(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4305481号
(P4305481)
(45)発行日　平成21年7月29日(2009.7.29)　(24)登録日　平成21年5月15日(2009.5.15)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 15/00 330B
H04L 9/32 (2006.01)　　H04L 9/00 673A

請求項の数 6　(全 21 頁)

(21)出願番号　特願2006-232001(P2006-232001)
(22)出願日　平成18年8月29日(2006.8.29)
(65)公開番号　特開2008-59033(P2008-59033A)
(43)公開日　平成20年3月13日(2008.3.13)
審査請求日　平成19年8月3日(2007.8.3)

(73)特許権者　000005267
ブラザー工業株式会社
愛知県名古屋市瑞穂区苗代町１５番１号
(74)代理人　110000110
特許業務法人快友国際特許事務所
(72)発明者　石本　関
愛知県名古屋市瑞穂区苗代町１５番１号
ブラザー工業株式会社内

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】通信システムと管理装置と情報処理装置

(57)【特許請求の範囲】
【請求項１】
情報処理装置と、
ユーザによって入力された新データを情報処理装置に出力することによって、情報処理装置に記憶されている旧データを更新することができる管理装置とを備える通信システムであり、
管理装置は、
情報処理装置から出力されたチャレンジデータを入力するチャレンジ入力手段と、
旧データを入力する管理装置側旧データ入力手段と、
新データを入力する管理装置側新データ入力手段と、
（１）チャレンジ入力手段に入力されたチャレンジデータを少なくとも２つの分割チャレンジデータに分割し、（２）管理装置側新データ入力手段に入力された新データを少なくとも２つの分割新データに分割し、（３）所定のデータ量のブロック毎に少なくとも１つの分割チャレンジデータと少なくとも１つの分割新データの両方が含まれるように組合せデータを作成し、（４）その組合せデータを、管理装置側旧データ入力手段に入力された旧データをキーとして、ブロック単位で暗号化する暗号化手段と、
暗号化手段によって暗号化された前記組合せデータを情報処理装置に出力する新データ出力手段とを有し、
情報処理装置は、
旧データを記憶する旧データ記憶手段と、

チャレンジデータを管理装置に出力するチャレンジ出力手段と、
チャレンジ出力手段から出力されたチャレンジデータを記憶するチャレンジ記憶手段と、
管理装置から出力された暗号化された前記組合せデータを入力する処理装置側新データ入力手段と、
処理装置側新データ入力手段に入力された暗号化された前記組合せデータを、旧データ記憶手段に記憶されている旧データをキーとしてブロック単位で復号し、各ブロックに含まれる分割チャレンジデータからチャレンジデータを再現するとともに、各ブロックに含まれる分割新データから新データを再現する復号手段と、
復号手段によって再現されたチャレンジデータとチャレンジ記憶手段に記憶されているチャレンジデータとを比較し、両者が一致した場合は、旧データ記憶手段に記憶されている旧データを復号手段によって再現された新データに更新し、両者が一致しない場合は、旧データ記憶手段に記憶されている旧データを更新することを禁止する更新手段とを有する
ことを特徴とする通信システム。
【請求項２】
旧データ記憶手段に記憶される前記旧データは、要約化された旧データであり、
チャレンジ出力手段によって出力される前記チャレンジデータは、要約化されたチャレンジデータであり、
チャレンジ記憶手段によって記憶される前記チャレンジデータは、前記要約化されたチャレンジデータであり、
チャレンジ入力手段に入力されるチャレンジデータは、前記要約化されたチャレンジデータであり、
暗号化手段は、管理装置側旧データ入力手段に入力された旧データから要約化された旧データを作成し、管理装置側新データ入力手段に入力された新データから要約化された新データを作成し、
暗号化手段によって分割される前記チャレンジデータは、チャレンジ入力手段に入力された前記要約化されたチャレンジデータであり、
暗号化手段によって分割される前記新データは、暗号化手段によって作成された前記要約化された新データであり、
暗号化手段が暗号化キーとして利用する前記旧データは、暗号化手段によって作成された前記要約化された旧データであり、
復号手段が復号化キーとして利用する前記旧データは、旧データ記憶手段に記憶されている前記要約化された旧データである
ことを特徴とする請求項１の通信システム。
【請求項３】
情報処理装置と通信可能に接続されて利用されるとともに、ユーザによって入力された新データを情報処理装置に出力することによって、情報処理装置に記憶されている旧データを更新することができる管理装置であり、
情報処理装置から出力されたチャレンジデータを入力するチャレンジ入力手段と、
旧データを入力する管理装置側旧データ入力手段と、
新データを入力する管理装置側新データ入力手段と、
（１）チャレンジ入力手段に入力されたチャレンジデータを少なくとも２つの分割チャレンジデータに分割し、（２）管理装置側新データ入力手段に入力された新データを少なくとも２つの分割新データに分割し、（３）所定のデータ量のブロック毎に少なくとも１つの分割チャレンジデータと少なくとも１つの分割新データの両方が含まれるように組合せデータを作成し、（４）その組合せデータを、管理装置側旧データ入力手段に入力された旧データをキーとして、ブロック単位で暗号化する暗号化手段と、
暗号化手段によって暗号化された前記組合せデータを情報処理装置に出力する新データ出力手段と

