(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
2008 年11 月6 日 (06.11.2008)

PCT

(10) 国際公開番号
WO 2008/132869 A1

(51) 国際特許分類:
G06F 21/24 (2006.01) *G09C 1/00* (2006.01)
G06F 12/00 (2006.01) *H04L 9/32* (2006.01)

(21) 国際出願番号: PCT/JP2008/053593

(22) 国際出願日: 2008 年2 月29 日 (29.02.2008)

(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2007-110532 2007 年4 月19 日 (19.04.2007) JP
特願2007-159613 2007 年6 月18 日 (18.06.2007) JP

(71) 出願人 (米国を除く全ての指定国について): 独立行政法人産業技術総合研究所 (NATIONAL INSTITUTE OF ADVANCED INDUSTRIAL SCIENCE AND TECHNOLOGY) [JP/JP]; 〒1008921 東京都千代田区霞が関１丁目３番１号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 藤巻 真 (FUJIMAKI, Makoto) [JP/JP]; 〒3058562 茨城県つくば市東１－１－１中央第４ 独立行政法人産業技術総合研究所内 Ibaraki (JP). 富永 淳二 (TOMINAGA, Junji) [JP/JP]; 〒3058562 茨城県つくば市東１－１－１中央第４ 独立行政法人産業技術総合研究所内 Ibaraki (JP). 桑原 正史 (KUWAHARA, Masashi) [JP/JP]; 〒3058562 茨城県つくば市東１－１－１中央第４ 独立行政法人産業技術総合研究所内 Ibaraki (JP).

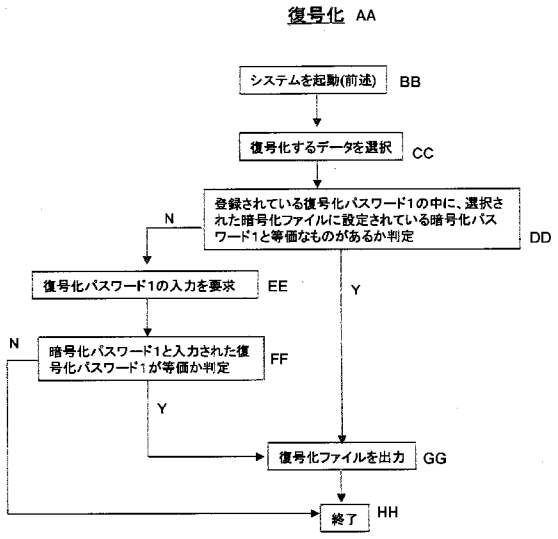
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH,

/続葉有/

(54) **Title:** GROUP ENCRYPTION AND DECRYPTION SYSTEM AND METHOD, AND PROGRAM

(54) 発明の名称: グループ用暗号化及び復号化システム及び方法、並びにプログラム

[図8]



AA DECRYPTION
BB START UP SYSTEM (DESCRIBED ABOVE)
CC SELECT DATA TO BE DECRYPTED
DD JUDGE WHETHER, IN REGISTERED DECRYPTION PASSWORDS (1), THERE ARE DECRYPTION PASSWORDS CORRESPONDING TO ENCRYPTION PASSWORDS (1) SET IN SELECTED ENCRYPTED FILE
EE REQUEST TO INPUT DECRYPTION PASSWORDS (1)
FF JUDGE WHETHER INPUT DECRYPTION PASSWORDS (1) CORRESPOND TO ENCRYPTION PASSWORDS (1)
GG OUTPUT DECRYPTED FILE
HH END

(57) **Abstract:** An encryption and decryption system sets at least one or more encryption passwords for one file and registers these encryption passwords in the system. A plurality of the encryption passwords different for each group to which the user belongs are registered in the system and the user selects at least one of the plurality of the encryption passwords to encrypt a file. In order to share the encrypted data with other users, the encryption and decryption system has a function of creating install software for installing an encryption and decryption system, in which the encryption passwords registered in the system and the decryption passwords corresponding to these encryption passwords are set, into personal computers of the other users.

(57) 要約: 本発明の暗号化及び復号化システムは、１つのファイルに対し暗号化パスワードを少なくとも１つ以上設定すると共に、この暗号化パスワードをシステム内に登録しておく。ユーザーの属するグループ毎に異なる複数の前記暗号化パスワードがシステム内に登録されていて、ユーザーは、ファイルの暗号化のために前記複数の暗号化パスワードの内、少なくとも１つを選択する。他のユーザーと暗号化されたデータを共有するために、当該システムに登録されている暗号化パスワード及びこの暗号化パスワードに等価な復号化パスワードが設定されている暗号化及び復号化システムを、当該他のユーザーのパーソナルコンピュータにインストールするためのインストール用ソフトウエアを作成する機能を有する。

WO 2008/132869 A1

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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

明 細 書

グループ用暗号化及び復号化システム及び方法、並びにプログラム

技術分野

[0001] 本発明は、暗号化時に暗号化パスワードを設定してファイルを暗号化して暗号化ファイルを作成すると共に、既に暗号化されている暗号化ファイルを、復号化パスワードを用いて復号化することにより元のファイルを復元するグループ用暗号化及び復号化システム及び方法、並びにプログラムに関する。

背景技術

[0002] 近年、個人情報等の機密データの管理が重要となってきており、その漏洩や紛失に対する対策、盗難対策が重要となっている。一般的な、コンピュータのデータに関するセキュリティー対策として、データの暗号化復号化が挙げられる。暗号化復号化技術として有名なものは、共通鍵暗号法と公開鍵暗号法である。共通鍵暗号法とは、暗号化する人と復号化する人とがそれぞれの操作を行うに際し、同じ鍵を使って暗号化、復号化を行う方法である。一方、公開鍵暗号法は、秘密鍵と公開鍵というペアの鍵を用いて、暗号化と複合化を行う手法で、どちらか一方の鍵で暗号化したデータは、もう一方の鍵を使わないと復号化できないという特徴を有している。(特許文献1参照。)

[0003] このように、従来種々の暗号化復号化技術が知られているが、このような技術は、送り側と受け側の間のデータ共有方法であり、グループ内で暗号化データを共有する方法としては適していない。特に、あるユーザーが、複数のグループに属することがある。このような場合、データを共有するグループ毎に、鍵(パスワード)を設定して、かつ、グループ毎の鍵を全て覚えておく必要がある。鍵を簡単化することにより、多数の鍵を覚えておくことは可能になるとしても、セキュリティー上問題があることは明白である。

特許文献1:特開2001－308843号公報

発明の開示

発明が解決しようとする課題

[0004] 本発明は、係る問題を解決して、暗号化及び復号化のパスワード入力を簡易にしつつ、セキュリティー機能を向上させて、特に、グループ内で暗号化データを共有することを目的としている。

また、暗号化解除のパスワードがランダムアタックによって解除される恐れがあるが、本発明は、このようなランダムアタックに備えることを目的としている。

課題を解決するための手段

[0005] 本発明のグループ用暗号化及び復号化システム及び方法、並びにプログラムは、暗号化時に暗号化パスワードを設定してファイルを暗号化して暗号化ファイルを作成すると共に、既に暗号化されている暗号化ファイルを復号化する際、当該ファイルの暗号化時に設定した暗号化パスワードと等価な復号化パスワードが入力されることによって復号化を許可し元のファイルを復元する。この暗号化パスワードは、1つのファイルに対して少なくとも1つ以上設定する。また、この暗号化パスワードは、システム内に登録されている。ユーザーの属するグループ毎に異なる複数の前記暗号化パスワードがシステム内に登録されていて、ユーザーは、ファイルの暗号化のために前記複数の暗号化パスワードの内、少なくとも1つを選択する。

[0006] 他のユーザーと暗号化されたデータを共有するために、当該システムに登録されている1つ又は複数の暗号化パスワード及びこの暗号化パスワードに等価な復号化パスワードが設定されている暗号化及び復号化システムを、当該他のユーザーのコンピュータにインストールするためのインストール用ソフトウエアを作成する機能を有する。

または、他のユーザーと暗号化されたデータを共有するために、当該システムに登録されている暗号化パスワード及び該暗号化パスワードに等価な復号化パスワードが設定されている1つ又は複数のグループを、当該他のユーザーが使用している同等のシステムに登録するための登録用ソフトウエアを作成する機能を有する。

発明の効果

[0007] 本発明によれば、暗号化及び復号化のパスワード入力を簡易にしつつ、セキュリティー機能を向上させて、特に、複数のグループに属する個人が、それぞれのグループ内でそれぞれ別々に暗号化データを共有することが可能となる。また、暗号化解

除のパスワードがランダムアタックによって解除される恐れを防ぐことができる。

図面の簡単な説明

[0008] [図1]本発明を具体化する暗号化及び復号化ソフトウエアの基本機能を説明する図である。

[図2]システムの起動時の動作(基本例)を説明する図である。

[図3]システムの終了時の動作を説明する図である。

[図4]システムに登録されている各種パスワードの暗号化及び復号化を説明する図である。

[図5]システムの起動時の動作を説明する図2とは異なる別の例を示す図である。

[図6]システムに登録されている各種パスワードの復号化を説明する図4とは異なる別の例を示す図である。

[図7]暗号化を説明する図である。

[図8]復号化を説明する図である。

[図9]復号化を説明する図8とは異なる別の例を示す図である。

[図10]複数のユーザーで構成されたグループの作成を説明する図である。

[図11]グループ表示例とグループの追加を説明する図である。

[図12]インストール用ソフトウエアの作成を説明する図である。

[図13]グループとそのグループ員の構成例を示す図である。

[図14]登録用ソフトウエアの使用方法を示す図である。

発明を実施するための最良の形態

[0009] 以下、例示に基づき、本発明を説明する。図1は、本発明を具体化する暗号化及び復号化ソフトウエアの基本機能を説明する図である。図中の「暗号化及び復号化ソフトウエア」としては、文書を暗号化し、かつ暗号化ファイルを復元することのできるそれ自体は周知のアルゴリズムで暗号化し、かつ復号化することができる。復号化とは、暗号化ファイルを元のファイルに復元することである。また、以下では、パーソナルコンピュータ(パソコン)での使用を主として説明するが、本システムは、データやファイルなどの電子情報を扱う全てのコンピュータ(電子計算機や携帯電話など)に、同様に適応が可能である。また、個人が所有する計算機端末(パソコンや携帯電話)以外

にも、サーバーとなるコンピュータに対し、複数のユーザーがアクセスして使用する場合のデータやファイルの送受信時のセキュリティーにも使用可能である。

[0010] 図示のように、機密文書などを、暗号化及び復号化ソフトウエアに入力する。暗号化及び復号化ソフトウエアは、暗号化したファイル(機密文書)を出力する。ファイルの暗号化は、システムを起動させ、システムが立ち上がった後、暗号化したいファイルを選択し、例えば、ソフトウエア画面上にドラッグ&ドロップ、又は、ソフトウエア上から当該ファイルを選択することによって、当該ファイルを暗号化する。暗号化されたファイルを暗号化ファイルと呼ぶ。ファイルを暗号化する際、ファイルにはパスワードを設定し、暗号化ファイルを復号化する際に、この設定されたパスワードと等価なパスワードが入力された時のみ復号化を許可する。この、暗号化時にファイルに設定するパスワードを暗号化パスワード、復号化時に入力するパスワードを復号化パスワードと呼ぶ。

[0011] 本発明では、暗号化時に少なくとも1つ以上の暗号化パスワードを設定する。この暗号化パスワードは、暗号化ファイル中に保持されている内容の漏洩を防ぐために設定される暗号化パスワードであり、以下、暗号化パスワード1と呼ぶ。暗号化パスワード1はグループ員の認証に使用できる(グループ形成、グループ員認証については後述)。暗号化パスワードは、システム内に記憶されている。

