、一般公衆回線を利用したインターネット５１０、ルータ５２０及びゲートウェイ装置４２０を介して事業者ネットワーク４００に接続され、事業者ネットワーク４００内の各種サーバと通信できる。ゲートウェイ装置４２０は、アクセス制限及びオペレーション内容の記録といった内部利用者に対する監査を行う監査ゲートウェイとしての機能と、後述のＶＰＮのゲートウェイとしての機能とを有する。なお、量販店６１０のデータ転送装置１０は、リモートアクセスサーバ４３０及び公衆交換電話網５３０を介して事業者ネットワーク４００に接続してもよい。

【００１３】

上記インターネット５１０には、ＯＳ更新情報提供サーバ５４０やウィルス駆除ソフト更新サーバ５５０等が設けられている。ＯＳ更新情報提供サーバ５４０は、各データ転送装置１０に実装されている基本ソフトであるＯＳの更新プログラムを提供する。ウィルス駆除ソフト更新サーバ５５０は、各データ転送装置１０に実装されているウィルス検知・駆除などを行うウィルス駆除ソフトの本体ファイル及び検知用パターンファイルの更新データを提供する。

【００１４】

上記事業者ネットワーク４００は、データ転送装置１０側のルータ４１０、アクセスゲートウェイ装置４２０及びリモートアクセスサーバ４３０に接続されたＩＰ－ＶＰＮ（Virtual Private Network）４４０と、広域イーサネット（Wide-Ethernet）網４５０とを備えている。ＩＰ－ＶＰＮ４４０には、ＲＡＤＩＵＳ（Remote Authentication Dial In User Service）認証サーバ４６０及びＰＫＩ（公開鍵基盤：Public Key Infrastructure）認証サーバ４７０が設けられている。ＲＡＤＩＵＳ認証サーバ４６０は、リモートで接続してきたデータ転送装置１０で入力されたユーザＩＤ（アカウント）とパスワードに基づいて、データ転送装置からＩＰ－ＶＰＮ４４０を利用しようとするユーザについて認証を行うサーバである。ＰＫＩ認証サーバ４７０は、データ転送装置１０に対して事前に配布

されているクライアント証明書に基づいて認証を行うサーバである。ＩＰ－ＶＰＮ４４０と広域イーサネット網４５０とは、ＩＤＳ（侵入検知システム）４８０を間に介して接続されている。ＩＤＳ４８０は、ＩＰ－ＶＰＮ４４０と広域イーサネット網４５０との間の通信回線を監視し、不正侵入を管理者に通知する。

【００１５】

上記広域イーサネット網４５０には、ドメインサーバ７００、ウィルス駆除ソフト管理サーバ７１０、ＷＳＵＳ（Windows Server Update Service）サーバ７２０、資産管理サーバ７３０、プログラム配信サーバ７４０が接続されている。また、必要に応じて、メンテナンスサーバ７５０を設けてもよい。

【００１６】

上記ドメインサーバ７００は、通信ネットワークを介して接続してくる各データ転送装置１０を含むように構築されたWindows（登録商標）のドメインを管理する。各データ転送装置１０には、ドメインへのログオンに使用されるユーザアカウントが割り当てられている。このユーザアカウントが所属するグループに対するWindows標準のグループポリシーにより、各データ転送装置１０におけるWindows系ＯＳ上の各種機能を一括して設定することができる。この一括設定により、Windows系ＯＳ上の各種機能のうち、データ転送装置１０で使用する機能以外の不要な機能やセキュリティ上好ましくない機能を使用不可にすることができる。

【００１７】

上記ウィルス駆除ソフト管理サーバ７１０は、各データ転送装置１０にインストールされているウィルス駆除ソフトウェアの更新ファイル（例えば、プログラム本体の更新ファイルやパターン更新ファイル）を、予め設定されたスケジューリングにより、インターネット５１０上のウィルス駆除ソフト更新サーバ５５０から取得する。なお、このときの更新ファイルの取得は、図示しないネットワーク接続（例えば、インターネットを介した接続）によっても行うことができる。各データ転送装置１０にインストールされているウィルス駆除ソフトウェアは、コンピュータウィルス、スパイウェア、不正侵入、ネットワークウィルス等に検知・削除などに対応できる機能のほか、ネットワークを介した外部との複数種類の通信を個別に許可したり禁止したりすることができるファイアウォール機能を有する。この種のウィルス駆除ソフトウェアとしては、例えばトレンドマイクロ株式会社製の「ウイルスバスター コーポレートエディション アドバンス」を使用することができる。ウィルス駆除ソフト管理サーバ７１０は、予め設定されたスケジューリングにより、上記ウィルス駆除ソフト更新サーバ５５０から取得された更新ファイルを各データ転送装置１０に配信する。各データ転送装置１０は、ウィルス駆除ソフト管理サーバ７１０から配信された更新ファイルを受信すると、その更新ファイルをインストール済みのウィルス駆除ソフトウェアに適用する。

【００１８】

上記ＷＳＵＳサーバ７２０は、各データ転送装置１０にインストールされているＯＳ（例えば、Windows系のＯＳ）のセキュリティ関連の更新プログラムを、予め設定されたスケジューリングにより、インターネット５１０上のＯＳ更新情報提供サーバ５４０から取得する。特に、外部からの攻撃などに対応した更新プログラム（例えば、Windows系のＯＳの場合、「重要な更新」として提供されている更新プログラム）について取得する。なお、このときの更新プログラムの取得は、図示しないネットワーク接続（例えば、インターネットを介した接続）によっても行うことができる。このＯＳ更新情報提供サーバ５４０から取得された更新プログラムは、運用管理者により、試験環境で実装アプリケーションに影響が出ないことを確認するためのテストが実行される。このテストの結果、問題がない場合は、各データ転送装置１０に対して「更新プログラム」の適用が指示される。ＷＳＵＳサーバ７２０は、予め設定されたスケジューリングにより、上記適用指示された「更新プログラム」を各データ転送装置１０に配信する。各データ転送装置１０は、ＷＳＵＳサーバ７２０から配信された更新プログラムを受信すると、その更新プログラムをインストールする。