を備える管理装置。
【請求項４】
管理装置と通信可能に接続されて利用されるとともに、自身が記憶している旧データをユーザによって管理装置に入力された新データに更新する情報処理装置であり、
チャレンジデータを管理装置に出力するチャレンジ出力手段と、
チャレンジ出力手段から出力されたチャレンジデータを記憶するチャレンジ記憶手段と、
旧データを記憶する旧データ記憶手段と、
管理装置から出力された暗号化された組合せデータを入力する処理装置側新データ入力手段と、
処理装置側新データ入力手段に入力された暗号化された前記組合せデータを、旧データ記憶手段に記憶されている旧データをキーとしてブロック単位で復号し、各ブロックの分割チャレンジデータからチャレンジデータを再現するとともに各ブロックの分割新データから新データを再現する復号手段と、
復号手段によって再現されたチャレンジデータとチャレンジ記憶手段に記憶されているチャレンジデータとを比較し、両者が一致した場合は、旧データ記憶手段に記憶されている旧データを復号手段によって再現された新データに更新し、両者が一致しない場合は、旧データ記憶手段に記憶されている旧データを更新することを禁止する更新手段と
を備え、
暗号化された前記組合せデータは、管理装置が、（１）管理装置に入力されたチャレンジデータを少なくとも２つの分割チャレンジデータに分割し、（２）管理装置に入力された新データを少なくとも２つの分割新データに分割し、（３）所定のデータ量のブロック毎に少なくとも１つの分割チャレンジデータと少なくとも１つの分割新データの両方が含まれるように組合せデータを作成し、（４）その組合せデータを、管理装置に入力された旧データをキーとして、ブロック単位で暗号化することによって作成されたものである
ことを特徴とする情報処理装置。
【請求項５】
情報処理装置に記憶されている旧データをユーザによって入力された新データに更新させる管理装置を実現するためのコンピュータプログラムであり、
その管理装置に搭載されるコンピュータに、以下の各工程、即ち、
情報処理装置から出力されたチャレンジデータを入力するチャレンジ入力工程と、
旧データを入力する管理装置側旧データ入力工程と、
新データを入力する管理装置側新データ入力工程と、
（１）チャレンジ入力工程で入力されたチャレンジデータを少なくとも２つの分割チャレンジデータに分割し、（２）管理装置側新データ入力工程で入力された新データを少なくとも２つの分割新データに分割し、（３）所定のデータ量のブロック毎に少なくとも１つの分割チャレンジデータと少なくとも１つの分割新データの両方が含まれるように組合せデータを作成し、（４）その組合せデータを、管理装置側旧データ入力工程で入力された旧データをキーとして、ブロック単位で暗号化する暗号化工程と、
暗号化工程で暗号化された前記組合せデータを情報処理装置に出力する新データ出力工程と
を実行させるコンピュータプログラム。
【請求項６】
自身が記憶している旧データをユーザによって管理装置に入力された新データに更新する情報処理装置を実現するためのコンピュータプログラムであり、
その情報処理装置に搭載されるコンピュータに、以下の各工程、即ち、
旧データを記憶する旧データ記憶工程と、
チャレンジデータを管理装置に出力するチャレンジ出力工程と、
チャレンジ出力工程で出力されたチャレンジデータを記憶するチャレンジ記憶工程と、
管理装置から出力された暗号化された組合せデータを入力する処理装置側新データ入力

工程と、
処理装置側新データ入力工程で入力された暗号化された前記組合せデータを、旧データ記憶工程で記憶された旧データをキーとしてブロック単位で復号し、各ブロックの分割チャレンジデータからチャレンジデータを再現するとともに各ブロックの分割新データから新データを再現する復号工程と、
復号工程で再現されたチャレンジデータとチャレンジ記憶工程で記憶されたチャレンジデータとを比較し、両者が一致した場合は、旧データ記憶工程で記憶された旧データを復号工程で再現された新データに更新し、両者が一致しない場合は、旧データ記憶工程で記憶された旧データを更新することを禁止する更新工程と
を実行させ、
暗号化された前記組合せデータは、管理装置が、（１）管理装置に入力されたチャレンジデータを少なくとも２つの分割チャレンジデータに分割し、（２）管理装置に入力された新データを少なくとも２つの分割新データに分割し、（３）所定のデータ量のブロック毎に少なくとも１つの分割チャレンジデータと少なくとも１つの分割新データの両方が含まれるように組合せデータを作成し、（４）その組合せデータを、管理装置に入力された旧データをキーとして、ブロック単位で暗号化することによって作成されたものである
ことを特徴とするコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置と、それと通信可能に接続されている管理装置とを備える通信システムに関する。特に、ユーザによって管理装置に入力された新データを情報処理装置に出力することによって、情報処理装置に記憶されている旧データを更新することができる通信システムに関する。
【背景技術】
【０００２】
例えば、プリンタとＰＣがローカルエリアネットワーク（ＬＡＮ）によって通信可能に接続されている通信システムが知られている。下記の特許文献１には、このような通信システムの一例が開示されている。ユーザは、ＰＣを操作することによって、プリンタに対して指示を送ることができる。例えば、ユーザは、ＰＣを操作することによって、プリンタの各種設定を変更することができる。
【０００３】
プリンタの誤作動等を防止するために、プリンタの各種設定を変更することは管理者に限定されるべきである。特許文献１では、プリンタの各種設定を変更するＰＣにインストールされたアプリケーションソフトの起動時に、パスワードの入力を要求する。適切なパスワードが入力された場合に、このアプリケーションソフトが起動され、プリンタの各種設定を変更することが許容される。
一方において、アクセスする側のデバイスが、アクセスされる側のデバイスにパスワードを送ることによって、ユーザ認証を行なう技術が広く知られている。なお、セキュリティを向上させるためには、パスワードが定期的に変更されることが好ましい。
【０００４】
【特許文献１】特開平１１－２９６４６６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
ネットワーク通信においては、その通信中におけるセキュリティを確保する必要がある。そのため、暗号化技術が採用されている。一般的な暗号化技術では、デバイス間で通信されるデータ（上記の例ではパスワード）を暗号化するために、そのデータとは別に暗号化（復号化）のためのキーが通信される。
本発明は、暗号キーを従来にはない斬新な手法で通信することができる技術を提供する

。本発明の技術は、情報処理装置に記憶されている旧データ（旧パスワード）を、ユーザによって管理装置に入力された新データ（例えば新パスワード）に更新する通信システムにおいて好適に利用される。

【課題を解決するための手段】

【０００６】

本発明は、情報処理装置と、ユーザによって入力された新データを情報処理装置に出力することによって、情報処理装置に記憶されている旧データを更新することができる管理装置とを備える通信システムである。管理装置は、情報処理装置から出力されたチャレンジデータを入力するチャレンジ入力手段と、旧データを入力する管理装置側旧データ入力手段と、新データを入力する管理装置側新データ入力手段と、（１）チャレンジ入力手段に入力されたチャレンジデータを少なくとも２つの分割チャレンジデータに分割し、（２）管理装置側新データ入力手段に入力された新データを少なくとも２つの分割新データに分割し、（３）所定のデータ量のブロック毎に少なくとも１つの分割チャレンジデータと少なくとも１つの分割新データの両方が含まれるように組合せデータを作成し、（４）その組合せデータを、管理装置側旧データ入力手段に入力された旧データをキーとして、ブロック単位で暗号化する暗号化手段と、暗号化手段によって暗号化された前記組合せデータを情報処理装置に出力する新データ出力手段とを有する。情報処理装置は、旧データを記憶する旧データ記憶手段と、チャレンジデータを管理装置に出力するチャレンジ出力手段と、チャレンジ出力手段から出力されたチャレンジデータを記憶するチャレンジ記憶手段と、管理装置から出力された暗号化された前記組合せデータを入力する処理装置側新データ入力手段と、処理装置側新データ入力手段に入力された暗号化された前記組合せデータを、旧データ記憶手段に記憶されている旧データをキーとしてブロック単位で復号し、各ブロックに含まれる分割チャレンジデータからチャレンジデータを再現するとともに、各ブロックに含まれる分割新データから新データを再現する復号手段と、復号手段によって再現されたチャレンジデータとチャレンジ記憶手段に記憶されているチャレンジデータとを比較し、両者が一致した場合は、旧データ記憶手段に記憶されている旧データを復号手段によって再現された新データに更新し、両者が一致しない場合は、旧データ記憶手段に記憶されている旧データを更新することを禁止する更新手段とを有する。