[0012] 本システムでは、複数の暗号化パスワードをシステムに記憶させて用いることができる。ユーザーはこのような複数のパスワードの中から1つのパスワードを選択し、暗号化パスワードとしてファイルを暗号化する。

以下では、1つのファイルを暗号化する際、1つの暗号化パスワード1を設定する場合について説明する。暗号化パスワードの個数が増えれば、セキュリティーは向上するが、使用時の煩雑さが増すこととなる。但し、基本的な原理は変わらない。

[0013] 暗号化された機密文書復元のためには、まず暗号化ファイルを選択し、暗号化及び復号化ソフトウエアに入力する。例えば、ソフトウエア画面上にドラッグ&ドロップ、又は、ソフトウエア上から当該ファイルを選択する。復号化パスワードの手入力が必要な場合、ソフトウエアは、対象となる暗号化ファイルに設定されている暗号化パスワード1に対応する復号化パスワードの入力を要求する。以下、暗号化パスワード1に

対応する復号化パスワードを復号化パスワード1と呼ぶ。入力された復号化パスワード1と暗号化パスワード1を照合し等価であれば、暗号化ファイルを復号化する。

[0014] 復号化を実施する別の方法として、復号化パスワード1をソフトウエア内(システム内)に登録しておく場合、暗号化されているファイルを選択し、ソフトウエア画面上にドラッグ&ドロップ、又は、ソフトウエア上から当該ファイルを選択する。このとき、ソフトウエア内の復号化パスワード1登録欄に予め復号化パスワード1を入力しておくと、ソフトウエアは、登録欄の復号化パスワード1と、ファイルに設定された暗号化パスワード1を照合し等価であれば(つまり復号化パスワード1登録欄に登録したパスワードが間違っていなければ)、ファイルを復号化する。そして、ソフトウエアは元の文書(機密文書など)を出力する。

[0015] 本ソフトウエアのインストール(本システムをコンピュータなどへ導入すること、または本システムをコンピュータなどで使用可能な状態にすること)は、以下のように行う。まず、インストール用ソフトウエアが収められているCDなどの記憶媒体をパーソナルコンピュータにセットする。又はインストール用ソフトウエアをダウンロードするなどして入手し、インストールの準備を行う。第三者に本ソフトウエアを盗まれ、非合法にインストールされることを防ぐため、インストールを許可するパスワード(インストール用パスワード。以下ISパスワードと呼ぶ)を設定しておくことが望ましい。ISパスワードを入力するとインストールを開始する。ISパスワードは上記の暗号化パスワード1や復号化パスワード1と同じとすると、パスワードの数が増えず利便性が向上する。

[0016] 各ソフトウエアにそれぞれの暗号化パスワード1，復号化パスワード1が付与されており、この暗号化パスワード1と復号化パスワード1は等価である。パスワードが等価であると言う意味は、通常はそれぞれが同一の文字列であることを意味する。しかし、片方のパスワードの文字列が、もう片方の等価なパスワードに対し何らかの演算を行うことによって得られる文字列と同じ場合も等価とみなすことができる。つまり、2つのパスワードをコンピュータが比較し、相関関係があると判断することができる場合、この2つのパスワードは等価であるといい、相関関係がないと判断することができる場合、この2つのパスワードは等価ではないという。

[0017] インストールを行うとこれらの2つのパスワードがシステム内に登録(保存)される。但

し、復号化パスワード1に関しては、システム内に登録するかしないかをユーザーが選択できるようにすると、以下に説明するようにユーザーがシステムの利便性やセキュリティーの度合いを選べるようになる。また、復号化パスワード1はインストール用ソフトウエア内には格納されておらず、例えばインストール用CDなどのパッケージなどに印刷されており、ユーザーが別途入力するとしても良い。インストール用ソフトウエア内に格納されている各種パスワード(暗号化パスワード1，復号化パスワード1)は、セキュリティー上、その一部又は全部が暗号化されて格納されていることが望ましい。暗号化されて格納されている各種パスワードの復号化パスワードをISパスワードと同じにしておき、インストール時のISパスワードの入力によって各種パスワードが復号化され、システム内に登録されるようにすると利便性が高くなる。

[0018] 復号化パスワード1をシステム内に登録することを選択すると、この復号化パスワード1に対応する暗号化パスワード1が設定されて暗号化されたファイルを復号化する際、ユーザーは復号化パスワード1を入力する必要が無い為、操作が簡便になる。しかし、この場合、後述するシステム起動パスワード(STパスワード)及び登録されている各種パスワードに対する暗号化パスワード(PSパスワード1)が破られると、その時点で上記のファイルは復号化が可能な状態となってしまい、よって、セキュリティーの度合いは低くなる。

[0019] 復号化パスワード1をシステム内に登録しないことを選択すると、STパスワード及びPSパスワード1が破られても、復号化パスワード1を知っているユーザー以外復号化を実施できない為セキュリティー性は向上するが、操作は煩雑になる。

以上の操作によって、このソフトウエアで暗号化したデータ(ファイル)を復号化する際のパスワードが設定される。その他、必要なファイルなどをコピーしインストールを完了する。

[0020] 登録された各種パスワードは、そのまま保存しておくと、解読され盗用されてしまう恐れがあるため、システムが起動していないとき、又は暗号化や複合化を実施しないときには、その一部又は全部を暗号化した状態でシステム内に保存しておく。この時設定される暗号化パスワードをPSパスワード1と呼ぶ。また、このPSパスワード1に対応する復号化パスワードをPSパスワード2と呼ぶ。PSパスワード1、2はインストール

時又は初回使用時に設定する。

[0021] 図2は、システムの起動時の動作(基本例)を説明する図である。まず、例えば、システムのアイコンをダブルクリックすることにより、システムを起動する。インストール時又は初回使用時に、本システムを起動するためのパスワード(STパスワード)を設定する。STパスワード設定以降はソフトウエア起動時にSTパスワードを入力する。本ソフトウエアは、入力されたSTパスワードの正誤評価を行い、誤りの場合はソフトウエアを終了させ、正しい場合はシステムを起動する。ここで、STパスワードをPSパスワード1と等価としておき、つまりPSパスワード2として用い、STパスワードの入力によってシステムの起動と同時にシステム内に登録されている複数の各種パスワードを復号化するように設定しておくと、別途各種パスワードの復号化を行う必要がなく利便性が高い。また、この場合、PSパスワード1、2を別途設定する手間も省ける。そして、暗号化/復号化の命令待ち(待機)をする。

[0022] 図3は、システムの終了時の動作を説明する図である。例えば、終了ボタンをクリックすることにより、システムを終了すると、登録されている複数の各種パスワードを暗号化して、本ソフトウエアを終了させる。

システムを起動したまま離席せざるを得ない場合などに、各種パスワードが復号化されたままの状態であることは望ましくない。よって、ユーザーが任意の時に各種パスワードを暗号化できるように設定することが望ましい。再使用時には、再度、暗号化された各種パスワードを復号化して使用する。図4はこの動作を説明する図である。ユーザーが各種パスワード暗号化操作を行うと、各種パスワードには、PSパスワード1が設定されて暗号化される。その後システムは待機状態となるが、このとき、各種パスワードは暗号化されており使用できない為、暗号化及び復号化の作業はできない。その後、ユーザーによってPSパスワード2が入力されると、システムは入力されたPSパスワード2とPSパスワード1を照合し等価であれば、各種パスワードを復号化し、暗号化/復号化の命令待ち(待機)をする。

[0023] 上記では、各種パスワードの暗号化はユーザーが行う場合を説明したが、ある特定時間システムが使用されなかった場合、自動的に各種パスワードが暗号化される、というような設定を行うと、より高いセキュリティーを得られる。

[0024] 図5は、システムの起動時の動作を説明する図2とは異なる別の例を示す図である。図示のシステムは、セキュリティーを考慮し、且つ使い勝手を考慮した改良版である。STパスワードの累積間違い回数が規定回数(例えば3回)を越えると、登録(保存)されている全ての暗号化パスワード1、復号化パスワード1を消去する。そして、再度グループを追加し各種パスワードを登録して(グループの作成を参照)、STパスワードの再設定をした後に、システムを起動する。

[0025] この再設定により、ユーザーはSTパスワードを忘れてしまっても、再度グループ追加作業を行うことで暗号化ファイルの復号化が可能となる。一方、盗難に遭った際、盗んだ側はグループの追加作業が行えない為、暗号化ファイルの復号化ができず、よってデータを盗み見ることができない。新しいSTパスワードの設定は、次回のシステム起動時でも良い。

[0026] 同様の設定がPSパスワード1、2に対しても可能である。このプロセスを図6に示す。PSパスワード2の累積間違い回数が規定回数(例えば3回)を越えると、登録(保存)されている全てのパスワードを消去する。そして、再度グループを追加し各種パスワードを登録して(グループの作成を参照)、PSパスワード1、2の再設定をした後に、システムを起動する。この場合も、新しいPSパスワード1、2の設定は、次回のシステム起動時でも良い。

[0027] 図7は、暗号化を説明する図である。まず、前述したようにして、システムを起動する。次に、暗号化するデータを選択し、ソフトウエア内に登録された複数の暗号化パスワード1の中から1つを選択する。選択された暗号化パスワード1を設定してファイルを暗号化して、暗号化ファイルを出力する。

[0028] システム起動時のSTパスワードと各種パスワードに対する暗号化パスワード(PSパスワード1)とが別々に設定されている場合は、システム起動後でファイルの暗号化を実施する前に各種パスワードに対する暗号化を解除する必要がある。

[0029] 図8は、復号化を説明する図である。前述したようにして、システムを起動する。復号化するデータを選択する。次に、システム内の復号化パスワード1登録欄に暗号化パスワード1と等価な復号化パスワード1が登録されているか判定する。等価な復号化パスワード1の登録が確認された場合、ファイルを復号化する。そして、ソフトウエア

は元の文書(機密文書など)を出力する。

[0030] 等価な復号化パスワード1がシステム内に登録されてない場合、復号化パスワード1の入力を要求する。ソフトウエアは、入力された復号化パスワード1と、ファイルに設定された暗号化パスワード1を照合し等価であればファイルを復号化する。そして、ソフトウエアは元の文書(機密文書など)を出力する。異なれば、終了(「再度パスワードを入力する」としても可)する。

[0031] 図9は、復号化を説明する図8とは異なる別の例を示す図である。盗難時のランダムアタックの予防機能付き版であり、システム起動パスワード(STパスワード)及び各種パスワードに対する暗号化パスワード(PSパスワード1、2)が破られた場合の動作を説明する図である。なお、ランダムアタックとは、暗証番号などを無限に入力し破る方法のことである。システムを起動し、復号化するデータを選択した後、システム内の復号化パスワード1登録欄に暗号化パスワード1と等価な復号化パスワード1が登録されているか判定する。等価な復号化パスワード1の登録が確認された場合、ファイルを復号化する。そして、ソフトウエアは元の文書(機密文書など)を出力する。

[0032] 等価な復号化パスワード1がシステム内に登録されてない場合、復号化パスワード1の入力を要求する。ソフトウエアは、入力された復号化パスワード1と、ファイルに設定された暗号化パスワード1を照合し等価であればファイルを復号化する。そして、ソフトウエアは元の文書(機密文書など)を出力する。復号化パスワード1の累積入力間違い回数が規定回数(例えば10回)を越えると、暗号化データを削除し、或いは当該ファイルに関連する登録されているパスワード(暗号化/復号化)を消去する。復号化パスワード1の登録がある場合、登録時に入力ミスがないとすると、直ちに、復号化ファイルを出力する。よって、盗難されシステム起動パスワードが破られてしまうと、セキュリティーは掛からないことになる。