【００１９】
上記資産管理サーバ７３０及びプログラム配信サーバ７４０は、各データ転送装置１０に実装されているドライバ及びアプリケーションのプログラムの保守管理を行う。この資産管理サーバ７３０用のソフトウェアとしては、例えばクオリティ株式会社製の「QND Plus Ver9.1」という市販ソフトを用いることができる。
【００２０】
上記資産管理サーバ７３０は、予め設定されたスケジューリングにより、「インベントリ一括収集」や「プログラム一括配信」等のタスクを実行する。上記「インベントリ一括収集」は、各データ転送装置１０に予め実装されている専用エージェントソフトと協働し、各データ転送装置１０のハードウェア及びソフトウェアの情報を収集するタスクである。例えば、資産管理サーバ７３０からデータ転送装置１０にインベントリ収集のタスク起動のコマンドが送信されると、データ転送装置１０に実装されているエージェントソフトがインベントリを収集して資産管理サーバ７３０に送信する。このタスクで収集されたインベントリにより、各データ転送装置１０のレジストリ設定情報やセキュリティ情報等の一元管理が可能になる。また、上記「プログラム一括配信」は、各データ転送装置１０に予め実装されている専用エージェントソフトと協働し、新規発売された携帯電話機に対応するドライバプログラムや、新規に開始されたサービス仕様に合わせて追加・変更などがなされたアプリケーションプログラムを、プログラム配信サーバ７４０からダウンロードさせて各データ転送装置１０に自動インストールさせるタスクである。例えば、資産管理サーバ７３０からデータ転送装置１０にプログラム一括配信のタスク起動のコマンドが送信されると、データ転送装置１０に実装されているエージェントソフトがプログラム配信サーバ７４０にアクセスし、指定されたドライバやアプリケーションのプログラムをダウンロードする。エージェントソフトは、ダウンロードしたプログラムをデータ転送装置１０に新規にインストールしたり、ダウンロードしたプログラムで更新したりする。
上記プログラム配信サーバ７４０は、各データ転送装置１０のエージェントソフトからの取得要求に応じて、指定されたドライバやアプリケーションのプログラムを各データ転送装置１０に送信する。
【００２１】
各データ転送装置１０は、携帯電話データ転送、電子メール送信などの利用状況を操作ログとして作成できる。各データ転送装置１０は、操作ログのファイルをメンテナンスサーバ７５０へＦＴＰによる通信によるファイル転送を行う。なお、当該ファイルは３ＤＥＳ等による暗号化によりセキュリティを保つことができる。
【００２２】
また、事業者ネットワーク４００には、上記サーバ７００～７５０のほか、メッセージ配信支援サーバ７６０、インターネット用の送信メールサーバ７７０及び加入者情報管理サーバ７８０が設けられている。
【００２３】
上記メッセージ配信支援サーバ７６０は、専用回線５００やインターネット５１０等の通信回線やルータ５２０などを介して、ショップ等６００や量販店６１０で使用されているデータ転送装置１０と通信することができる。メッセージ配信支援サーバ７６０は、ＷＥＢサーバとしての機能と、送信メールサーバとしての機能とを備えている。メッセージ配信支援サーバ７６０とデータ転送装置１０との間のアプリケーション層の通信プロトコルとしては、ＷＥＢサーバとして機能する場合にＨＴＴＰ（Hyper Text Transfer Protocol）が用いられ、送信メールサーバとして機能する場合にＳＭＴＰ（Simple Mail Transfer Protocol）が用いられる。ＷＥＢサーバとして機能する場合には、よりセキュリティを高めるために、上記ＨＴＴＰに代えてＨＴＴＰＳ（Hyper Text Transfer Protocol over SSL）を用いてもよい。
【００２４】
上記メッセージ配信支援サーバ７６０は、そのコンピュータ装置に所定のプログラムを読み込んで実行することにより、メールアドレス取得手段、メールアドレス送信手段及び

電子メール送信手段として機能する。上記メールアドレス取得手段は、データ転送装置１０から受信した電話番号（端末識別番号）に基づいて、携帯電話機の利用者に割り当てられている携帯電話通信網の加入者用のメールアドレスを取得する。上記メールアドレス送信手段は、前記取得したメールアドレスをデータ転送装置１０に送信する。上記電子メール送信手段は、データ転送装置１０から受信した電子メールを、インターネットに公開された加入者用の送信メールサーバ７７０を介して送信する。

【００２５】

上記送信メールサーバ７７０は、メッセージ配信支援サーバ７６０等から受けた送信対象の電子メールを外部のインターネット５１０にあるメールサーバに転送するものであり、ＭＴＡ（Message Transfer Agent）サーバやＳＭＴＰサーバとも呼ばれる。この送信メールサーバ７７０で電子メールが送受信されるときのプロトコルとしてはＳＭＴＰが使用される。また、送信メールサーバ７７０には、インターネット上で一意に識別可能な固定のグローバルＩＰアドレスが設定されている。このグローバルＩＰアドレスに対応付けて、携帯電話通信網の加入者用のメールアドレスと同じドメイン名を有するＳＭＴＰサーバアドレスが登録されている。これにより、送信メールサーバ７７０を介して送信される電子メールが、いわゆるなりすましメールとして処理されることもないので、本実施形態における変更通知メッセージを含む電子メールは、真の送信者からの電子メールとして各宛先のメールアドレスに届く。

【００２６】

上記加入者情報管理サーバ７８０は、携帯電話通信網の加入者（利用者）の情報を管理するＣＵＲ（Common User Repository）サーバであり、各加入者について、加入者ＩＤ、携帯電話機の電話番号（端末識別番号）、メールアドレス等が保存されたデータベースを備えている。この加入者情報管理サーバ７８０は、上記メッセージ配信支援サーバ７６０から、例えば携帯電話機の電話番号に基づきメールアドレスを要求する取得要求を受信すると、その電話番号に対応するメールアドレス、すなわちその電話番号の携帯電話機の利用者が使用する携帯電話通信網の加入者用のメールアドレスを、メッセージ配信支援サーバ７６０に返信する。この加入者情報管理サーバ７８０とメッセージ配信支援サーバ７６０との間のプロトコルとしては、例えばＬＤＡＰ（Lightweight Directory Access Protocol）が使用される。

【００２７】

なお、上記複数のサーバ７００～７８０はそれぞれ、１台のコンピュータ装置で構成してもいいし、複数のコンピュータ装置をネットワーク接続して協働して動作するように構成してもよい。また、複数のサーバ７００～７８０の２以上を１台のコンピュータ装置で構成してもよい。

【００２８】

図２はデータ転送装置１０の斜視図である。本実施形態のデータ転送装置１０は、電子計算機であるノートブック型のコンピュータ装置（以下、「ノートパソコン」という。）２０と、そのノートパソコン２０の操作部に装着するアダプター３０とを備えている。アダプター３０は、ケーシング部材３１０と、そのケーシング部材３１０の内部に設けた接続ケーブル分岐部とを備えている。ノートパソコン２０は、所定のＯＳプログラムやアプリケーションプログラムがインストールされて実行されることにより、データ転送処理時の各種制御を行う制御手段として用いられる。

【００２９】

データ転送装置１０のノートパソコン２０は、電話番号・メールアドレスの変更通知処理を行うときには、メールアドレスデータ読み出し手段と、端末識別番号データ送信手段と、電子メールデータ生成手段と、電子メールデータ送信手段と、データ削除手段として機能する。上記メールアドレスデータ読み出し手段は、データ転送装置１０に接続された図４に示す携帯電話機４０Ａ，４０Ｂの電話番号（端末識別番号）のデータと旧携帯電話機４０Ａに保存されているメールアドレスのデータとを読み出す。上記端末識別番号データ送信手段は新携帯電話機４０Ｂから読み出した電話番号のデータを、携帯電話通信網を