図１を参照して、本発明の別の形態の技術を説明する。図１は、本発明の別の形態の通信システムの構成を簡単に示したものである。なお、図１は、あくまで本発明の別の形態の構成を例示するものである。図１の内容及びそれに関する以下の説明によって、本発明の技術的範囲が限定的に解釈されることはない。本発明の技術的範囲は、特許請求の範囲に記載された事項によって客観的に定められる。

通信システム２は、管理装置１０と情報処理装置２５を備える。管理装置１０は、ユーザによって入力された新データを情報処理装置２５に出力することによって、情報処理装置２５に記憶されている旧データを更新することができる。

【０００７】

管理装置１０は、管理装置側旧データ入力手段１２と管理装置側新データ入力手段１４と暗号化手段１６と新データ出力手段１８を有する。

管理装置側旧データ入力手段１２は、旧データ（例えばＤ１）を入力する。この旧データＤ１は、ユーザによって管理装置１０に過去に入力され、情報処理装置２５に記憶されたものである。管理装置１０のユーザは、旧データを記憶している。ユーザは、情報処理装置２５に記憶されている旧データＤ１を新データ（例えばＤ２）に更新する場合に、自身が記憶している旧データＤ１を管理装置１０に入力することができる。一方において、管理装置１０は、ユーザによって過去に入力された旧データＤ１を継続して記憶しておいてもよい。これによれば、ユーザは、旧データＤ１を新データＤ２に更新する場合に、旧データＤ１を管理装置１０に入力しなくてもよい。

管理装置側新データ入力手段１４は、新データＤ２を入力する。新データＤ２は、ユーザによって管理装置１０に入力される。なお、旧データ入力手段１２と新データ入力手段１４は、別体に構成されていてもよいし、一体に構成されていてもよい。

暗号化手段１６は、管理装置側新データ入力手段１２に入力された新データＤ２を、管理装置側旧データ入力手段１４に入力された旧データＤ１をキーとして暗号化する。以下では、Ｄ１をキーとして暗号化された新データＤ２をＥ（Ｄ２，Ｄ１）と表現する。

新データ出力手段１８は、暗号化手段１６によって暗号化された新データＥ（Ｄ２，Ｄ１）を情報処理装置２５に出力する。

【０００８】

情報処理装置２５は、旧データ記憶手段３０と処理装置側新データ入力手段３２と復号手段３４と更新手段３６を有する。

旧データ記憶手段３０は、旧データＤ１を記憶している。旧データＤ１は、ユーザによって管理装置１０に過去に入力されたものである。

処理装置側新データ入力手段３２は、管理装置１０から出力された暗号化された新データＥ（Ｄ２，Ｄ１）を入力する。

復号手段３４は、処理装置側新データ入力手段３２に入力された暗号化された新データＥ（Ｄ２，Ｄ１）を、旧データ記憶手段３０に記憶されている旧データＤ１をキーとして復号する。

更新手段３６は、旧データ記憶手段３０に記憶されている旧データＤ１を、復号手段３４によって復号された新データＤ２に更新する。

【０００９】

上記の管理装置１０は、ユーザによって過去に入力されたデータＤ１を利用して、新データＤ２を暗号化する。上述したように、管理装置１０は、ユーザによって過去に入力された旧データＤ１を継続して記憶しておき、その旧データＤ１を利用して新データＤ２を暗号化してもよい。一方において、管理装置１０は、新データＤ２と旧データＤ１の両方を入力することをユーザに要求し、その旧データＤ１を利用して新データＤ２を暗号化してもよい。情報処理装置２５は、暗号化された新データＥ（Ｄ２，Ｄ１）を、旧データ記憶手段３０に記憶されている旧データＤ１をキーとして復号することができる。これにより、旧データＤ１を新データＤ２に更新することができる。ユーザは、情報処理装置２５で更新されたデータＤ２をデータＤ３にさらに更新することができる。この場合、データＤ２が旧データになり、データＤ３が新データになる。管理装置１０は、旧データＤ２をキーとして新データＤ３を暗号化する。情報処理装置２５には、過去に更新された旧データＤ２が記憶されている。情報処理装置２５は、暗号化された新データＥ（Ｄ３，Ｄ２）を旧データＤ２をキーとして復号することができる。これにより、旧データＤ２を新データＤ３に更新することができる。

本発明の通信システム２によると、旧データ（例えば旧パスワード）がキーとなって新データの暗号化及び復号化が行なわれる。即ち、情報処理装置２５で更新されるべきデータ（例えばパスワード）を管理装置１０から情報処理装置２５に送ることが、暗号キーを送ることを兼用している。このために、管理装置１０と情報処理装置２５の間では、情報処理装置２５で更新されるべきデータの他に、暗号キーを通信する必要がない。本発明の通信システム２は、従来にない斬新な思想で暗号キーを通信することができる。

【００１０】

情報処理装置２５は、チャレンジデータＣＤを管理装置１０に出力するチャレンジ出力手段３８と、チャレンジ出力手段３８から出力されたチャレンジデータＣＤを記憶するチャレンジ記憶手段４０とをさらに有していてもよい。また、管理装置１０は、情報処理装置２５から出力されたチャレンジデータＣＤを入力するチャレンジ入力手段２０をさらに有していてもよい。

「チャレンジデータ」は、情報処理装置２５と管理装置１０の間でデータ通信が安全に実行されたことを確認するためのデータである。本明細書の「チャレンジデータ」は、どのような形式のデータであってもよい。例えば、情報処理装置２５は、１つの数値をランダムに選択することによって、チャレンジデータを生成することができる。