[0033] 本システムは複数のユーザーで構成されたグループを形成することができる。グループ内では暗号化データを共有できる。つまり、グループ内のあるユーザーによって暗号化されたデータを同一グループ内の他のユーザーが復号化して中身を見られる。同一の暗号化パスワード1及び復号化パスワード1のソフトウエア(以下、同一番号ソフトウエアと呼ぶ)を、他の人(あるグループのグループ員など)のパソコンに、インス

トールすることによって、暗号化されたデータを共有可能となる。例えば、電子メールで重要データを送信する際、データを暗号化して特定個人に送信した場合、相手側パソコンに同一番号ソフトウエアがインストールされていれば、その特定個人のみがデータを暗号化解除して使用することができ、その他の人は、例えデータを盗んでも、暗号化解除できないため、データ内容を盗むことができない。ユーザーは複数のグループに属することが可能である。勿論、個人でのセキュリティーの為に使用することも可能である。

[0034] 次に、どのように複数のグループに属するかについて図10に沿って説明する。A氏を新たにグループGのグループ員にするために、A氏にグループGで使用しているソフトウエアのインストール用ソフトウエアが入ったCDグループGを渡し、A氏のパソコンにインストールする。ちなみに、ここでは、インストール用ソフトウエアはCD内に格納されているとしているが、これは、当然他のどのような記憶媒体も用いることが可能である。或いは、A氏にグループGで使用しているソフトウエアで作成したインストール用ソフトウエアを渡し、A氏のパソコンにインストールする(インストール用ソフトウエアの作成については後述)。

[0035] まず、前述の様に、インストール用パスワード(ISパスワード)が設定されている場合、ISパスワードを入力する。ISパスワードの入力によって、CD又はインストール用ソフトウエアに暗号化されて格納されていた各種パスワードが復号化される。ISパスワードが設定されていない場合、直ちにインストールが開始される。次に、本システムが当該パソコンで既に使用されているか判定する。A氏が本システムを初めてインストールする場合、A氏のパソコンにシステムがインストールされ、グループGの各種パスワード(暗号化パスワード1, 復号化パスワード1)がシステム内に登録される。但し、前述のように、復号化パスワード1に関しては、システム内に登録するかしないかをユーザーが選択できるように設定が可能である。また、復号化パスワード1はCDやインストール用ソフトウエア内には格納されておらず、別途口頭、郵送または電子メールなどでA氏に伝え、A氏が別途入力するとしても良い。A氏が当該パソコンで既に本システムを使用している場合、A氏が使用しているシステムに、グループGの各種パスワードが追加登録される。この場合、インストール用ソフトウエアは、単に新しいグルー

プを追加登録する為の登録用ソフトウエアとして働く。各種パスワード(暗号化パスワード1，復号化パスワード1)はCD毎又はインストール用ソフトウエア毎に異なる値が予め設定されている。

[0036] A氏が既に本システムを使用していることが当初から分かっている場合には、システムをインストールする必要が無い為、わざわざインストール用ソフトウエアをA氏に送る必要はない。この場合、A氏をユーザーとして加えたいグループの各種パスワードを登録する為のソフトウエア(登録用ソフトウエア)をA氏に渡し、A氏が所有しているシステムに各種パスワードの登録のみを行い、グループを追加(グループを新規登録)すれば良い。この登録用ソフトウエアの実施方法はインストール用ソフトウエアの実施方法と殆ど同じである。

[0037] 登録用ソフトウエアの実施方法を図14に示す。インストール用ソフトウエアと同様に、開始時に実施を許可するパスワード(ISパスワード)が設定されている場合、ISパスワードを入力する。ISパスワードの入力によって、登録用ソフトウエアに暗号化されて格納されていた各種パスワードが復号化され、A氏のシステムにグループGの各種パスワード(暗号化パスワード1，復号化パスワード1)が登録される。ISパスワードが設定されていない場合は、登録用ソフトウエアを実施すると、直ちに登録が開始される。前述のように、復号化パスワード1に関しては、システム内に登録するかしないかをユーザーが選択できるように設定が可能である。また、復号化パスワード1は登録用ソフトウエア内には格納されておらず、別途口頭、郵送または電子メールなどでA氏に伝え、A氏が別途入力するとしても良い。

[0038] 図11は、あるユーザーが属しているグループの表示例とグループの追加を説明する図である。図11において、グループ名は、ユーザーが自由に入力できるグループを識別するための名前である。ユーザーパスワード登録欄は、この欄にチェックを入れることで、ユーザーパスワード(復号化パスワード1を意味する)をシステムに登録することが可能となる。この欄にチェックがないと(例 ××サークル)ユーザーパスワードは登録されていない。よって、このグループで暗合化されたファイルをこのユーザーが復号化するには毎回ユーザーパスワードを入力する必要がある。このことは、セキュリティーを高めるが、操作は煩雑になる。

[0039] 図12は、インストール用ソフトウエアの作成を説明する図である。インストール用ソフトウエア作成アイコンをクリックして、インストー用ソフトウエア(インストール実行ファイル)を作成する。グループ員としたいメンバーにファイルを送付する(その後の動作は、図10に例示したグループの作成を参照)。同様に、登録用ソフトウエアの作成も登録用ソフトウエア作成アイコンをクリックすることによって行うことができる。

[0040] インストール用ソフトウエア作成アイコン、及び登録用ソフトウエア作成アイコンはグループ毎に1つあり、それぞれのグループに対していずれかのソフトウエアを作成することができる。インストール用ソフトウエアには、対象グループの各種パスワード情報(暗号化パスワード1, 復号化パスワード1)、及びソフトウエアのインストール用システムが含まれている。登録用ソフトウエアには、各種パスワード情報、及びこれらの情報を他のシステムに登録する為のシステムが含まれている。また、あるユーザーを一度に複数のグループのグループ員とする場合に便利なように、1つのインストール用ソフトウエアまたは1つの登録用ソフトウエア中に複数のグループの各種パスワードを入れることが出来るようにしても良い。

上述の様に、インストール用ソフトウエア及び登録用ソフトウエアには、上述の様な各種パスワード情報、及びインストール又はパスワード登録に必要な機能が備えられている。よって、インストール用ソフトウエア及び登録用ソフトウエアの作成とは、これらの各種パスワード情報及びインストール又はパスワード登録に必要な機能を備えたソフトウエアを生成することである。これらのソフトウエアの作成は、システム内に予め、インストール又はパスワード登録に必要な機能を備えるソフトウエアを用意しておき、このソフトウエア中に、上述のような特定の各種パスワードを組み込むことによって、容易に実施できる。つまり、システム中に、平時は、特定のパスワード情報が入っていないインストール又はパスワード登録に必要な機能を備えたソフトウエアを用意しておき、あるユーザーをある特定のグループのグループ員に入れたい場合に、当該グループのパスワード情報をこれらのソフトウエア中に登録し、インストール用ソフトウエア又は登録用ソフトウエアを作成する。作成されたソフトウエアを用いて、グループ員にしたいユーザーのコンピュータに、当該システムのインストール又は当該パスワード情報の登録を行えば良い。

[0041] インストール用ソフトウエアや登録用ソフトウエアは、一度に多くのメンバーを1つのグループに入れる際に非常に便利である。なぜなら、通常インストール用のCDは1枚か2枚程度しか無い為、多くのメンバーをグループに入れる際にはこのCDを多数複製するか回覧する必要がある。しかし、インストール用ソフトウエア作成機能または登録用ソフトウエア作成機能があれば、ある特定のグループのメンバーを一度に増やしたい場合、上記の手順にてそのグループ用のインストール用ソフトウエアまたは登録用ソフトウエアを作成後、このソフトウエアを電子メールなどで、メンバーに入れたいユーザーに送るだけで良い。

[0042] また、多くのユーザーが属しているグループでは、誰がそのグループ用のCDを保管しているのか分からなくなってしまう恐れがある。しかし、インストール用ソフトウエア作成機能または登録用ソフトウエア作成機能が有れば、CDを用いなくても新たにメンバーが増やせることから、CDの管理の必要がなくなる。

[0043] 但し、全てのユーザーにインストール用ソフトウエアや登録用ソフトウエアの作成機能を持たせると、グループのユーザー数が際限なく増加してしまう恐れがあり、また、不当にユーザーを増やすメンバーが現れる恐れもある。よって、下記の2種類のインストール用ソフトウエアを作成出来るようにするとさらに良い。1つは、上述した、全ての機能をインストールするソフトウエア(全機能インストールソフトウエア)であり、もう1つは、ユーザーとしては全く同じ機能であるが、このグループのインストール用ソフトウエア作成ボタン(アイコン)及び登録用ソフトウエア作成ボタン(アイコン)がない、つまり、このグループのインストール用ソフトウエアや登録用ソフトウエアを生成できないシステムをインストールするソフトウエア(機能限定インストールソフトウエア)である。このことを実現するには、全機能インストールソフトウエアを作成するアイコンと機能限定インストールソフトウエアを作成するアイコンとを用意すると良い。

[0044] 機能限定インストールソフトウエアによってシステムをインストールしたユーザー、又は機能限定インストールソフトウエアによって新たにグループを追加したユーザーは、このグループのインストール用ソフトウエアや登録用ソフトウエアを生成できない。よって、グループ員が勝手にさらなるグループ員追加を行わないようにするために用いることができる。

[0045] 同様の機構は登録用ソフトウエア作成時にも適応できる。つまり、新たに登録したグループにおいてインストール用ソフトウエアや登録用ソフトウエアの作成ボタンを付与する登録用ソフトウエアと、登録したグループにおいてインストール用ソフトウエアや登録用ソフトウエアの作成ボタンを付与しない登録用ソフトウエアとの、それぞれを作成できるようにしておけば良い。

[0046] 図13は、グループとそのグループ員の構成例を示す図である（各グループG1～G6は楕円で示し、グループ員名はアルファベットで示す）。グループ毎のユーザーパスワード（復号化パスワード1）、グループ員を表1に示す。

[表1]

グループ	ユーザーパスワード	グループ員
グループＧ１	5456wagT	A、B、C、D、E
グループＧ２	Joue7T51	C、F、G、H
グループＧ３	28regraT	A、B、C、K、N
グループＧ４	HrUme63	C、D、E、J、L、M
グループＧ５	Aime42R	I、L、M
グループＧ６	6398reik	Ｉのみ(Ｉの個人使用)

[0047] この時、例えば、ユーザーCはグループG1、G2、G3、G4に属しているので、これらのグループに属している他のユーザーがこれらのグループを指定して暗号化したファイルを復号化して読むことができる。但し、ユーザーCはグループG5には属していないので、ユーザーLやMがグループG5を指定して暗号化したファイルは復号化できない。

[0048] また、ユーザーIはグループG5に属し、且つ個人使用の為のグループG6のソフトウエアをインストールしている。ユーザーIがグループG5を指定して暗号化した場合、ユーザーLやMはこの暗号化ファイルの復号化が可能であるが、グループG5に属していない他のユーザーはこのファイルを復号化することができない。また、ユーザーIがグループG6を指定して暗号化を行った場合には、他のユーザーは誰も復号化できないため、ユーザーI個人での情報保護に使用可能である。

[0049] ユーザーCの使用しているシステムに登録してあるグループに関して表2に纏める。表2中には、インストールファイル生成機能の有無(例)も示した。

[表2]

グループ	ユーザーパスワード	インストールファイル生成機能
グループG１	5456wagT	あり
グループG２	(記憶させていない)	あり
グループG３	28regraT	なし
グループG４	HrUme63	なし

[0050] このような場合、ユーザーCは、グループG1及びG2に関して、CD又は全機能インストールソフトウエアを用いてインストールしており、よって、インストールファイル生成機能が付いており、さらにグループ員を増やすことができる。また、グループG2に対しては、解除パスワードを記憶させていない為、暗号化解除の際、毎回、解除パスワードを入力することを選択している。これは、グループG2における機密性が高い場合に有効である。