介してメッセージ配信支援サーバ７６０に送信する。上記電子メールデータ生成手段は、メッセージ配信支援サーバ７６０から受信したメールアドレスを送信元（Ｆｒｏｍアドレス）とし、旧携帯電話機４０Ａから読み出した複数のメールアドレスを送信先とし、利用者が指定した配信対象のメッセージ（変更通知メッセージ）をメール本文とした、電子メールのデータを生成する。上記電子メールデータ送信手段は、前記電子メールのデータをメッセージ配信支援サーバ７６０に送信する。上記データ削除手段は、電子メールのデータを生成した後、旧携帯電話機４０Ａから読み出したデータを削除する。

【００３０】

上記ケーシング部材３１０は、ノートパソコン２０の表示部２１０を露出させるとともに操作部２２０（図３参照）を覆うように設けられている。また、ノートパソコン２０の操作部２２０の上面部には、各種キーからなるキーボード部２２１やポインティングデバイス２２２等が設けられている。さらに、このノートパソコン２０の例では、操作部２２０と表示部２１０とを接合するヒンジ部にほど近い操作部の上面に、電源スイッチ部２２３を備えている。ケーシング部材３１０は、上ケース３２０及び下ケース３３０を組み合わせて構成されている。上記接続ケーブル分岐部は、下ケース３３０の内部に設けてあり、ノートパソコン２０の操作部２２０の外部接続インターフェースに接続された接続ケーブルを複数に分岐するものである。ノートパソコン２０と接続ケーブル分岐部とは、接続インターフェースを介してケーブルやアタッチメントコネクタ等により接続され、利用者がいたずらに触れないよう、正面からは視認できない位置に配置されている。複数の接続ケーブル５０は、下ケース３３０の正面側板３３０Ａに形成されているケーブル通過孔３３１を通って外側に出すことができる。各接続ケーブル５０の先端部には、外部接続インターフェースが異なる各種の携帯電話機４０に対応させて専用のコネクタ５１が取り付けられている。例えば、ＰＤＣ（Personal Digital Cellular）携帯電話機のシリアル端子用のコネクタ、ＰＤＣ携帯電話機のＵＳＢ（Universal Serial Bus）端子用のコネクタ、第３世代携帯電話機の端子用のコネクタ等が取り付けられている。更に、メーカ独自仕様の端子を有する携帯電話機に対応するコネクタも取り付けられている。なお、これらコネクタは、装置の設置後に増減設がいつでもできるよう、接続ケーブル分岐部とは汎用のコネクタで接続されるとともに、ケーブル通過孔３３１は複数設けられている。

【００３１】

上記各コネクタ５１の表面には、そのコネクタに接続可能な携帯電話機の種類を示す端末識別記号と、コネクタの上下（表裏）を識別するための上下識別記号（例えば、おもてに対して「Ａ」，裏に対して「Ｂ」）とが付されている。

【００３２】

また、下ケース３３０の正面側板３３０Ａには、各種のメモリカード６０を装着できるように複数のメモリカードスロット３３２が設けられている。このメモリカード６０には、携帯電話機４０から読み出したデータを保存したり、携帯電話機４０へ書き込むコピー対象のデータを保存しておいたりすることができる。

【００３３】

また、データ転送装置１０のノートパソコン２０はＬＡＮ接続用の端子を有し、ＬＡＮケーブルを介して店舗６００内にあるインターネット接続用のルータに接続されている。

【００３４】

図４は、上記構成のデータ転送装置１０を使用している様子を示す斜視図である。例えば古い携帯電話機４０Ａから新しい携帯電話機４０Ｂにメモリダイヤル等のデータを転送するときには、データ転送装置１０の２つの載置部３２２上にそれぞれ、新旧の携帯電話機４０Ａ，４０Ｂをそれぞれ載置する。そして、まず、図４に示すようにデータ転送元の旧携帯電話機４０Ａに所定の接続ケーブル５０Ａを接続する。この状態で、所定のデータ転送用ソフトウェアを起動し、初期設定、機種選択、ケーブル選択、認証処理などを実行した後、旧携帯電話機４０Ａから転送対象のメモリダイヤルなどのデータをノートパソコン２０内のメモリに一旦読み出して保存する。次に、図５に示すように、旧携帯電話機４０Ａから接続ケーブル５０Ａを外し、データ転送先の新携帯電話機４０Ｂに所定の接続ケ

ーブル５０Ｂを接続する。この状態で、ノートパソコン２０内のメモリに保存していた転送対象のデータを新携帯電話機４０Ｂに書き込む。

【００３５】

上記構成のデータ転送装置１０を不特定のユーザに操作可能な環境である量販店に設置した場合、利用者の誤操作や意図的な不正操作によってサーバが不正に利用されたり、一般のネットワークサイトへアクセスされてスパイウェアやワームなどが取り込まれてしまったりすることにより、セキュリティが低下するおそれがある。また、データ転送装置とサーバとの間でインターネットなどの公衆の通信ネットワークを利用する場合には、通信が盗聴されたり通信内容が改ざんされたりすることによりセキュリティが低下するおそれもある。

特に、上記量販店等の不特定のユーザに操作可能な場所に設置されている多数のデータ転送装置１０に対し、そのデータ転送装置１０で使用されるアプリケーションプログラムのパッチやバージョンアップ版を上記プログラム配信サーバ等から安全に一括配布する場合、データ転送装置１０とプログラム配信サーバ等との間の通信のセキュリティを確保する必要がある。ウィルス駆除ソフト管理サーバ７１０から多数のデータ転送装置１０にウィルス駆除ソフトウェアの更新ファイルを配信する場合や、ＷＳＵＳサーバ７２０から多数のデータ転送装置１０にＯＳ関係のセキュリティ関連の更新プログラムを安全に一括配信する場合も、同様にデータ転送装置１０と各サーバ７１０、７２０との間の通信のセキュリティを確保する必要がある。

そこで、本実施形態では、不特定のユーザに操作可能な環境下にある各量販店６１０に設置されたデータ転送装置１０と事業者ネットワーク４００側のサーバ群との通信のセキュリティを高めるべく、各データ転送装置１０のノートパソコン２０を電源オンするときの処理を以下のように実行している。

【００３６】

図６は、量販店６１０に設置されたデータ転送装置１０のノートパソコン２０を電源オンしたときのノートパソコン２０と事業者ネットワーク４００上のサーバとの間の通信処理の一例を示す説明図である。図７は、そのノートパソコン２０の電源オンから事業者ネットワーク４００上のサーバとのＶＰＮ通信が可能になるまでの手順の一例を示すフローチャートである。なお、図６及び図７の例では、データ転送装置１０のノートパソコン２０から事業者ネットワーク４００にインターネット５１０を介して接続する場合について示している。

【００３７】

上記量販店６１０に設置されたデータ転送装置１０のノートパソコン２０の電源がオンされる（図７のＳ１）と、ノートパソコン２０に実装されているWindows系ＯＳ（例えば、Windows2000（登録商標）やWindowsXP（登録商標））が起動し（図７のＳ２）、ローカルパソコンであるノートパソコン２０へのWindowsログオンが、予め設定した特定のアカウントによるキャッシュログオンによって自動実行される（図７のＳ３）。このキャッシュログオンに使用されるアカウントは、上記事業者ネットワーク４００上のサーバ群７００～７８０との通信が可能なユーザのために予め設定されたWindowsのユーザグループに属している。このユーザグループには、サーバ群７００～７８０との通信を伴う特定の業務以外にノートパソコン２０が使用されないように、Windowsグループポリシーによる各種設定が予めなされている。このWindowsグループポリシーによる設定は、例えば次の（１）～（３）に示すデスクトップ画面、スタートメニュー、ブラウザソフト（Internet Explorer）の設定である。