【００１１】

上記のチャレンジデータが利用される場合、管理装置１０は、以下のように動作しても

よい。
暗号化手段１６は、管理装置側新データ入力手段１４に入力された新データＤ２とチャレンジ入力手段２０に入力されたチャレンジデータＣＤとの組合せのデータ（Ｄ２＋ＣＤ）を、管理装置側旧データ入力手段１２に入力された旧データＤ１をキーとして暗号化する。以下では、暗号化された組合せデータをＥ（Ｄ２＋ＣＤ，Ｄ１）と表現する。
新データ出力手段１８は、暗号化手段１６によって暗号化された組合せデータＥ（Ｄ２＋ＣＤ，Ｄ１）を情報処理装置２５に出力する。
【００１２】
また、情報処理装置２５は、以下のように動作してもよい。
処理装置側新データ入力手段３２は、管理装置１０から出力された暗号化された組合せデータＥ（Ｄ２＋ＣＤ，Ｄ１）を入力する。
復号手段３４は、処理装置側新データ入力手段３２に入力された暗号化された組合せデータＥ（Ｄ２＋ＣＤ，Ｄ１）を、旧データ記憶手段３０に記憶されている旧データＤ１をキーとして復号する。
更新手段３６は、復号手段３４によって復号された組合せデータ（Ｄ２＋ＣＤ）に含まれるチャレンジデータＣＤと、チャレンジ記憶手段４０に記憶されているチャレンジデータＣＤとを比較する。更新手段３６は、両者が一致した場合は、旧データ記憶手段３０に記憶されている旧データＤ１を、復号された組合せデータ（Ｄ２＋ＣＤ）に含まれる新データＤ２に更新する。更新手段３６は、両者が一致しない場合は、旧データ記憶手段３０に記憶されている旧データＤ１を更新することを禁止する。
【００１３】
チャレンジデータＣＤを利用すると、以下の効果が得られる。
（１）暗号化された組合せデータＥ（Ｄ２＋ＣＤ，Ｄ１）が管理装置１０から情報処理装置２５に送られる場合に、その組合せデータが損傷することがある。例えば、通信回線上に配置されている他の装置（例えばルータ等）によって組合せデータが改ざんされることがある。この場合、組合せデータに含まれるチャレンジデータが変わるために、組合せデータに含まれるチャレンジデータとチャレンジ記憶手段４０に記憶されているチャレンジデータが一致しない。更新手段３６は、チャレンジデータが一致しない場合にデータの更新を実行しない。通信中に組合せデータが損傷した場合に情報処理装置２５においてデータが更新されることを防止することができる。
（２）ユーザは、旧データＤ１を新データＤ２に更新する際に、旧データＤ１を管理装置１０に入力することができる。この旧データＤ１が正しく入力されなかった場合（例えばＤ１’が入力された場合）、組合せデータ（Ｄ２＋ＣＤ）はデータＤ１’によって暗号化されることになる。暗号化された組合せデータＥ（Ｄ２＋ＣＤ，Ｄ１’）は、旧データＤ１によって復号される。この場合、暗号キーと復号キーが一致しないために、復号された組合せデータに含まれるチャレンジデータとチャレンジ記憶手段４０に記憶されているチャレンジデータＣＤが一致しない。更新手段３６は、チャレンジデータが一致しない場合にデータの更新を実行しない。ユーザによって旧データＤ１が正しく入力されなかった場合に情報処理装置２５においてデータが更新されることを防止することができる。
【００１４】
上記の通信システム２では、要約化されたデータを利用してもよい。データの要約化は、様々な手法を利用して実行することができる。例えば、ハッシュ関数を利用してデータを要約化（ハッシュ化）することができる。
データを要約化すると、データ量を一定化することができる。この場合、デバイス間でのデータ通信や各デバイスがデータを利用する処理等を容易に実行することができるようになることが期待される。
【００１５】
要約化されたデータが利用される場合、管理装置１０と情報処理装置２５は、以下のように動作してもよい。
旧データ記憶手段３０は、旧データＤ１が要約化された要約旧データＨ（Ｄ１）を記憶

する。
チャレンジ出力手段３８は、チャレンジデータＣＤが要約化された要約チャレンジデータＨ（ＣＤ）を管理装置１０に出力する。
チャレンジ記憶手段４０は、チャレンジ出力手段３８から出力された要約チャレンジデータＨ（ＣＤ）を記憶する。
チャレンジ入力手段２０は、情報処理装置３０から出力された要約チャレンジデータＨ（ＣＤ）を入力する。
暗号化手段１６は、管理装置側旧データ入力手段１２に入力された旧データＤ１を要約化して要約旧データＨ（Ｄ１）を作成するとともに、管理装置側新データ入力手段１４に入力された新データＤ２を要約化して要約新データＨ（Ｄ２）を作成する。暗号化手段１６は、その要約新データＨ（Ｄ２）とチャレンジ入力手段２０に入力された要約チャレンジデータＨ（ＣＤ）とから組合せデータ（Ｈ（Ｄ２）＋Ｈ（ＣＤ））を作成し、その組合せデータ（Ｈ（Ｄ２）＋Ｈ（ＣＤ））を要約旧データＨ（Ｄ１）をキーとして暗号化する。以下では、ここで暗号化された組合せデータをＥ（Ｈ（Ｄ２）＋Ｈ（ＣＤ），Ｈ（Ｄ１））と表現する。
復号手段３４は、処理装置側新データ入力手段３２に入力された暗号化された組合せデータＥ（Ｈ（Ｄ２）＋Ｈ（ＣＤ），Ｈ（Ｄ１））を、旧データ記憶手段３０に記憶されている要約旧データＨ（Ｄ１）をキーとして復号する。
更新手段３６は、復号手段３４によって復号された組合せデータ（Ｈ（Ｄ２）＋Ｈ（ＣＤ））に含まれる要約チャレンジデータＨ（ＣＤ）と、チャレンジ記憶手段４０に記憶されている要約チャレンジデータＨ（ＣＤ）とを比較する。更新手段３６は、両者が一致した場合は、旧データ記憶手段３０に記憶されている要約旧データＨ（Ｄ１）を、復号された組合せデータ（Ｈ（Ｄ２）＋Ｈ（ＣＤ））に含まれる要約新データＨ（Ｄ２）に更新する。更新手段３６は、両者が一致しない場合は、要約旧データＨ（Ｄ１）の更新を実行しない。

【００１６】

本発明の技術は、次のように表現することもできる。この技術は、情報処理装置と管理装置を備える通信システムに関する。管理装置は、ユーザによって入力された新パスワードを情報処理装置に出力することによって、情報処理装置に記憶されている旧パスワードを更新することができる。
なお、本明細書の「パスワード」という用語は、デバイスがユーザ認証に利用する文字、数字、記号等のあらゆるデータを含む概念である。
以下では、この通信システムの管理装置と情報処理装置の構成を説明する。これらは、上記した図１を参考にすると理解しやすい。