[0051] ユーザーCはグループG3及びG4に関しては、インストールファイル生成機能が無い。これは、これらのグループの他のグループ員から送られてきた(渡された)機能限定インストールソフトウエアを用いて、グループの追加を行ったからである。

ユーザーIの例を表3に纏める。

[表3]

グループ	ユーザーパスワード	インストールファイル生成機能
グループG５	Aime42R	あり
グループG６	6398reik	あり

[0052] ユーザーIの場合、グループG5とG6のみがシステムに登録してある。但し、グループG6にはユーザーIしかグループ員がいない。つまりこれはユーザーIがCDを購入し、個人データの保護用に使用しているためである。

[0053] 変形例1:

以下に、パスワードに関する変形例を挙げる。以上では、いずれのパスワードも、ある1つの文字列であった。しかし各パスワードは複数用意しても良く、または、分割された複数の文字列の組み合わせから生成しても良い。例えば、表1中のグループG1のユーザーパスワードは5456wagTであるが、このパスワードを5456とwagTの2つに分

割してシステム内に登録しておき、暗号化時、及び復号化時にこの2つの分割パスワードを足し合わせ、元のパスワードを生成してもよい。また、復号化パスワードのみを幾つかに分割して設定しても良い。例えば、暗号化時には1つのパスワード5456wagTを設定しておき、復号化パスワードとして5456の部分はシステムに登録し、wagTの部分のみを復号化パスワード1の入力時に入力するようにしても良い。勿論、分割された複数のパスワードから元のパスワードを形成する際の演算は足し合わせのみでなく、あらゆる計算可能な演算を用いることができる。

[0054] 変形例2:

以上では、パスワードはすべて文字列である場合を説明したが、全てのパスワードはパーソナルコンピュータへ物理的に接続する外部接続素子、例えば、USB(Universal Serial Bus)(登録商標)準拠コネクタによって接続する外部素子、赤外線通信デバイス、SD(Secure Digital)(登録商標)、IEEE1394、PC Card(登録商標)、COMPACTFLASH(登録商標)、Smart Media(登録商標)、MEMORY STICK(登録商標)、xD－Picture Card(登録商標)、FeliCa(登録商標)、ISO／IEC IS 18092又はBluetooth(登録商標)の準拠デバイス等に置き換えることができる。つまり、パスワードの入力を求められた際、パスワード入力の代わりにユーザーが所有するある特定の外部接続素子をパーソナルコンピュータに接続することによってパスワードの入力と等価と見なすことができる。

[0055] また、全てのパスワードは文字列のみでなく、指紋や静脈紋などの特定の画像データやパターンデータを用いることも可能である。

また、本システムでは、各種パスワードがシステム内に暗号化されて保存されているが、盗難時パスワードデータが解読される恐れもあるため、これらのパスワードデータはシステムがインストールされているパーソナルコンピュータに内蔵の記憶装置や記憶媒体ではなく、取り外しが可能な記憶装置や記憶媒体、例えばフロッピー(登録商標)ディスクや外部接続が可能なハードディスクやメモリーに保存するのも良い。

請求の範囲

[1] 暗号化時に暗号化パスワードを設定してファイルを暗号化して暗号化ファイルを作成すると共に、既に暗号化されている暗号化ファイルを復号化する際、当該ファイルの暗号化時に設定した暗号化パスワードと等価な復号化パスワードが入力されることによって復号化を許可し元のファイルを復元する暗号化及び復号化システムにおいて、

前記暗号化パスワードは、1つのファイルに対して少なくとも1つ以上設定され、かつ、前記暗号化パスワードはシステム内に登録されており、かつ、ユーザーの属するグループ毎に異なる複数の前記暗号化パスワードがシステム内に登録されていて、ユーザーは、ファイルの暗号化のために前記複数の暗号化パスワードの内、少なくとも1つを選択する手段と、

他のユーザーと暗号化されたデータを共有するために、当該システムに登録されている1つ又は複数の暗号化パスワード及び該暗号化パスワードに等価な復号化パスワードが設定されている暗号化及び復号化システムを、当該他のユーザーのコンピュータにインストールするためのインストール用ソフトウエアを作成する手段と、を有する暗号化及び復号化システム。

[2] 暗号化時に暗号化パスワードを設定してファイルを暗号化して暗号化ファイルを作成すると共に、既に暗号化されている暗号化ファイルを復号化する際、当該ファイルの暗号化時に設定した暗号化パスワードと等価な復号化パスワードが入力されることによって復号化を許可し元のファイルを復元する暗号化及び復号化システムにおいて、

前記暗号化パスワードは、1つのファイルに対して少なくとも1つ以上設定され、かつ、前記暗号化パスワードはシステム内に登録されており、かつ、ユーザーの属するグループ毎に異なる複数の前記暗号化パスワードがシステム内に登録されていて、ユーザーは、ファイルの暗号化のために前記複数の暗号化パスワードの内、少なくとも1つを選択する手段と、

他のユーザーと暗号化されたデータを共有するために、当該システムに登録されている暗号化パスワード及び該暗号化パスワードに等価な復号化パスワードが設定さ

れている1つ又は複数のグループを、当該他のユーザーが使用している同等のシステムに登録するための登録用ソフトウエアを作成する手段と、を有する暗号化及び復号化システム。

[3] 少なくとも1つ以上の前記暗号化パスワードは、暗号化及び復号化ソフトウエアをインストールする際に、システム内に登録される請求項1または2に記載の暗号化及び復号化システム。

[4] 前記暗号化ファイルを復号化する際の前記復号化パスワードの入力において、暗号化パスワードに等価な復号化パスワードはパスワード記憶欄に予め記憶させておくことが可能な請求項1から3のいずれかに記載の暗号化及び復号化システム。

[5] 前記暗号化パスワードは、前記システムのシリアル番号である請求項1から3のいずれかに記載の暗号化及び復号化システム。

[6] ユーザーが指定した任意の時やシステム終了時に、該システム内に登録されている各種パスワードの一部又は全部は暗号化して保存する、請求項1から5のいずれかに記載の暗号化及び復号化システム。

[7] 該システム内に登録されている各種パスワードの一部又は全部は暗号化して保存し、必要な時に、各種パスワード復号化用パスワードを入力して各種パスワードを復号化して使用する請求項1から6のいずれかに記載の暗号化及び復号化システム。

[8] 前記各種パスワード復号化用パスワードは、当該システムの立ち上げのために入力する起動パスワードと同じであり、該システム起動時に前記起動パスワードの入力によって前記登録されている各種パスワードを復号化して使用する請求項6または7に記載の暗号化及び復号化システム。

[9] 前記各種パスワードを復号化するに際し、前記各種パスワード復号化用パスワードの入力の累積間違い回数が規定回数を越えると、登録されている各種パスワードの全てを消去する請求項6から8のいずれかに記載の暗号化及び復号化システム。

[10] 入力された前記復号化パスワードが、暗号化時に選択された暗号化パスワードと等価か判定され、イエスの場合、復号化ファイルを出力し、かつ、復号化パスワードの累積入力間違い回数が規定回数を越えると、暗号化データを削除し、或いは登録されている当該暗号化データに関連するパスワードを消去する請求項1または2に記

載の暗号化及び復号化システム。

[11] 暗号化時に暗号化パスワードを設定してファイルを暗号化して暗号化ファイルを作成すると共に、既に暗号化されている暗号化ファイルを復号化する際、当該ファイルの暗号化時に設定した暗号化パスワードと等価な復号化パスワードが入力されることによって復号化を許可し元のファイルを復元する暗号化及び復号化方法において、

前記暗号化パスワードは、1つのファイルに対して少なくとも1つ以上設定され、かつ、前記暗号化パスワードはシステム内に登録されており、かつ、ユーザーの属するグループ毎に異なる複数の前記暗号化パスワードがシステム内に登録されていて、ユーザーは、ファイルの暗号化のために前記複数の暗号化パスワードの内、少なくとも1つを選択し、

他のユーザーと暗号化されたデータを共有するために、当該システムに登録されている1つ又は複数の暗号化パスワード及び該暗号化パスワードに等価な復号化パスワードが設定されている暗号化及び復号化システムを、当該他のユーザーのコンピュータにインストールするためのインストール用ソフトウエアを作成する、ことから成る暗号化及び復号化方法。

[12] 暗号化時に暗号化パスワードを設定してファイルを暗号化して暗号化ファイルを作成すると共に、既に暗号化されている暗号化ファイルを復号化する際、当該ファイルの暗号化時に設定した暗号化パスワードと等価な復号化パスワードが入力されることによって復号化を許可し元のファイルを復元する暗号化及び復号化方法において、

前記暗号化パスワードは、1つのファイルに対して少なくとも1つ以上設定され、かつ、前記暗号化パスワードはシステム内に登録されており、かつ、ユーザーの属するグループ毎に異なる複数の前記暗号化パスワードがシステム内に登録されていて、ユーザーは、ファイルの暗号化のために前記複数の暗号化パスワードの内、少なくとも1つを選択し、

他のユーザーと暗号化されたデータを共有するために、当該システムに登録されている暗号化パスワード及び該暗号化パスワードに等価な復号化パスワードが設定されている1つ又は複数のグループを、当該他のユーザーが使用している同等のシステムに登録するための登録用ソフトウエアを作成する、ことから成る暗号化及び復号

化方法。

[13] 少なくとも1つ以上の前記暗号化パスワードは、暗号化及び復号化ソフトウエアをインストールする際に、システム内に登録される請求項11または12に記載の暗号化及び復号化方法。

[14] 暗号化時に暗号化パスワードを設定してファイルを暗号化して暗号化ファイルを作成すると共に、既に暗号化されている暗号化ファイルを復号化する際、当該ファイルの暗号化時に設定した暗号化パスワードと等価な復号化パスワードが入力されることによって復号化を許可し元のファイルを復元する暗号化及び復号化プログラムにおいて、

前記暗号化パスワードは、1つのファイルに対して少なくとも1つ以上設定され、かつ、前記暗号化パスワードはシステム内に登録されており、かつ、ユーザーの属するグループ毎に異なる複数の前記暗号化パスワードがシステム内に登録されていて、ユーザーは、ファイルの暗号化のために前記複数の暗号化パスワードの内、少なくとも1つを選択し、

他のユーザーと暗号化されたデータを共有するために、当該システムに登録されている1つ又は複数の暗号化パスワード及び該暗号化パスワードに等価な復号化パスワードが設定されている暗号化及び復号化システムを、当該他のユーザーのコンピュータにインストールするためのインストール用ソフトウエアを作成する、ことから成る各手順を実行する暗号化及び復号化プログラム。

[15] 暗号化時に暗号化パスワードを設定してファイルを暗号化して暗号化ファイルを作成すると共に、既に暗号化されている暗号化ファイルを復号化する際、当該ファイルの暗号化時に設定した暗号化パスワードと等価な復号化パスワードが入力されることによって復号化を許可し元のファイルを復元する暗号化及び復号化プログラムにおいて、

前記暗号化パスワードは、1つのファイルに対して少なくとも1つ以上設定され、かつ、前記暗号化パスワードはシステム内に登録されており、かつ、ユーザーの属するグループ毎に異なる複数の前記暗号化パスワードがシステム内に登録されていて、ユーザーは、ファイルの暗号化のために前記複数の暗号化パスワードの内、少なくと