（１）ノートパソコン２０の目的外使用を阻止するために、デスクトップ画面上に不要なアイコンを表示しない。

（２）ノートパソコン２０の目的外使用を阻止するために、スタートメニューのプログラムに不要なアプリケーションを表示しない。スタートメニューのプログラムにはＶＰＮのみ表示されている。コントロールパネル、ファイル名を指定して実行等のwindows機能をアクティブにするアイコンメニューは表示されない。

（３）Windowsファイルシステムへの不正侵入やアプリケーションの改ざん等を防止するために、ブラウザソフト（Internet Explorer）における次のＡ～Ｅのサブメニューを非活性にする。
Ａ．「編集」メニューにある「切り取り」、「コピー」及び「貼り付け」
Ｂ．「表示」メニューにある「ソース」
Ｃ．「表示」－「ツールバー」メニューにある「標準のボタン」、「アドレスバー」及び「リンク」
Ｄ．「表示」－「エクスプローラバー」メニューにある「お気に入り」
Ｅ．windowsタスクバーの右クリックで表示されるエクスプローラ

【００３８】
次に、データ転送装置１０のノートパソコン２０では、上記Windowsグループポリシーに基づいて、デスクトップ画面やスタートメニュー等の初期設定が自動実行される（図７のＳ４）。また、ノートパソコン２０では前述のウィルス駆除ソフトウェアも自動で起動される。このウィルス駆除ソフトウェアのファイアウォール機能により、外部ネットワークへの接続として、下記ＶＰＮによる事業者ネットワーク４００への接続のみが許可され、目的外使用のための外部への不正接続を防止している。

【００３９】
次に、データ転送装置１０のノートパソコン２０では、事業者ネットワーク４００との間で仮想的なプライベートネットワークであるＶＰＮを構築するためのＶＰＮ起動処理が自動実行される（図７のＳ５）。ＶＰＮにより、インターネットを介する場合でも、専用線に匹敵する閉域環境を構築することができる。このＶＰＮには、ネットワーク層で動作してＩＰパケットの暗号化と認証を行う、ＴＣＰ／ＩＰ環境で汎用的に用いることができるＩＰｓｅｃ（IP Security）と呼ばれるセキュリティ技術が用いられている。

【００４０】
上記ＶＰＮの構築の際に、ＰＫＩ認証及びＲＡＤＩＵＳ認証が自動実行される（図７のＳ６，Ｓ７）。ＰＫＩ認証で使用するクライアント証明書は、各データ転送装置のノートパソコン２０について予め発行され、それぞれ対応するノートパソコン２０内に保存されている。上記ＰＫＩ認証では、ノートパソコン２０内に保存されているクライアント証明書に基づいて、ノートパソコン２０が正規のクライアントであることを認証する。認証に失敗すると、上記ＶＰＮが構築されず、事業者ネットワーク４００内のサーバ群と通信できない。上記ＲＡＤＩＵＳ認証では、ノートパソコン２０で自動入力されたユーザＩＤ（アカウント）とパスワードに基づいて、ノートパソコン２０が正規のクライアントであることを認証する。この場合も、認証に失敗すると、上記ＶＰＮが構築されず、事業者ネットワーク４００内のサーバ群と通信できない。

【００４１】
上記ＰＫＩ認証及びＲＡＤＩＵＳ認証に成功してＶＰＮの構築が完了すると、ＶＰＮを介してデータ転送装置のノートパソコン２０と事業者ネットワーク４００上のサーバ群との間でＩＰｓｅｃによる通信が開始される（図７のＳ８）。そして、ドメインのログオン画面で、予め登録されている所定のドメインユーザのアカウント及びパスワードが自動入力されることによりドメイン認証が自動実行されるとともに、上記サーバ群との通信を利用してサービスを受けるための所定のアプリケーションの初期画面が表示される（図７のＳ９）。後述の例では、メッセージ配信支援サーバ７６０との通信を伴うメッセージ配信サービスの初期画面が表示される。この後、ユーザは上記アプリケーションによる各種サービスを利用することができる（図７のＳ１０）。サービスの利用が終了すると、ＩＰｓｅｃによる通信が終了し、ＶＰＮ接続が切断される（図７のＳ１１）。

【００４２】
なお、上記サービスの利用中に何らかの理由でＶＰＮ接続が切断した場合は、ユーザが操作しなくても、前述のＶＰＮ起動並びにＰＫＩ認証及びＲＡＤＩＵＳ認証が自動実行され、ＶＰＮが再構築される。

【００４３】

以上のように、ユーザに意識させないで、データ転送装置１０のノートパソコン２０の電源をＯＮしてから上記ドメイン認証及び初期画面の表示までの処理が自動実行されるので、上記ノートパソコン２０の起動操作を簡略化できるだけでなく、ユーザの誤操作や意図的な不正使用を抑止することができる。

【００４４】

図８は、上記構成の通信システムにおいて、データ転送装置１０のノートパソコン２０と事業者ネットワーク４００上のメッセージ配信支援サーバ７６０とが通信可能になった後、メッセージ配信支援サーバ７６０との通信を伴うサービスを利用するときの処理の流れの一例を示すシーケンス図である。この処理は、旧携帯電話機４０Ａから新携帯電話機４０Ｂへ転送したメモリダイヤルの複数のメールアドレス宛に所望のメッセージを含む電子メールを一斉に送信する処理である。まず、前述のように旧携帯電話機４０Ａをケーブル５０Ａに接続する。この状態で、旧携帯電話機４０Ａから転送対象のメモリダイヤルなどのデータがノートパソコン２０内のメモリに一旦読み出されて保存される（Ｓ１）。次に、利用者は、ノートパソコン２０に表示されたメニュー上で、利用者の新携帯電話機４０Ｂの電話番号及びメールアドレスを電子メールで通知する「番号・アドレス変更通知」を選択する（Ｓ２）。なお、「番号・アドレス変更通知」の選択は、旧携帯電話機４０Ａからのデータ読み出し前に行ってもよい。

【００４５】

次に、旧携帯電話機４０Ａから接続ケーブル５０Ａを外すとともに、新携帯電話機４０Ｂに接続ケーブル５０Ｂを接続する。この状態で、ノートパソコン２０内のメモリに保存していた転送対象のデータが新携帯電話機４０Ｂに書き込まれる（Ｓ３）。そして、新携帯電話機４０Ｂに保存されている携帯電話機４０Ｂの電話番号が、ノートパソコン２０内のメモリに一旦読み出されて保存される（Ｓ４）。