【００１７】

管理装置は、管理装置側旧パスワード入力手段と管理装置側新パスワード入力手段と暗号化手段と新パスワード出力手段を有する。
管理装置側旧パスワード入力手段は、旧パスワードを入力する。ユーザは、情報処理装置に記憶されている旧パスワードを新パスワードに更新する場合に、自身が記憶している旧パスワードを管理装置に入力することができる。一方において、管理装置は、ユーザによって過去に入力された旧パスワードを継続して記憶しておいてもよい。これによれば、ユーザは、旧パスワードを新パスワードに更新する際に、旧パスワードを管理装置に入力しなくてもよい。
管理装置側新パスワード入力手段は、新パスワードを入力する。
暗号化手段は、管理装置側旧パスワード入力手段に入力された旧パスワードをハッシュ化してハッシュ化旧パスワードを作成し、管理装置側新パスワード入力手段に入力された新パスワードをハッシュ化してハッシュ化新パスワードを作成し、そのハッシュ化新パスワードをハッシュ化旧パスワードをキーとして暗号化する。
新パスワード出力手段は、暗号化手段によって暗号化されたハッシュ化新パスワードを情報処理装置に出力する。

【００１８】
情報処理装置は、旧パスワード記憶手段と処理装置側新パスワード入力手段と復号手段と更新手段を有する。
旧パスワード記憶手段は、旧パスワードがハッシュ化されたハッシュ化旧パスワードを記憶している。
処理装置側新パスワード入力手段は、管理装置から出力された暗号化されたハッシュ化新パスワードを入力する。
復号手段は、処理装置側新パスワード入力手段に入力された暗号化されたハッシュ化新パスワードを、旧パスワード記憶手段に記憶されているハッシュ化旧パスワードをキーとして復号する。
更新手段は、旧パスワード記憶手段に記憶されているハッシュ化旧パスワードを、復号手段によって復号されたハッシュ化新パスワードに更新する。
【００１９】
上記の通信システムによると、情報処理装置で更新されるべきパスワードを管理装置から情報処理装置に送ることが、暗号キーを送ることを兼用している。このために、管理装置と情報処理装置の間では、情報処理装置で更新されるべきパスワードの他に、暗号キーを通信する必要がない。本発明の通信システムは、従来にない斬新な思想で暗号キーを通信することができる。
また、上記の通信システムは、管理装置と情報処理装置の間でハッシュ化されたデータが通信される。ハッシュ化されたデータは、データ量が一定である。この場合、デバイス間でのデータ通信や各デバイスがデータを利用する処理等を容易に実行することができるようになることが期待される。
【００２０】
本発明では、次の管理装置を提供する。この管理装置の構成は、図１を参照すると理解しやすい。
管理装置１０は、情報処理装置２５と通信可能に接続されて利用されるとともに、ユーザによって入力された新データＤ２を情報処理装置２５に出力することによって、情報処理装置２５に記憶されている旧データＤ１を更新することができる。
管理装置１０は、旧データＤ１を入力する管理装置側旧データ入力手段１２と、新データＤ２を入力する管理装置側新データ入力手段１４と、管理装置側新データ入力手段１４に入力された新データＤ２を管理装置側旧データ入力手段１２に入力された旧データＤ１をキーとして暗号化する暗号化手段１６と、暗号化手段１６によって暗号化された新データＤ２を情報処理装置２５に出力する新データ出力手段１８とを備える。
この管理装置１０は、従来にない斬新な手法で情報処理装置２５に暗号キーを送ることができる。
【００２１】
次の情報処理装置も有用である。この情報処理装置の構成は、図１を参照すると理解しやすい。
情報処理装置２５は、管理装置１０と通信可能に接続されて利用されるとともに、自身が記憶している旧データＤ１をユーザによって管理装置１０に入力された新データＤ２に更新する。
この情報処理装置２５は、旧データＤ１を記憶する旧データ記憶手段３０と、管理装置１０から出力された暗号化された新データＤ２を入力する処理装置側新データ入力手段３２と、処理装置側新データ入力手段３２に入力された暗号化された新データＤ２を旧データ記憶手段３０に記憶されている旧データＤ１をキーとして復号する復号手段３４と、旧データ記憶手段３０に記憶されている旧データＤ１を復号手段３４によって復号された新データＤ２に更新する更新手段３６とを有する。
この情報処理装置２５は、従来にない斬新な手法でデータの復号化とデータの更新を実行することができる。
【００２２】

上記した管理装置を実現するためのコンピュータプログラムも、本発明の創作物の１つである。このコンピュータプログラムは、管理装置に搭載されるコンピュータに、以下の各工程を実行させる。
（１）ユーザによって入力された新データを、ユーザによって入力された旧データをキーとして暗号化する暗号化工程。
（２）暗号化工程で暗号化された新データを情報処理装置に出力する新データ出力工程。
このコンピュータプログラムによると、従来にない斬新な手法で情報処理装置に暗号キーを送る管理装置を実現することができる。

【００２３】

上記した情報処理装置を実現するためのコンピュータプログラムも、本発明の創作物の１つである。このコンピュータプログラムは、情報処理装置に搭載されるコンピュータに、以下の各工程を実行させる。
（１）管理装置から出力された暗号化された新データが入力されると、その暗号化された新データを、情報処理装置に記憶されている旧データをキーとして復号する復号工程。
（２）情報処理装置に記憶されている旧データを、復号工程で復号された新データに更新する更新工程。
このコンピュータプログラムによると、従来にない斬新な手法でデータの復号化とデータの更新を実行する情報処理装置を実現することができる。

【発明を実施するための最良の形態】

【００２４】

ここでは、以下の実施例に記載の技術の主要な特徴をまとめておく。
（形態１）管理装置は、インターネットに接続されて利用されるコンピュータ（ＰＣ）である。
（形態２）情報処理装置は、インターネットに接続されて利用される複合機である。この複合機は、スキャナ装置と印刷装置を少なくとも有する。この複合機は、インターネットファクシミリとして機能する。
（形態３）情報処理装置は、管理装置から情報処理装置を操作する際のログイン用のパスワードを記憶している。管理装置は、ユーザによって入力されたパスワードを情報処理装置に出力する。情報処理装置は、管理装置から出力されたパスワードを入力する。情報処理装置は、入力されたパスワードと自身が記憶しているパスワードとを比較し、両者が一致した場合に、管理装置からの指示に応じた処理を実行する。
（形態４）情報処理装置は、複数の管理装置と通信可能に接続されている。情報処理装置は、複数の管理装置によって共用されている。情報処理装置は、個々の管理装置について、その管理装置から情報処理装置を操作する際のログイン用のパスワードを記憶している。