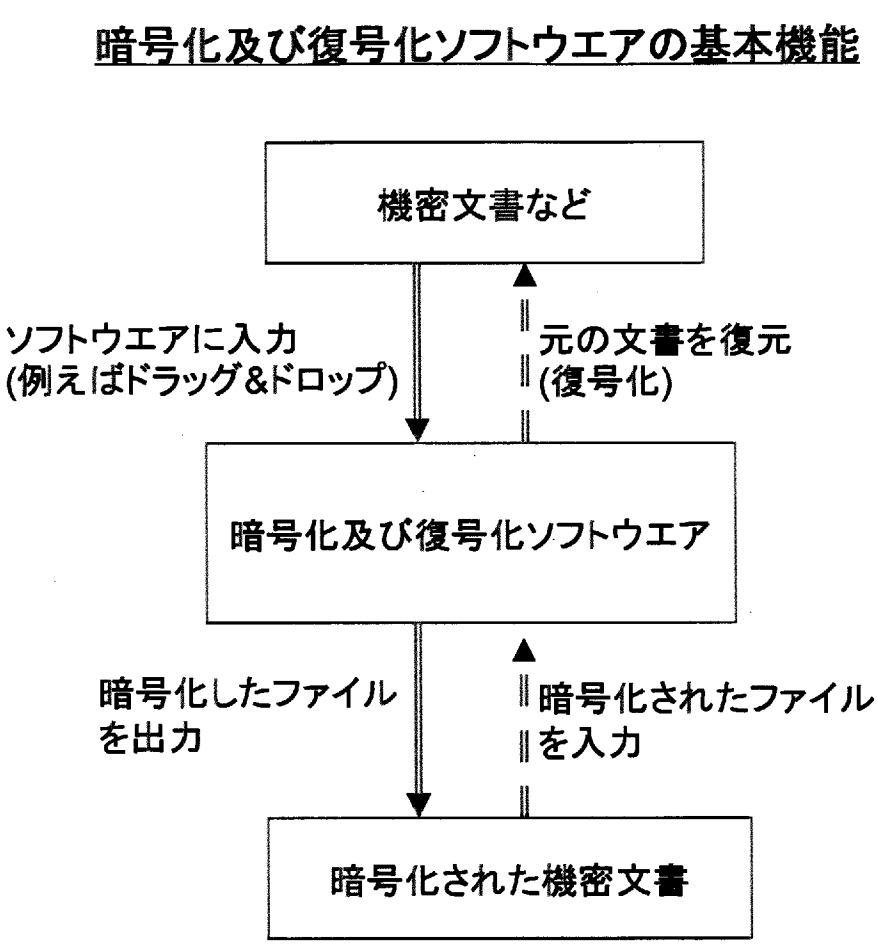
も1つを選択し、

他のユーザーと暗号化されたデータを共有するために、当該システムに登録されている暗号化パスワード及び該暗号化パスワードに等価な復号化パスワードが設定されている1つ又は複数のグループを、当該他のユーザーが使用している同等のシステムに登録するための登録用ソフトウエアを作成する、ことから成る各手順を実行する暗号化及び復号化プログラム。

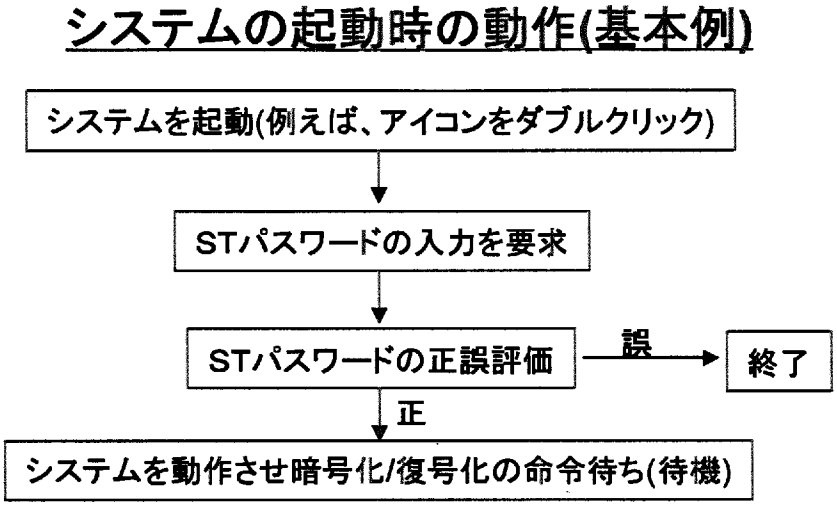
[16] 少なくとも1つ以上の前記暗号化パスワードは、暗号化及び復号化ソフトウエアをインストールする際に、システム内に登録される請求項14または15に記載の暗号化及び復号化プログラム。

WO 2008/132869 PCT/JP2008/053593

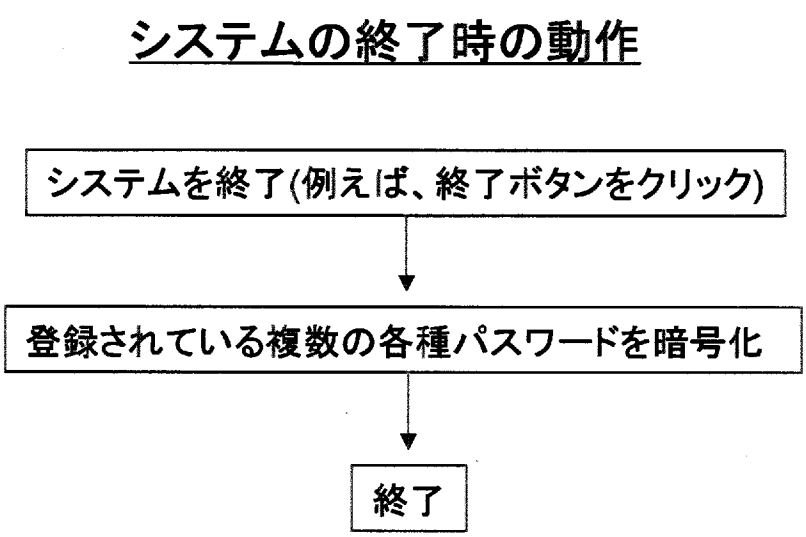
[図1]



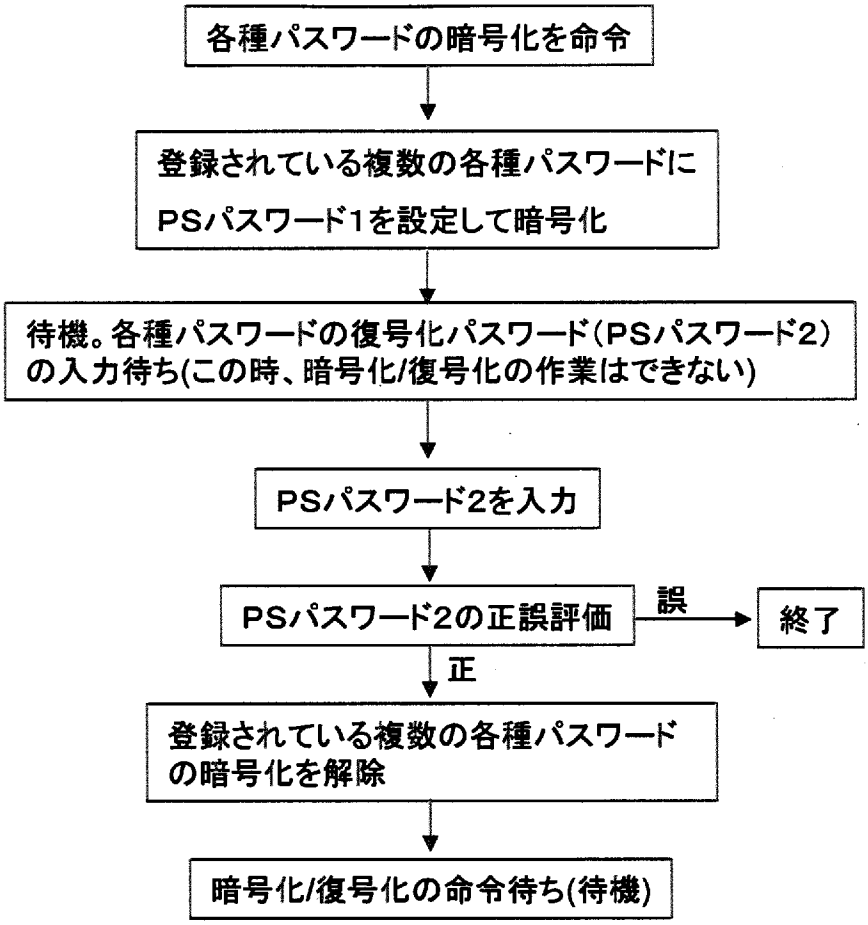
[図2]



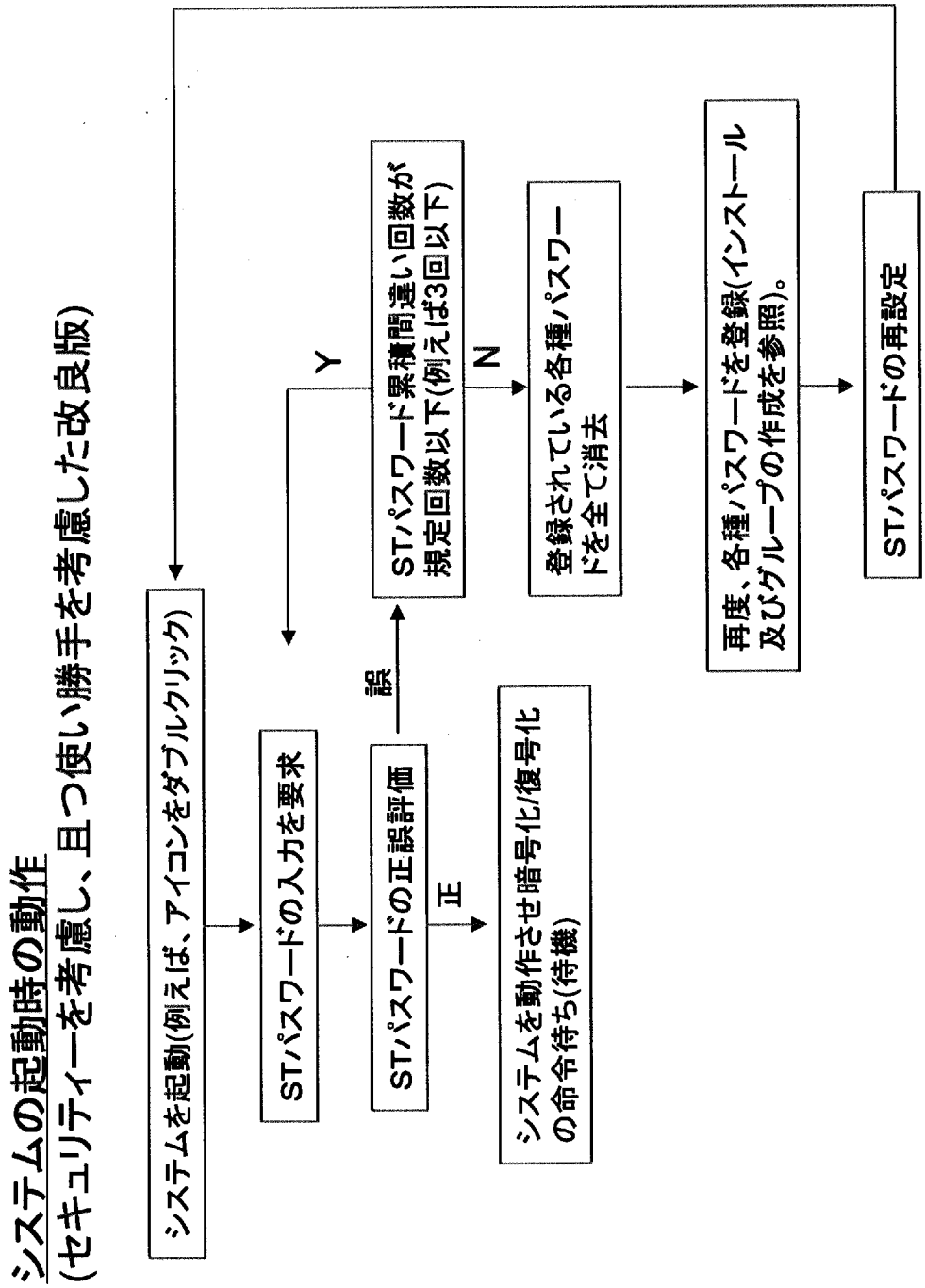
[図3]