【００４６】

次に、データ転送装置１０のノートパソコン２０は、新携帯電話機４０Ｂへのデータ書き込みを開始したら、新携帯電話機４０Ｂの電話番号とともに、その電話番号に対応するメールアドレスを問い合わせるメールアドレス問い合わせをメッセージ配信支援サーバ７６０に送信する。このメールアドレス問い合わせの送信には、セキュリティを担保するためにＨＴＴＰＳによる暗号化通信を用いてもよい。

【００４７】

メッセージ配信支援サーバ７６０は、データ転送装置１０から受信したメールアドレス問い合わせに基づき、電話番号に対応するメールアドレスを、加入者情報管理サーバ７８０に問い合わせて取得する。このメールアドレスの問い合わせには、ＬＤＡＰの通信プロトコルが使用される。メッセージ配信支援サーバ７６０は、加入者情報管理サーバ７８０から取得したメールアドレスを、データ転送装置１０のノートパソコン２０にＨＴＴＰで転送する。

【００４８】

なお、上記新携帯電話機４０Ｂの電話番号に対応するメールアドレスの問い合わせは、新携帯電話機４０Ｂへのデータ書き込み処理中以外のタイミングで行うことができる。このメールアドレスの問い合わせは、新携帯電話機４０Ｂの電話番号を取得した後であって、変更通知メッセージの電子メールの作成前であれば、任意のタイミングで行うことができる。

【００４９】

次に、データ転送装置１０のノートパソコン２０は、メッセージ配信支援サーバ７６０から受信したメールアドレスを電話番号とともに画面に表示する。この表示により、利用者は、電子メールで配信する変更通知メッセージに含まれる電話番号とメールアドレスの内容を確認できる。

【００５０】

次に、利用者は、データ転送装置１０のノートパソコン２０を操作し、電子メールの送信テンプレートのリストを表示し、そのリストから、希望の送信テンプレートを選択し（

Ｓ５）、利用者の氏名、電話番号及び自分の最新メールアドレスを、メール本文の所定位置に記載するように、通知メッセージの内容を設定する（Ｓ６）。さらに、利用者は、旧携帯電話機４０Ａから読み出して画面に表示された複数のメールアドレスから、メッセージの一斉送信の対象にする送信先のメールアドレスを選択し、送信リストを作成する（Ｓ７）。この送信先のメールアドレスの選択は、送信先から外すメールアドレスを指定することによって行ってもよい。

【００５１】

次に、データ転送装置１０のノートパソコン２０は、利用者が選択した複数のメールアドレスを送信先とした電子メールのデータを生成する。本実施形態では、所定件数（例えば１００件）までのメールアドレスを送信先として１通の電子メールのデータを生成することができる。この電子メールのメール本文に、上記設定した通知メッセージの内容が埋め込まれ、送信元のメールアドレス（Ｆｒｏｍアドレス）には、加入者情報管理サーバ７８０から取得した利用者の最新メールアドレスが設定される。なお、この最新メールアドレスとしては、ドメイン名の部分だけが変更になり「@」マークよりも前の部分をそれまで使用していた変更前のメールアドレスと同じものを設定する場合が多い。このような場合は、送信元のメールアドレス（Ｆｒｏｍアドレス）に各利用者共通のシステムのメールアドレスを設定する場合に比して、変更通知メールを受信した受信者が、その変更通知メールを不審なメールと勘違いして削除してしまう危険性が少ない。

【００５２】

次に、データ転送装置１０のノートパソコン２０は、番号・アドレス変更通知送信を確認する操作を受け付ける（Ｓ８）と、上記生成された電子メールをメッセージ配信支援サーバ７６０に送信される。メッセージ配信支援サーバ７６０は、送信メールサーバ７７０における規約に則り、データ転送装置１０から受信した複数宛先が設定された１通の電子メールを、１宛先（メールアドレス）１通の電子メールに分解する処理を行い、各送信先のメールアドレスごとに個別の電子メールのデータを生成する（Ｓ９）。このように生成された複数の電子メールは、メッセージ配信支援サーバ７６０におけるメール送信待ちのキューにスタックされる。その後、メッセージ配信支援サーバ７６０は、予め設定されているスケジューラにより、上記生成した複数の個別電子メールを順次、送信メールサーバ７７０にＳＭＴＰで送信するように、メールスルーを実行する。

なお、送信メールサーバ７７０が複数宛先（メールアドレス）の１通の電子メールの処理を許可する場合には、メッセージ配信支援サーバ７６０は、上記電子メールの分解処理を行わずに、データ転送装置１０から受信した複数宛先（メールアドレス）が設定された１通の電子メールをそのまま送信メールサーバ７７０に送信してもよい。

【００５３】

送信メールサーバ７７０は、メッセージ配信支援サーバ７６０から受信した各個別電子メールを外部のメールサーバにＳＭＴＰで送信するように、メールスルーを実行する。ここで、送信メールサーバ７７０の送信抑止時間設定機能（スケジュール機能）により、例えば、その送信メールサーバでのメール滞留時や深夜帯には、上記外部のメールサーバへの電子メールの送信を抑止するようにしてもよい。

【００５４】

データ転送装置１０のノートパソコン２０は、メッセージ配信支援サーバ７６０に電子メールリクエストを送信した後、ノートパソコン２０に保存されている携帯電話番号やメールアドレスのデータ等の個人情報をすべて削除し（Ｓ１０）、その後、一連のデータ転送処理を終了する。これにより、ノートパソコン２０を介して個人情報が漏洩するのを防止できる。

【００５５】

上記図８のサービス例では、旧携帯電話機からのデータ取得を前処理として行い、新携帯電話機からの電話番号取得を後処理として説明したが、処理の手順はこれに限られない。例えば、新携帯電話機から電話番号を取得した後、データ転送装置１０がメッセージ配信支援サーバ７６０へメールアドレスの問合せをするまでに、旧携帯電話機からのメール

アドレス等のデータを取得するようにしてもよい。

【００５６】

また、上記図８のサービス例では、データ転送装置１０にて変更通知メッセージの作成処理を行うようにしたが、当該変更通知メッセージの作成処理をメッセージ配信支援サーバ７６０にて行うようにしてもよい。この場合、データ転送装置１０より取得した新旧各携帯電話機の情報をメッセージ配信支援サーバ７６０に転送するとともに、当該情報を最終処理で削除するように構成する。そして、データ転送装置１０は、メッセージ配信支援サーバ７６０のリモートコンソール端末として操作できるように構成すればよい。

【００５７】

また、上記図８のサービス例では、旧携帯電話機４０Ｂから読み出した複数のメールアドレス宛にメッセージを含む電子メールを送信する場合に、配信対象のメッセージを含む電子メールが何らかの理由で配達されなかったときには、その不達通知が利用者の最新メールアドレス宛（新携帯電話機）に届く。よって、電子メールの配達状況を利用者が容易に把握できる。しかも、電子メールのデータを作成した後、データ転送装置１０での処理が終了する前に、旧携帯電話機４０Ｂから読み出した個人情報であるメールアドレス等のデータを削除するので、かかるメールアドレス等の個人情報を通信ネットーク上のサーバに保存してパソコン等の端末装置からアクセスできるようにした場合とは異なり、個人情報保護の点が優れている。