【００２５】

（形態５）管理装置は、所定のデータ量を単位データ量とするブロック単位で組合せデータ（新データとチャレンジデータとの組合せのデータ）を暗号化する。情報処理装置は、組合せデータをブロック毎に復号する。
（形態６）管理装置は、暗号化された組合せデータの少なくとも１つのブロックに、チャレンジデータの少なくとも一部と新データ（新パスワード）の少なくとも一部の両方を含ませる。
（形態７）管理装置は、チャレンジデータを少なくとも２つの分割チャレンジデータに分割し、新データ（新パスワード）の少なくとも一部が一方の分割チャレンジデータと他方の分割チャレンジデータの間に配置された組合せデータを作成する。
（形態８）管理装置は、暗号化された組合せデータの全てのブロックのそれぞれに、少なくとも１つの分割チャレンジデータを含ませる。
（形態９）管理装置は、新データ（新パスワード）を少なくとも２つの分割新パスワードデータに分割し、暗号化された組合せデータの全てのブロックのそれぞれに、少なくとも１つの分割チャレンジデータと少なくとも１つの分割新パスワードデータの両方を含ませ

る。
（形態１０）情報処理装置は、復号された組合せデータからチャレンジデータと新データ（新パスワード）を再現するためのルールを記憶している。
【実施例】
【００２６】
（第１実施例）
図面を参照して本発明の実施例を説明する。図２は、本実施例の通信システム５０の構成を簡単に示す。通信システム５０は、管理装置６０と複合機８０等を有する。管理装置６０と複合機８０は、インターネット９８によって相互に通信可能に接続されている。
【００２７】
（管理装置の構成）
管理装置６０は、制御装置６２と記憶装置６４と表示装置６６と操作装置６８と入出力ポート７０等を有する。
制御装置６２は、ＣＰＵ等によって構成されている。制御装置６２は、管理装置６０が実行する各処理を統括的に制御する。
記憶装置６４は、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ等によって構成されている。記憶装置６４は、制御装置６２が各処理を実行するためのプログラムを記憶している。記憶装置６４は、例えば、ユーザによって入力されたパスワードを複合機８０に出力するためのプログラムや、複合機８０に記憶されている管理装置６０のパスワードを変更するためのプログラム等を記憶している。また、記憶装置６４は、各処理が実行される過程で利用されるデータを一時的に記憶することができる。
表示装置６６は、液晶ディスプレイ等によって構成されている。表示装置６６は、様々なデータを表示することができる。
操作装置６８は、マウスやキーボード等によって構成されている。ユーザは、操作装置６８を操作することによって、様々な情報を管理装置６０に入力することができる。
入出力ポート７０には、インターネット回線９８ａが接続されている。管理装置８０は、インターネット回線９８ａを介してインターネット９８に接続されている。
なお、図２では、１つの管理装置６０しか図示されていない。しかしながら、実際は複数の管理装置６０が存在する。複数の管理装置６０のそれぞれが、インターネット９８に接続されている。複数の管理装置６０は、次に説明する複合機８０を共用している。
【００２８】
（複合機の構成）
複合機８０は、スキャナ装置８２と制御装置８４と記憶装置８６と表示装置８８と操作装置９０と印刷装置９２と入出力ポート９４等を有する。
スキャナ装置８２は、ＣＣＤ（Ｃｈａｒｇｅ Ｃｏｕｐｌｅｄ Ｄｅｖｉｃｅ）又はＣＩＳ（Ｃｏｎｔａｃｔ Ｉｍａｇｅ Ｓｅｎｓｏｒ）を有する。スキャナ装置８２は、原稿をスキャンして画像データを生成する。
制御装置８４は、ＣＰＵ等によって構成されている。制御装置８４は、複合機８０が実行する各処理を統括的に制御する。
記憶装置８６は、ＲＯＭ、ＲＡＭ、ＥＥＰＲＯＭ等によって構成されている。記憶装置８６は、制御装置８４が各処理を実行するためのプログラムを記憶したり、各処理が実行される過程で利用されるデータを一時的に記憶したりする。本実施例の記憶装置８６は、チャレンジ記憶領域８６ａとパスワード記憶領域８６ｂと再現ルール記憶領域８６ｃを少なくとも有する。チャレンジ記憶領域８６ａによって記憶されるデータは、後で詳しく説明する。パスワード記憶領域８６ｂは、複合機８０へのログイン用のＩＤとパスワードの組合せを記憶している。パスワード記憶領域８６ｂは、個々の管理装置６０についてＩＤとパスワードを記憶している。例えば、管理装置６０のログイン用のＩＤが「ＸＸＸ６０」であってパスワードが「ＹＹＹＹＹ」である場合、「ＸＸＸ６０」と「ＹＹＹＹＹ」の組合せを記憶している。再現ルール記憶領域８６ｃの記憶内容は、後で詳しく説明する。
表示装置８８は、液晶ディスプレイ等によって構成されている。表示装置８８は、様々

なデータを表示することができる。
操作装置９０は、複数のキーによって構成されている。ユーザは、操作装置９０を操作することによって、複合機８０に様々な情報を入力することができる。
印刷装置９２は、スキャナ装置８２によって作成された画像データを印刷媒体に印刷する。
入出力ポート９４には、インターネット回線９８ｂが接続されている。複合機８０は、インターネット回線９８ｂを介してインターネット９８に接続されている。複合機８０は、インターネット９８を介して複数の管理装置６０に接続されている。
【００２９】
上述したように、複合機８０のパスワード記憶領域８６ｂには、ログイン用ＩＤとパスワードの組合せが記憶されている。管理装置６０のユーザは、自身が記憶しているＩＤとパスワードを、操作装置６８を利用して管理装置６０に入力することができる。管理装置６０は、入力されたＩＤ（例えば「ＸＸＸ６０」）と、入力されたパスワード（例えば「ＹＹＹＹＹ」）を複合機８０に出力する。
複合機８０は、管理装置６０から出力されたＩＤ「ＸＸＸ６０」とパスワード「ＹＹＹＹＹ」の組合せが、パスワード記憶領域８６ｂが記憶されているのか否かを判断する。即ち、複合機８０は、ユーザ認証を実行する。複合機８０は、ユーザ認証が成功した場合に、管理装置６０からの指示に応じた処理を実行する。例えば、複合機８０は、自身に記憶されている各種の設定を管理装置６０からの指示に応じて変更する。ユーザ認証が失敗した場合、複合機８０は、管理装置６０からの指示に応じた処理を実行しない。
なお、管理装置６０から複合機８０に送られるパスワードは、暗号化されることが好ましい。ここでの暗号化の手法は、公知の手法が用いられる。
また、管理装置６０と複合機８０の間では、ＵＤＰ／ＩＰを利用してパスワード等のデータが通信される。
【００３０】
管理装置６０のユーザは、複合機８０に記憶されているパスワードを変更することができる。例えば、ＩＤ「ＸＸＸ６０」とパスワード「ＹＹＹＹＹ」の組合せが複合機８０に記憶されている場合、管理装置６０のユーザは、そのパスワード「ＹＹＹＹＹ」を新しいパスワード「ＺＺＺＺＺ」に変更させることができる。
以下では、複合機８０に記憶されているパスワードが変更される際に、管理装置６０や複合機８０によって実行される処理（以下ではパスワード変更処理と呼ぶ）について説明する。
【００３１】
（パスワード変更処理の概要）
まず、パスワード変更処理の概要を説明する。図３は、管理装置６０と複合機８０によって実行されるパスワード変更処理のタイムチャートを示す。
（Ａ１）複合機８０のパスワード記憶領域８６ｂ（図２参照）には、管理装置６０のパスワードが記憶されている。パスワードは、ハッシュ化（ダイジェスト化）されている。いかなるデータ量のデータであっても、ハッシュ化されると一定のデータ量になる。本実施例では、ＳＨＡ１（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ　１）のハッシュ関数を利用してデータがハッシュ化される（ＳＨＡ１を利用した場合、ハッシュ化後のデータは２０バイトになる）。パスワード記憶領域８６ｂには、管理装置６０のＩＤとハッシュ化されたパスワードＨ（Ｄ１）の組合せが記憶されている。
（Ａ２）管理装置６０は、複合機８０に記憶されているパスワードを変更することがユーザによって指示されると、複合機８０が暗号化に対応しているのか否かを複合機８０に問い合わせる。
（Ａ３）複合機８０は、暗号化に対応している場合、暗号化に対応していることを示す情報を管理装置６０に出力する。複合機８０は、暗号化に対応していない場合、暗号化に対応していないことを示す情報を管理装置６０に出力する。なお、以下では、複合機８０が暗号化に対応しているものとして説明を続ける。