システムの終了時の動作
システムを終了(例えば、終了ボタンをクリック)
登録されている複数の各種パスワードを暗号化
終了

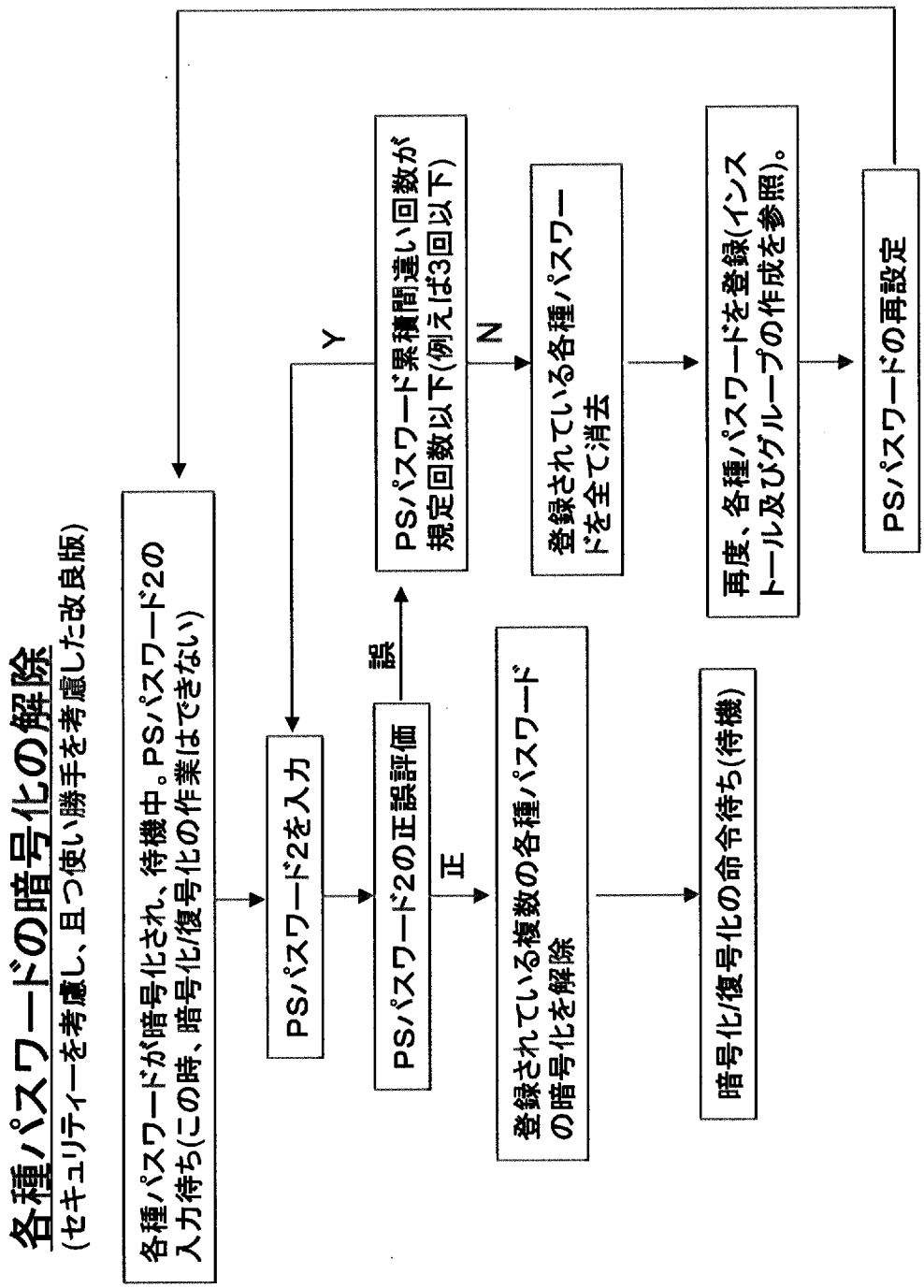
[図4]


各種パスワードの暗号化・復号化
各種パスワードの暗号化を命令
登録されている複数の各種パスワードに
PSパスワード1を設定して暗号化
待機。各種パスワードの復号化パスワード(PSパスワード2)
の入力待ち(この時、暗号化/復号化の作業はできない)
PSパスワード2を入力
PSパスワード2の正誤評価
誤
終了
正
登録されている複数の各種パスワード
の暗号化を解除
暗号化/復号化の命令待ち(待機)

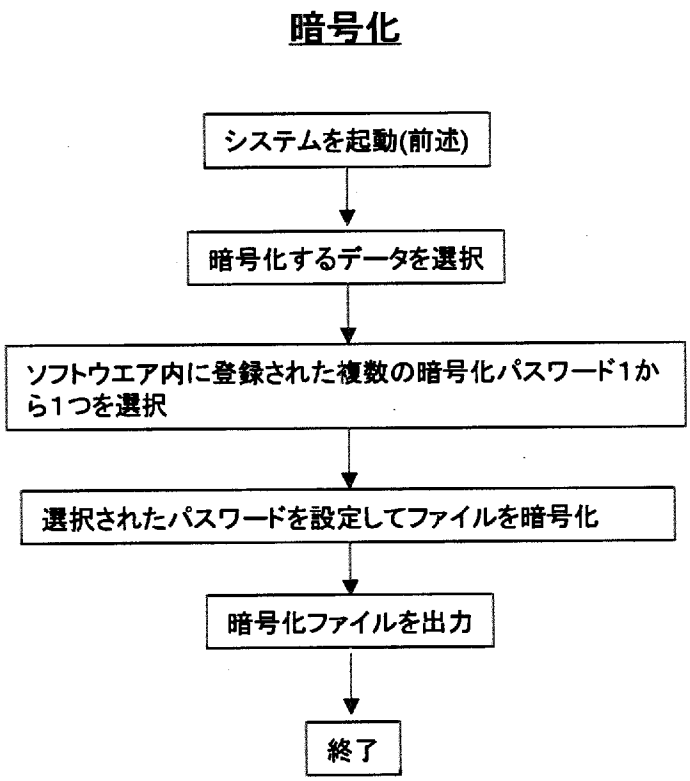
[図5]


システムの起動時の動作
(セキュリティーを考慮し、且つ使い勝手を考慮した改良版)
システムを起動(例えば、アイコンをダブルクリック)
STパスワードの入力を要求
STパスワードの正誤評価
誤
正
Y
STパスワード累積間違い回数が規定回数以下(例えば3回以下)
N
システムを動作させ暗号化/復号化の命令待ち(待機)
登録されている各種パスワードを全て消去
再度、各種パスワードを登録(インストール及びグループの作成を参照)。
STパスワードの再設定

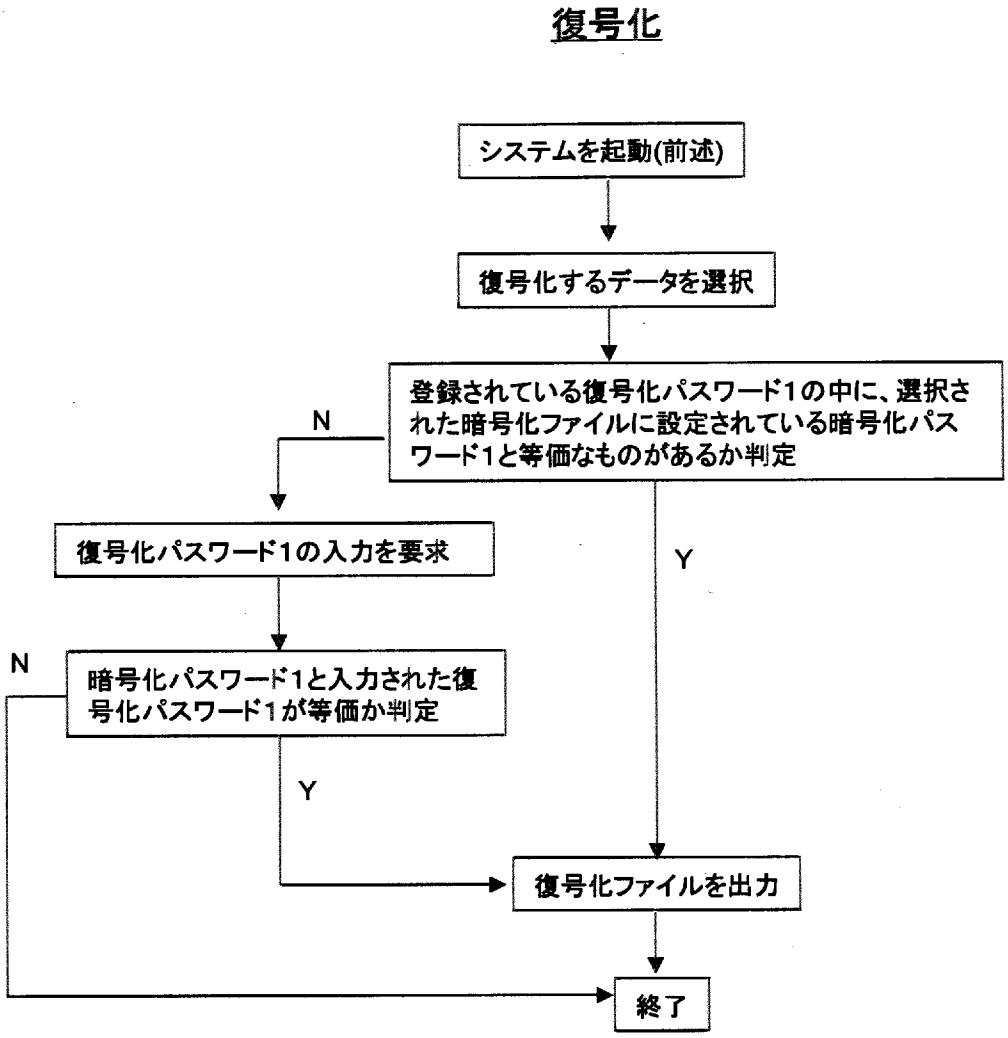
[図6]


各種パスワードの暗号化の解除
(セキュリティーを考慮し、且つ使い勝手を考慮した改良版)
各種パスワードが暗号化され、待機中。PSパスワード2の入力待ち(この時、暗号化/復号化の作業はできない)
PSパスワード2を入力
PSパスワード2の正誤評価
誤
正
Y
PSパスワード累積間違い回数が規定回数以下(例えば3回以下)
N
登録されている各種パスワードを全て消去
PSパスワードの再設定
再度、各種パスワードを登録(インストール及びグループの作成を参照)。
登録されている複数の各種パスワードの暗号化を解除
暗号化/復号化の命令待ち(待機)