【００５８】

また、上記図８のサービス例では、利用者の旧携帯電話機４０Ａから読み出した複数のメールアドレス宛に、その利用者が使用する最新のメールアドレス及び新携帯電話機４０Ｂの電話番号の変更を一斉に配信して通知することができる。

【００５９】

また、上記図８のサービス例では、旧携帯電話機４０Ａから新携帯電話機４０Ｂへのデータ転送の際にデータ転送装置１０に読み出される電話番号のデータ及びメモリダイヤルのメールアドレスのデータを、変更通知メッセージ配信用の電子メールの送信に流用することができるので、電子メールの送信処理の効率化を図ることができる。

【００６０】

また、上記図８のサービス例では、旧携帯電話機４０Ａから読み出した複数のメールアドレスのうち利用者が希望するメールアドレスのみに前記電子メールを送信できるので、携帯電話機から削除し忘れたメールアドレスなど、利用者がメッセージの配信を希望しないメールアドレスには、無駄な電子メール送信が行われないようにすることができる。

【００６１】

また、上記図８のサービス例では、配信対象のメッセージが、携帯電話機の機種変更を行ったときの電話番号・メールアドレスの変更通知を行うメッセージである場合について説明したが、配信対象のメッセージはこれに限定されるものではない。また、携帯電話機の機種変更の場合だけではなく、例えば、それまで使用していた携帯電話機を一旦解約し新しい携帯電話機を新規に契約する場合にも適用できる。

【００６２】

以上、本実施形態によれば、データ転送装置１０のノートパソコン２０の電源をオンして起動を開始すると、その起動処理時に、予め設定された特定のアカウントで自動ログオンされ、事業者ネットワーク４００を介してサーバ７００～７８０に自動接続されるので、ログオンのためのパスワード入力やサーバへの接続操作が不要になってセキュリティが高まるとともに、そのパスワード入力等を利用者に意識させることがないので利用者の利便性も高まる。しかも、上記自動ログオンした特定のアカウントでは、通信ネットワークを介した外部への接続先が上記事業者ネットワーク４００上のサーバ７００～７８０に制限されているので、上記自動ログオン後、利用者が上記サーバ以外の外部接続先に通信ネットワークを介して接続するのを制限でき、一般のネットワークサイトへのアクセスを抑止してスパイウェアやワーム等が取り込まれてしまうのを防止できるので、セキュリティを更に高めることができる。更に、上記サーバ７００～７８０に接続された後、クライア

ント証明書（デジタル証明書）によるクライアント認証及び暗号化通信を利用するＶＰＮがサーバ７００～７８０との間に構築され、そのＶＰＮ上でサーバ７００～７８０と通信できるので、サーバとの通信の盗聴や通信内容の改ざんの危険性を低減できるので、更にセキュリティを高めることができる。また、データ転送装置１０のノートパソコン２０の起動処理が終了すると、上記サーバとの通信を伴うサービスを利用するときの初期画面が表示されるので、初期画面を表示するための利用者の個別操作が不要となり、利用者の利便性を更に高めることができる。以上により、上記データ転送装置１０が不特定の利用者によって操作可能な状態で設置される場合でも、利用者の利便性を確保しつつ、そのデータ転送装置１０から公衆の通信ネットワークを介してサーバ７００～７８０との通信を伴うサービスを利用するときのセキュリティを総合的に高めることができる。

【００６３】

特に、本実施形態では、データ転送装置１０とメッセージ配信支援サーバ７６０との通信を伴うサービスを利用する際に、携帯電話機の電話番号やメールアドレスなどの個人情報が送受信されるが、かかる個人情報保護対策として高いセキュリティを担保することができる。

【００６４】

また、本実施形態によれば、前記サーバへのＶＰＮ接続時に通信が切断された場合には、サーバに接続するためのＶＰＮが再構築されるので、サーバとの通信切断時におけるＶＰＮの再構築のための利用者による操作が不要となるとともに、かかる再接続及び再構築の処理を利用者に意識させることもない。

【００６５】

また、本実施形態によれば、データ転送装置１０のノートパソコン２０の起動処理時にドメインユーザのアカウントで自動ログオンされるので、ＶＰＮ上に構築されたネットワークドメインへログオンするための利用者の操作が不要になるとともに、かかるネットワークドメインへのログオン処理を利用者に意識させることもない。

【００６６】

また、本実施形態によれば、データ転送装置１０のノートパソコン２０の起動処理時に、そのノートパソコン２０の汎用のデスクトップ画面及びメニュー画面に前記サーバの利用に不要なアイコンを表示しないように設定しているので、サーバの利用に不要なアイコンに対する利用者の誤操作や意識的な不正操作を防止し、利用者の不正使用を抑止することにより、更にセキュリティを高めることができる。

【００６７】

また、本実施形態によれば、データ転送装置１０のノートパソコン２０の起動処理時に、そのノートパソコン２０に組み込まれている汎用のアプリケーションプログラムについてサーバの利用に不要な機能を制限するように設定しているので、汎用のアプリケーションプログラムの機能のうちサーバ利用に不要な機能が利用者の誤操作又は意識的な操作によって利用されるのを回避することにより、更にセキュリティを高めることができる。

【００６８】

また、本実施形態によれば、各データ転送装置１０のノートパソコン２０で個別に基本ＯＳプログラムの更新操作を行うことなく、ＷＳＵＳサーバ７２０から各ノートパソコン２０に対して基本ＯＳプログラムの更新プログラムを一括配信することにより、各通信端末装置のノートパソコン２０における基本ＯＳプログラムを遠隔的に一括更新することができる。

【００６９】

また、本実施形態によれば、データ転送装置１０から事業者ネットワーク４００上のサーバ７００～７８０との通信を伴うサービスを利用するときに使用する新規プログラム又は修正プログラムを複数のデータ転送装置１０のノートパソコン２０に一括配信するプログラム管理サーバを備えてもよい。この場合には、各データ転送装置１０のノートパソコン２０で個別に新規プログラム又は修正プログラムをダウンロードする操作を行うことなく、プログラム配信サーバ７４０から各データ転送装置１０のノートパソコン２０に対し

て新規プログラム又は修正プログラムを一括配信することにより、各ノートパソコン２０における新規プログラム等のダウンロード及びそのインストールが容易になる。

【００７０】

また、本実施形態によれば、資産管理サーバ７３０が各データ転送装置１０のノートパソコン２０から収集したハードウェア及びソフトウェアに関する情報に基づいて各ノートパソコン２０を一元管理できる。

【００７１】

以上、本発明の好ましい実施形態を説明したが、本発明の範囲又は趣旨から逸脱することなく、特許請求の範囲に記載された技術的事項の範囲内において、開示した実施形態に種々の変更を加えることができる。

【００７２】

例えば、上記実施形態では、通信端末装置が、携帯電話機間のデータ転送に利用できるように量販店に設置され、通信事業者ネットワーク上のサーバと通信して各種サービスを受けることができるノートパソコン２０を備えたデータ転送装置１０である場合について説明したが、本発明は、他の通信端末装置にも適用できる。例えば、不特定のユーザに操作可能な環境に設置されセキュリティを確保した状態で通信ネットワーク上のサーバと通信してサービスを受けるような他の通信端末装置にも適用できる。