（Ａ４）管理装置６０は、チャレンジデータを出力することを複合機８０に要求する。
（Ａ５）複合機８０は、チャレンジデータ（乱数値）を作成する。複合機８０は、チャレンジデータをハッシュ化する。以下では、ハッシュ化されたチャレンジデータをＨ（Ｃ）と記載する。チャレンジデータＨ（Ｃ）は、チャレンジ記憶領域８６ａ（図２参照）に記憶される。
（Ａ６）複合機８０は、ハッシュ化されたチャレンジデータＨ（Ｃ）を管理装置６０に出力する。
【００３２】
（Ａ７）ユーザは、複合機８０に記憶されているパスワードを変更する際に、管理装置６０の現在のパスワードを管理装置６０に入力する。本実施例では、現在のパスワードをＤ１と表現する。しかしながら、ユーザが正しいパスワードを入力するとは限らない。以下では、管理装置６０にユーザが入力した現在のパスワード（即ち旧パスワード）をＤ１’と記載する。管理装置６０は、入力された旧パスワードＤ１’をハッシュ化する。以下では、ハッシュ化された旧パスワードをＨ（Ｄ１’）と記載する。
（Ａ８）ユーザは、新パスワードＤ２を管理装置６０に入力する。管理装置６０は、入力された新パスワードＤ２をハッシュ化する。以下では、ハッシュ化された新パスワードをＨ（Ｄ２）と記載する。
（Ａ９）管理装置６０は、上記のＡ６で入力されたチャレンジデータＨ（Ｃ）とＡ８で作成された新パスワードＨ（Ｄ２）との組合せのデータを、Ａ７で作成された旧パスワードＨ（Ｄ１’）をキーとして暗号化する。この組合せデータの構造は、後で詳しく説明する。なお、以下では、暗号化された組合せデータをＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’））と記載する。
（Ａ１０）管理装置６０は、暗号化された組合せデータＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’））を複合機８０に出力する。
【００３３】
（Ａ１１）複合機８０は、暗号化された組合せデータＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’））を、パスワード記憶領域８６ｂ（図２参照）に記憶されている旧パスワードＨ（Ｄ１）をキーとして復号する。
（Ａ１２）複合機８０は、復号された組合せデータ（Ｈ（Ｃ）＋Ｈ（Ｄ２））に含まれるチャレンジデータＨ（Ｃ）と、上記のＡ５でチャレンジ記憶領域８６ａに記憶されたチャレンジデータＨ（Ｃ）を比較する。ユーザによって管理装置６０に入力された旧パスワードＤ１’が正しいパスワードＤ１であり、かつ、上記のＡ１０のデータ通信中に組合せデータＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’））が改ざんされなかった場合は、２つのチャレンジデータが一致するはずである。
　一方において、ユーザによって管理装置６０に入力された旧パスワードＤ１’が正しいパスワードＤ１ではなかった場合、組合せデータ（Ｈ（Ｃ）＋Ｈ（Ｄ２））の暗号化のためのキーと、復号化のためのキーが一致しないことになる。この場合、復号化されたチャレンジデータは、チャレンジ記憶領域８６ａに記憶されているチャレンジデータに一致しない。また、上記のＡ１０のデータ通信中に組合せデータＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’））が改ざんされた場合、組合せデータに含まれるチャレンジデータが改ざんされることになる。この場合も、復号化されたチャレンジデータは、チャレンジ記憶領域８６ａに記憶されているチャレンジデータに一致しない。
（Ａ１３）複合機８０は、Ａ１２で比較された２つのチャレンジデータが一致した場合に、パスワード記憶領域８６ｂ（図２参照）に記憶されている旧パスワードＨ（Ｄ１）を、復号された組合せデータ（Ｈ（Ｃ）＋Ｈ（Ｄ２））に含まれる新パスワードＨ（Ｄ２）に更新する。
（Ａ１４）複合機８０は、パスワードを変更することを許可したのか否かを管理装置６０に出力する。
【００３４】
（管理装置のパスワード変更処理）

続いて、管理装置６０が実行するパスワード変更処理について詳しく説明する。図４は、管理装置６０のパスワード変更処理のフローチャートを示す。以下の処理は、管理装置６０の制御装置６２（図２参照）によって実行される。

管理装置６０のユーザは、操作装置６８（図２参照）を操作することによって、現在のパスワード（旧パスワード）と新パスワードとパスワード変更命令を管理装置６０に入力することができる。管理装置６０は、旧パスワードＤ１’と新パスワードＤ２とパスワード変更命令を入力する（Ｓ２０）。