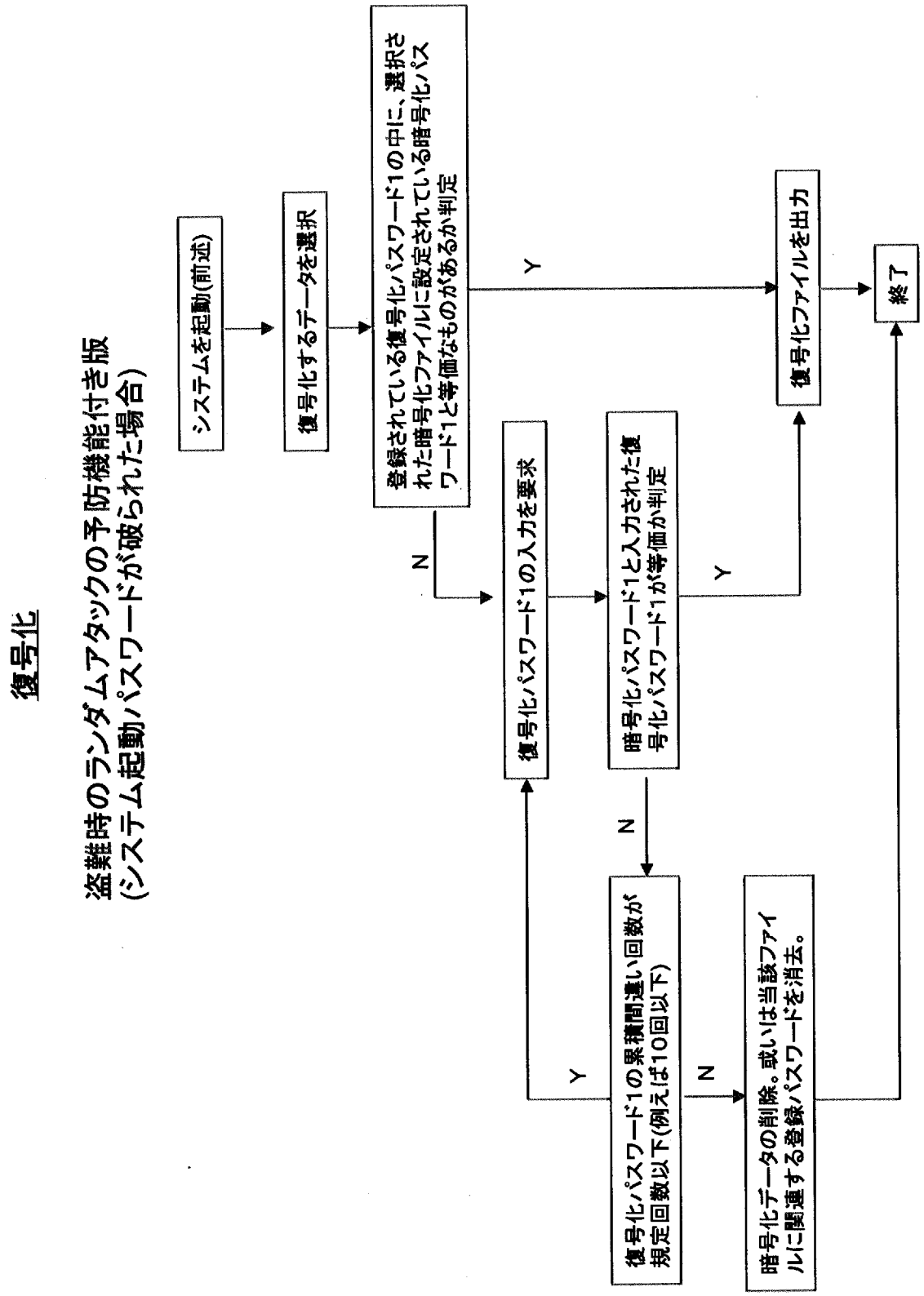
[図7]


暗号化
システムを起動(前述)
暗号化するデータを選択
ソフトウエア内に登録された複数の暗号化パスワード1から1つを選択
選択されたパスワードを設定してファイルを暗号化
暗号化ファイルを出力
終了

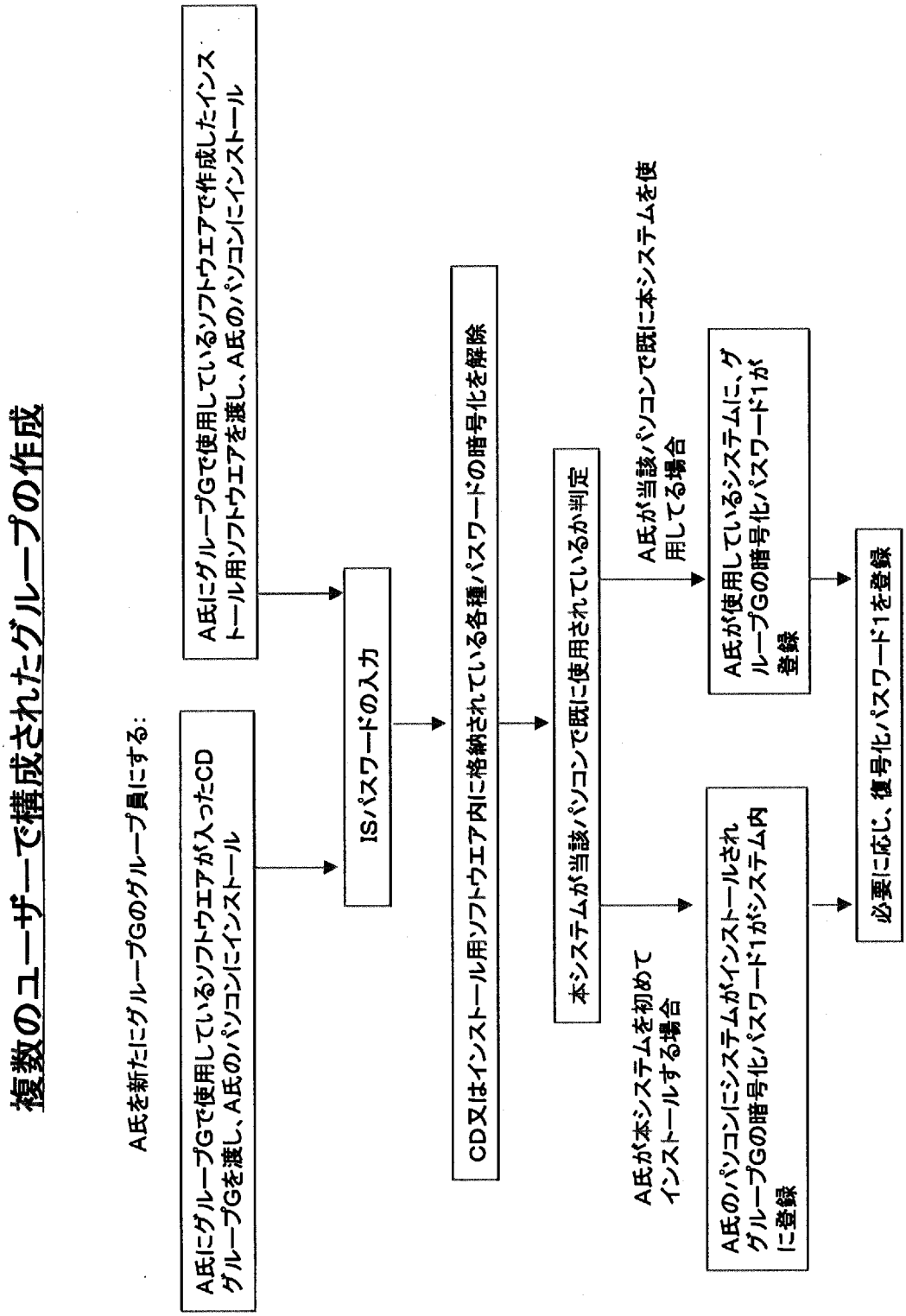
[図8]


復号化
システムを起動(前述)
復号化するデータを選択
登録されている復号化パスワード1の中に、選択された暗号化ファイルに設定されている暗号化パスワード1と等価なものがあるか判定
N
Y
復号化パスワード1の入力を要求
N
暗号化パスワード1と入力された復号化パスワード1が等価か判定
Y
復号化ファイルを出力
終了

[図9]


復号化
盗難時のランダムアタックの予防機能付き版
(システム起動パスワードが破られた場合)
システムを起動(前述)
復号化するデータを選択
登録されている復号化パスワード1の中に、選択された暗号化ファイルに設定されている暗号化パスワード1と等価なものがあるか判定
Y
N
復号化パスワード1の入力を要求
暗号化パスワード1と入力された復号化パスワード1が等価か判定
Y
N
復号化ファイルを出力
終了
復号化パスワード1の累積間違い回数が規定回数以下(例えば10回以下)
Y
N
暗号化データの削除。或いは当該ファイルに関連する登録パスワードを消去。

[図10]


複数のユーザーで構成されたグループの作成
A氏を新たにグループGのグループ員にする:
A氏にグループGで使用しているソフトウエアが入ったCD
グループGを渡し、A氏のパソコンにインストール
A氏にグループGで使用しているソフトウエアで作成したインス
トール用ソフトウエアを渡し、A氏のパソコンにインストール
ISパスワードの入力
CD又はインストール用ソフトウエア内に格納されている各種パスワードの暗号化を解除
本システムが当該パソコンで既に使用されているか判定
A氏が本システムを初めて
インストールする場合
A氏のパソコンにシステムがインストールされ
グループGの暗号化パスワード1がシステム内
に登録
A氏が当該パソコンで既に本システムを使
用してる場合
A氏が使用しているシステムに、グ
ループGの暗号化パスワード1が
登録
必要に応じ、復号化パスワード1を登録

[図11]

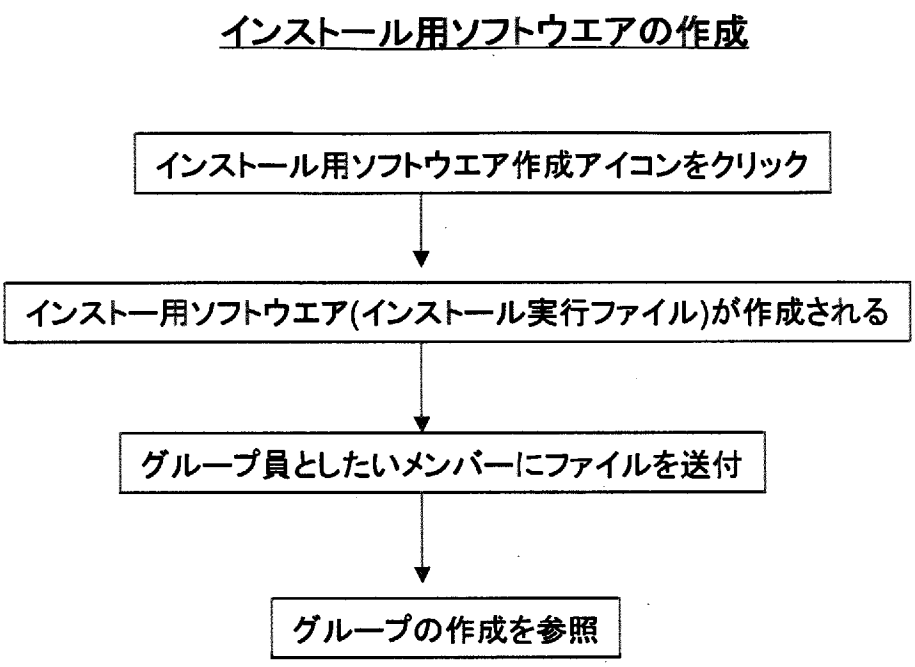
グループ表示例とグループの追加

グループ名	ユーザー パスワード登録	ユーザーパスワード
個人使用	✓	985whq
○○株式会社	✓	54egae
××サークル		
△△研究チーム	✓	6pmea3