【図面の簡単な説明】

【００７３】

【図１】本発明の実施形態に係る通信システムの全体構成の一例を示す説明図。

【図２】データ転送装置の斜視図。

【図３】データ転送装置に用いるノートパソコンの斜視図。

【図４】データ転送元の携帯電話機を接続したデータ転送装置の斜視図。

【図５】データ転送先の携帯電話機を接続したデータ転送装置の斜視図。

【図６】データ転送装置のノートパソコンを電源オンしたときのノートパソコンと事業者ネットワーク上のサーバとの間の通信処理の一例を示す説明図。

【図７】ノートパソコンの電源オンから事業者ネットワーク上のサーバとのＶＰＮ通信が可能になるまでの手順の一例を示すフローチャート。

【図８】データ転送装置とメッセージ配信支援サーバとの通信を伴うサービスを利用するときの処理の流れの一例を示すシーケンス図。

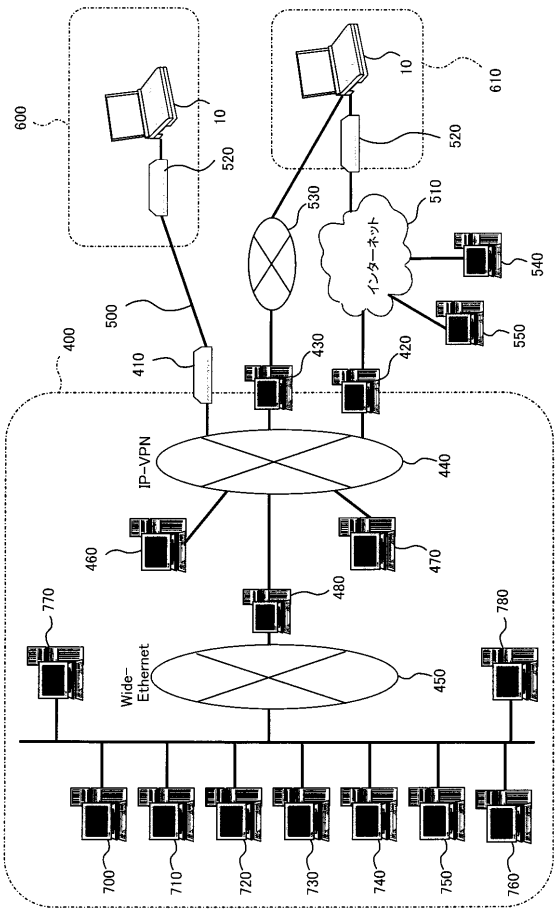
【符号の説明】

【００７４】

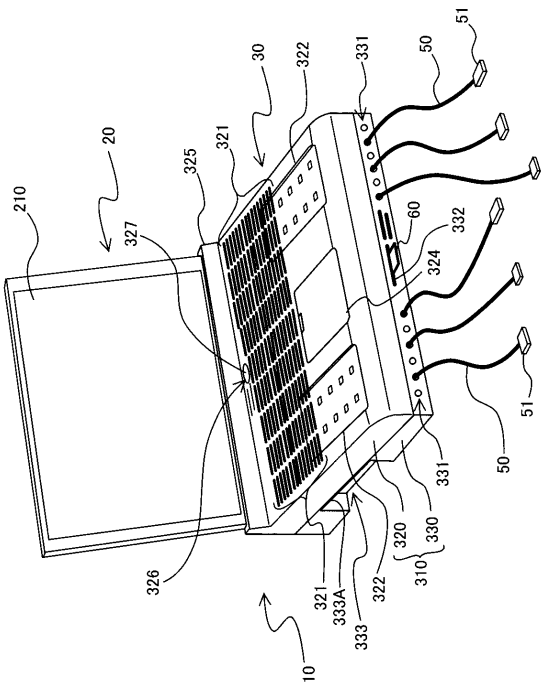
１０　データ転送装置（通信端末装置）
２０　ノートパソコン（コンピュータ装置）
３０　アダプター
４０　携帯電話機
４００　事業者ネットワーク
４２０　アクセスゲートウェイ装置
４３０　リモートアクセスサーバ
４４０　ＩＰ－ＶＰＮ
４５０　広域イーサネット網
４６０　ＲＡＤＩＵＳ認証サーバ
４７０　ＰＫＩ認証サーバ
５１０　インターネット
６１０　量販店
７００　ドメインサーバ
７１０　ウィルス駆除ソフト管理サーバ
７２０　ＷＳＵＳサーバ
７３０　資産管理サーバ
７４０　プログラム配信サーバ