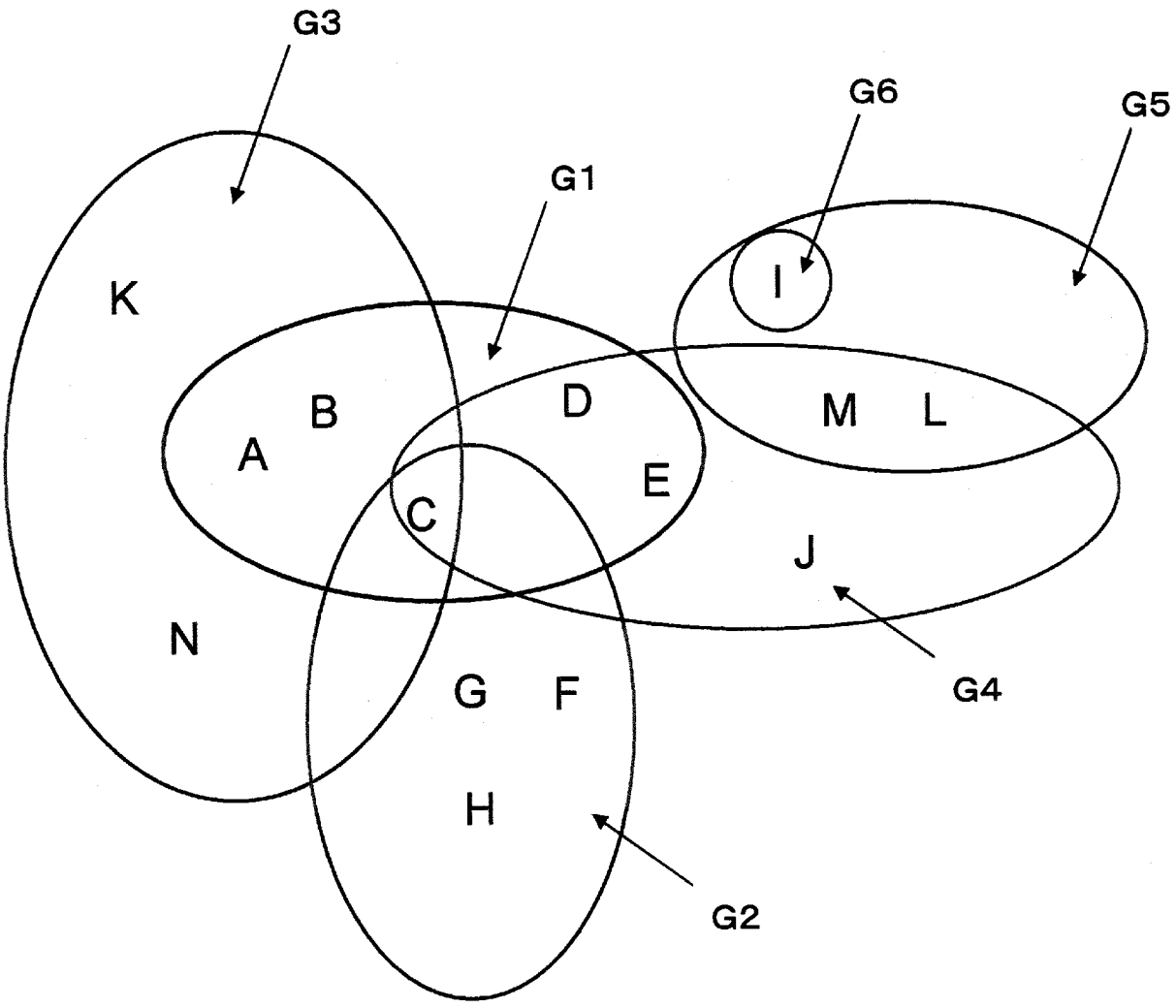
↓○□グループを追加すると

グループ名	ユーザー パスワード登録	ユーザーパスワード
個人使用	✓	985whq
○○株式会社	✓	54egae
××サークル		
△△研究チーム	✓	6pmea3
○□グループ	✓	674tmq

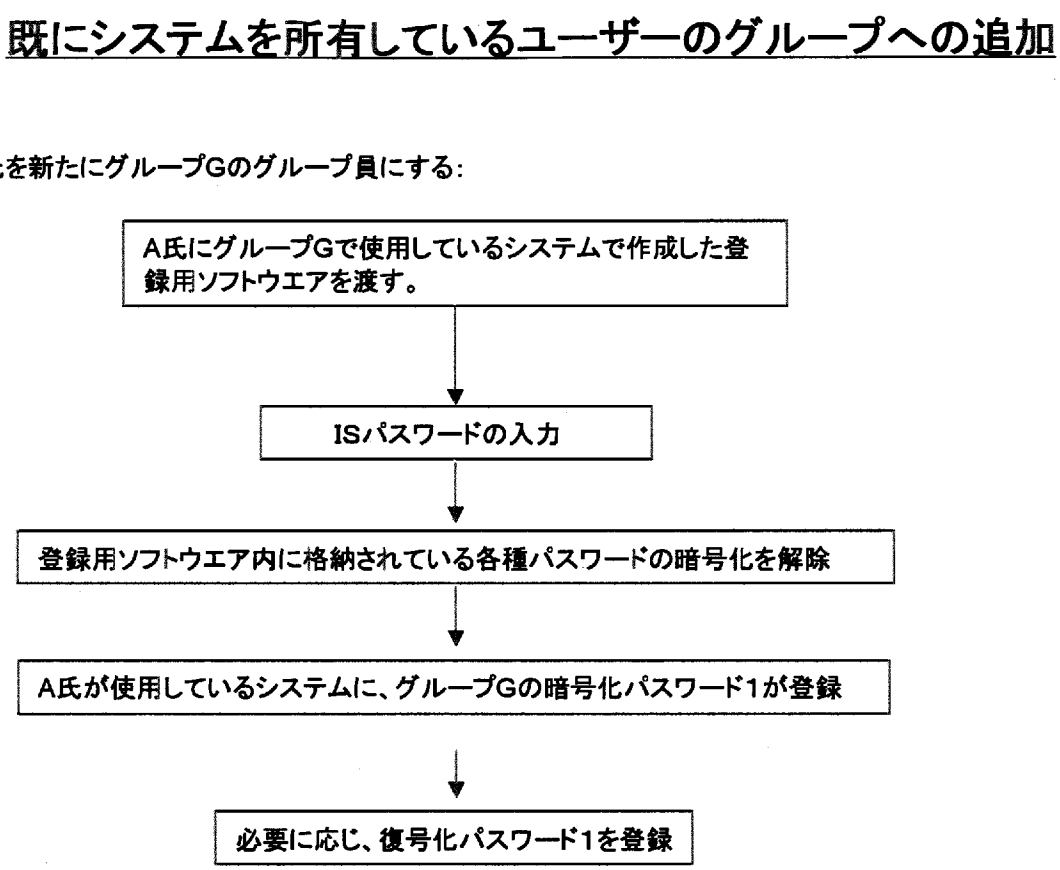
[図12]


インストール用ソフトウエアの作成
インストール用ソフトウエア作成アイコンをクリック
インストー用ソフトウエア(インストール実行ファイル)が作成される
グループ員としたいメンバーにファイルを送付
グループの作成を参照

[図13]


G3
G6
G5
G1
K
I
B
D
A
M
L
E
C
J
N
G4
G
F
H
G2

[図14]


既にシステムを所有しているユーザーのグループへの追加
A氏を新たにグループGのグループ員にする:
A氏にグループGで使用しているシステムで作成した登録用ソフトウエアを渡す。
ISパスワードの入力
登録用ソフトウエア内に格納されている各種パスワードの暗号化を解除
A氏が使用しているシステムに、グループGの暗号化パスワード1が登録
必要に応じ、復号化パスワード1を登録

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/053593

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/24(2006.01)i, *G06F12/00*(2006.01)i, *G09C1/00*(2006.01)i, *H04L9/32*(2006.01)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)
G06F21/24, G06F12/00, G09C1/00, H04L9/32

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	1996-2008
Kokai Jitsuyo Shinan Koho	1971-2008	Toroku Jitsuyo Shinan Koho	1994-2008

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	JP 2004-072151 A (Mitsubishi Electric Corp.), 04 March, 2004 (04.03.04), Description, Par. Nos. [0032] to [0060], [0074] to [0079]; Figs. 1 to 4, 7 to 12 (Family: none)	1-16
Y	JP 2003-216037 A (Yazaki Corp.), 30 July, 2003 (30.07.03), Description, Par. Nos. [0149] to [0158], [0174]; Figs. 19 to 21 & JP 2007-104731 A & JP 2007-104732 A & US 2003/0095659 A1 & US 2007/0019811 A1 & EP 1313259 A2	1-16

☒ 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 28 May, 2008 (28.05.08)	Date of mailing of the international search report 10 June, 2008 (10.06.08)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2008/053593

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 06-051958 A (Fuji Xerox Co., Ltd.), 25 February, 1994 (25.02.94), Description, Par. Nos. [0009] to [0023]; Fig. 1 (Family: none)	1-16
A	JP 2000-207175 A (NEC Corp.), 28 July, 2000 (28.07.00), Description, Par. Nos. [0020] to [0038]; Fig. 1 (Family: none)	1-16
Y	JP 2000-099385 A (Toshiba Corp.), 07 April, 2000 (07.04.00), Description, Par. Nos. [0010] to [0012], [0038] to [0039] (Family: none)	2,12,15
Y	JP 2005-209181 A (Sorun Corp.), 04 August, 2005 (04.08.05), Description, Par. Nos. [0035], [0117], [0135]; Figs. 1 to 21 (Family: none)	5
A	JP 2006-155382 A (Nomura Research Institute, Ltd.), 15 June, 2006 (15.06.06), Description, Par. No. [0070] (Family: none)	9-10
A	JP 2001-016655 A (Advanced Mobile Telecommunications Security Technology Research Laboratories Co., Ltd.), 19 January, 2001 (19.01.01), Description, Par. Nos. [0016], [0037] (Family: none)	10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００８／０５３５９３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/24(2006.01)i, G06F12/00(2006.01)i, G09C1/00(2006.01)i, H04L9/32(2006.01)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.　G06F21/24, G06F12/00, G09C1/00, H04L9/32

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	１９７１－２００８年
日本国実用新案登録公報	１９９６－２００８年
日本国登録実用新案公報	１９９４－２００８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	関連する請求の範囲の番号
Y	JP 2004-072151 A (三菱電機株式会社) 2004.03.04, 明細書第0032段落乃至第0060段落、第0074段落乃至第0079段落、図面図1乃至図4、図7乃至図12 (ファミリーなし)	1-16
Y	JP 2003-216037 A (矢崎総業株式会社) 2003.07.30, 明細書第0149段落乃至第0158段落、第0174段落、図面図19乃至図21 & JP 2007-104731 A & JP 2007-104732 A & US 2003/0095659 A1 & US 2007/0019811 A1 & EP 1313259 A2	1-16

☑　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 ２８．０５．２００８	国際調査報告の発送日 １０．０６．２００８
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　３９８３ 岸野　徹 電話番号　０３－３５８１－１１０１　内線　３５４６

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００７年４月）

Ｃ（続き）．　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	関連する請求の範囲の番号
A	JP 06-051958 A(富士ゼロックス株式会社)1994.02.25,明細書第0009段落乃至第0023段落、図面図1 （ファミリーなし）	1-16
A	JP 2000-207175 A（日本電気株式会社）2000.07.28,明細書第0020段落乃至第0038段落、図面図1 （ファミリーなし）	1-16
Y	JP 2000-099385 A（株式会社東芝）2000.04.07,明細書第0010段落乃至第0012段落、第0038段落乃至第0039段落 （ファミリーなし）	2,12,15
Y	JP 2005-209181 A（ソラン株式会社）2005.08.04,明細書第0035段落,第0117段落、第0135段落、図面図1乃至図21 （ファミリーなし）	5
A	JP 2006-155382 A（株式会社野村総合研究所）2006.06.15,明細書第0070段落 （ファミリーなし）	9-10
A	JP 2001-016655 A（株式会社高度移動通信セキュリティ技術研究所）2001.01.19,明細書第0016段落、第0037段落 （ファミリーなし）	10