７５０　メンテナンスサーバ
７６０　メッセージ配信支援サーバ
７７０　送信メールサーバ
７８０　加入者情報管理サーバ

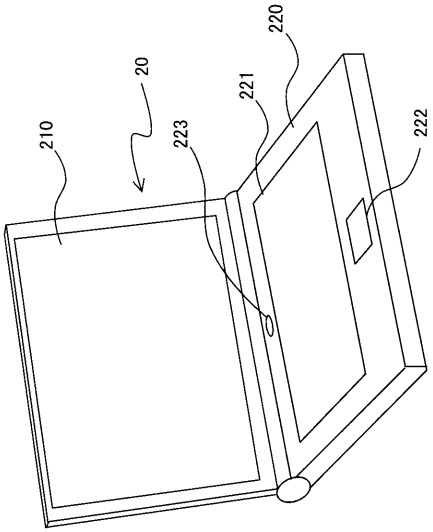
【図１】



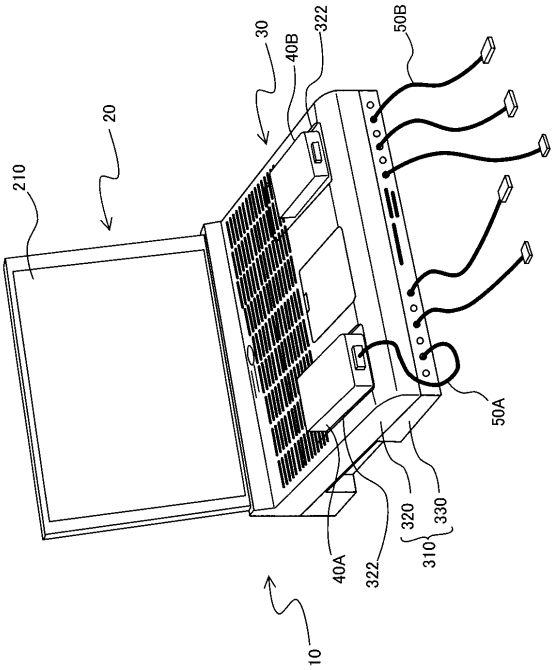
【図２】



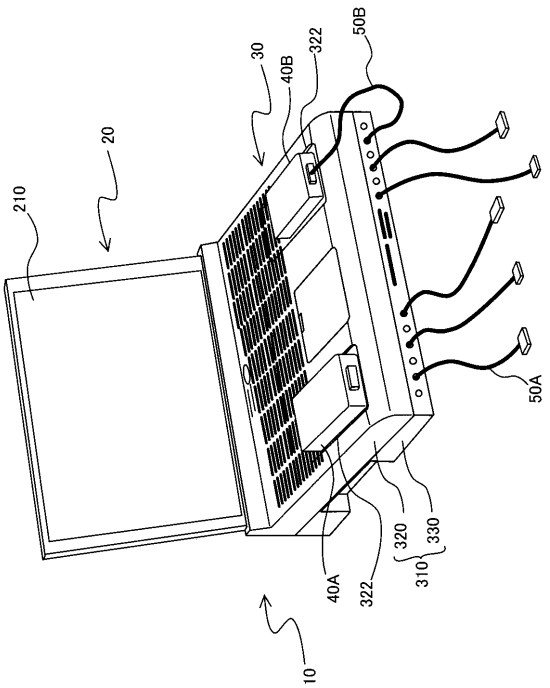
【図３】


210
20
223
221
220
222

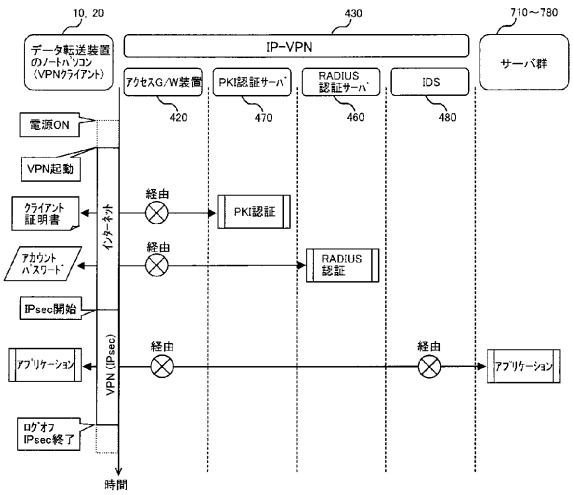
【図４】


30
40B
322
50B
20
210
50A
320
330
310
40A
322
10

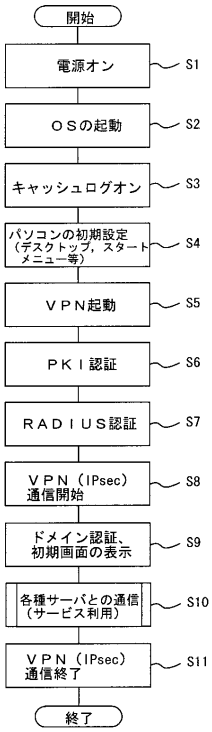
【図５】


30
40B
322
50B
20
210
50A
320
330
310
40A
322
10

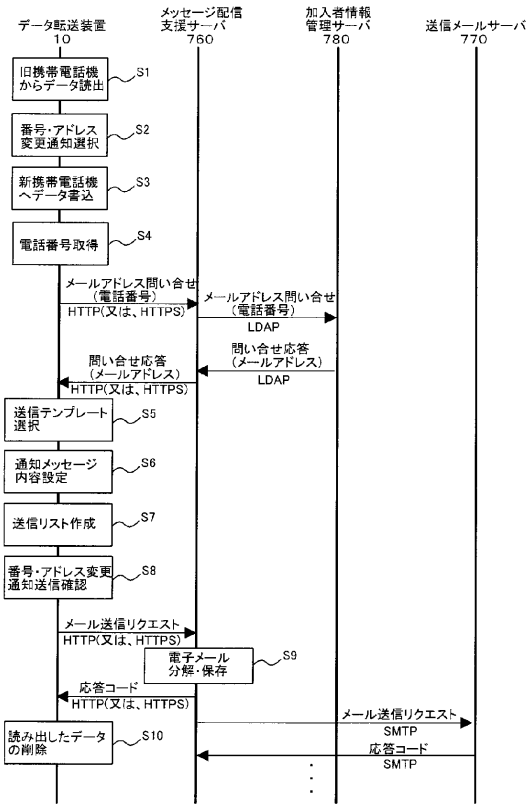
【図６】


10, 20
430
710～780
データ転送装置
のノートパソコン
（VPNクライアント）
IP-VPN
サーバ群
アクセスG/W装置
PKI認証サーバ
RADIUS
認証サーバ
IDS
420
470
460
480
電源ON
VPN起動
クライアント
証明書
経由
PKI認証
アカウント
パスワード
経由
RADIUS
認証
IPsec開始
アプリケーション
経由
経由
アプリケーション
ログオフ
IPsec終了
インターネット
VPN（IPsec）
時間

【図７】


開始
電源オン
S1
ＯＳの起動
S2
キャッシュログオン
S3
パソコンの初期設定（デスクトップ，スタートメニュー等）
S4
ＶＰＮ起動
S5
ＰＫＩ認証
S6
ＲＡＤＩＵＳ認証
S7
ＶＰＮ（IPsec）通信開始
S8
ドメイン認証、初期画面の表示
S9
各種サーバとの通信（サービス利用）
S10
ＶＰＮ（IPsec）通信終了
S11
終了

【図８】


データ転送装置 10
メッセージ配信支援サーバ 760
加入者情報管理サーバ 780
送信メールサーバ 770
旧携帯電話機からデータ読出
S1
番号・アドレス変更通知選択
S2
新携帯電話機へデータ書込
S3
電話番号取得
S4
メールアドレス問い合せ（電話番号）
HTTP(又は、HTTPS)
メールアドレス問い合せ（電話番号）
LDAP
問い合せ応答（メールアドレス）
LDAP
問い合せ応答（メールアドレス）
HTTP(又は、HTTPS)
送信テンプレート選択
S5
通知メッセージ内容設定
S6
送信リスト作成
S7
番号・アドレス変更通知送信確認
S8
メール送信リクエスト
HTTP(又は、HTTPS)
電子メール分解・保存
S9
応答コード
HTTP(又は、HTTPS)
メール送信リクエスト
SMTP
読み出したデータの削除
S10
応答コード
SMTP

フロントページの続き

(72)発明者　高橋　健太郎
東京都港区東新橋一丁目９番１号　ボーダフォン株式会社内

審査官　田中　慎太郎

(56)参考文献　特開２００４－０２３４８５（ＪＰ，Ａ）
桑名潤平，ＳｏｆｔＥｔｈｅｒの進化系　ＰａｃｋｅｔｉＸ　ＶＰＮ　２．０がやってきた　次世代ＶＰＮプラットフォームを完全解説！　VIRTUAL PRIVATE NETWORK，ＳｏｆｔｗａｒｅＤｅｓｉｇｎ　Ｎｏ．１８３，日本，（株）技術評論社，２００６年　1月１８日，第１８３号，p.154-163
増井雄一郎，Ｌｉｎｕｘならこんなに使える！　低スペックＰＣ活用大作戦，日経Ｌｉｎｕｘ第７巻　第９号，日本，日経ＢＰ社，２００５年　９月　８日，第７巻　第９号，p.43-53

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｈ０４Ｌ　１２／６６