管理装置６０は、複合機８０が暗号化に対応しているのか否かを問い合わせる（Ｓ２２）。この処理は、図３のＡ２に相当する。

管理装置６０は、複合機８０が暗号化に対応しているのか否かを判断する（Ｓ２４）。ここでＮＯの場合、管理装置６０は、新パスワードＤ２を複合機８０に出力する（Ｓ２６）。新パスワードＤ２は、出力に際してハッシュ化されないし、また、旧パスワードＤ１’をキーとして暗号化されることもない。Ｓ２６が実行されると、複合機８０は、旧パスワードＤ１を新パスワードＤ２に更新することになる。なお、Ｓ２６では、ユーザによって入力された旧パスワードＤ１’が複合機８０に出力されることが好ましい。この場合、複合機８０は、旧パスワードＤ１’をハッシュ化する。ユーザによって入力されてハッシュ化された旧パスワードＤ１’がパスワード記憶領域８６ｂ（図２参照）に記憶されている場合に、ハッシュ化された旧パスワードＤ１を、同じく複合機８０においてハッシュ化された新パスワードＤ２に更新することが好ましい。

【００３５】

Ｓ２４でＹＥＳの場合、管理装置６０は、チャレンジデータを出力するように複合機８０に指示する（Ｓ２８）。これにより、複合機８０から管理装置６０にチャレンジデータＨ（Ｃ）が送られることになる。Ｓ２８の処理は、図３のＡ４に相当する。管理装置６０は、チャレンジデータＨ（Ｃ）を入力する（Ｓ３０）。

管理装置６０は、Ｓ２０で入力された旧パスワードＤ１’をハッシュ化する（Ｓ３２）。これにより、ハッシュ化された旧パスワードＨ（Ｄ１’）が作成されることになる。さらに、管理装置６０は、Ｓ２０で入力された新パスワードＤ２をハッシュ化する（Ｓ３２）。これにより、ハッシュ化された新パスワードＨ（Ｄ２）が作成されることになる。Ｓ３２の処理は、図３のＡ７とＡ８に相当する。

管理装置６０は、チャレンジデータＨ（Ｃ）と新パスワードＨ（Ｄ２）との組合せのデータ（Ｈ（Ｃ）＋Ｈ（Ｄ２））を作成する。管理装置６０は、旧パスワードＨ（Ｄ１）をキーとして、組合せデータ（Ｈ（Ｃ）＋Ｈ（Ｄ２））を暗号化する（Ｓ３４）。Ｓ３４の処理は、図３のＡ９に相当する。

【００３６】

図５を参照して、Ｓ３４の処理の内容を詳しく説明する。

図５（ａ）は、ハッシュ化されたチャレンジデータＨ（Ｃ）を示す。チャレンジデータＨ（Ｃ）は、２０バイトである。

図５（ｂ）は、ハッシュ化された新パスワードＨ（Ｄ２）を示す。新パスワードＨ（Ｄ２）は、２０バイトである。なお、チャレンジデータＨ（Ｃ）及び新パスワードＨ（Ｄ２）は、ＳＨＡ１を利用するため、共に２０バイトになる。

図５（ｃ）は、暗号化された組合せデータＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’））を示す。組合せデータＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’））は、以下のようにして作成される。

【００３７】

（１）２０バイトのチャレンジデータＨ（Ｃ）が、１バイト目から８バイト目までの第１分割チャレンジデータと、９バイト目から１６バイト目までの第２分割チャレンジデータと、１７バイト目から２０バイト目までの第３分割チャレンジデータに分割される。

（２）２０バイトの新パスワードＨ（Ｄ２）が、１バイト目から８バイト目までの第１分割パスワードデータと、９バイト目から１６バイト目までの第２分割パスワードデータと、１７バイト目～２０バイト目までの第３分割パスワードデータに分割される。

（３）第１分割チャレンジデータ、第１分割パスワードデータ、第２分割チャレンジデータ、第２分割パスワードデータ、第３分割チャレンジデータ、第３分割パスワードデータの順に並び替えられた組合せデータが作成される。この組合せデータの全データ量は、４０バイトである

（４）本実施例では、ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）を利用して、組合せデータをブロック単位で暗号化する。ＡＥＳで暗号化される１つのブロックのデータ量は、所定の固定値である（例えば１６バイトで固定。以下では１０バイトを例にして説明する）。上記したように、組合せデータの全データ量は、４０バイトである。組合せデータを１６バイトの倍数にしなければ、ブロック単位で暗号化することができない。このために、第３分割チャレンジデータと第３分割パスワードデータの間に４バイトのチャレンジ用ダミーデータが追加される。また、第３分割パスワードデータの後に４バイトのパスワード用ダミーデータが追加される。これにより、組合せデータの全データ量が４８バイトになり、組合せデータを３つのブロック１００，１０２，１０４によって暗号化することができる。

（５）ブロックデータ１００，１０２，１０４のそれぞれは、旧パスワードＨ（Ｄ１’）をキーとして暗号化される。ＡＥＳを利用して１つのブロックデータ（例えば１００）を暗号化するためには、所定のデータ量のキーが必要とされる（本実施例では１６バイトのキーとする）。これに対し、旧パスワードＨ（Ｄ１’）は、２０バイトである。本実施例では、旧パスワードＨ（Ｄ１’）の１バイト目から１６バイト目までのデータがキーとして利用される。即ち、旧パスワードＨ（Ｄ１’）の１７バイト目から２０バイト目までは、キーとして利用されない。

【００３８】

暗号化された組合せデータＥ（Ｈ（Ｃ）＋（Ｈ（Ｄ２），Ｈ（Ｄ１’））は、３つのブロックデータ１００，１０２，１０４によって構成されている。第１ブロックデータ１００は、８バイトの第１分割チャレンジデータと８バイトの第１分割パスワードデータを含む。第２ブロックデータ１０２は、８バイトの第２分割チャレンジデータと８バイトの第２分割パスワードデータを含む。第３ブロックデータ１０４は、４バイトの第３分割チャレンジデータと４バイトのチャレンジ用ダミーデータと４バイトの第３分割パスワードデータと４バイトのパスワード用ダミーデータを含む。

全てのブロックデータ１００，１０２，１０４のそれぞれに、分割チャレンジデータと分割パスワードデータの両方が含まれている。各ブロックデータ１００，１０２，１０４では、そのブロックに含まれる分割チャレンジデータのデータ量と分割パスワードデータのデータ量は等しい。

【００３９】

図４の暗号化処理（Ｓ３４）が終了すると、管理装置６０は、暗号化された組合せデータＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’））を複合機８０に出力する（Ｓ３６）。これにより、旧パスワードＨ（Ｄ１）が新パスワードＨ（Ｄ２）に更新される処理が複合機８０によって実行される。Ｓ３６の処理は、図３のＡ１０に相当する。

管理装置６０は、複合機８０から出力されたパスワード変更処理結果を入力する（Ｓ３８）。パスワード変更処理結果は、パスワードが正常に変更されたのか否かを示す情報である。管理装置６０は、パスワード変更処理結果を表示装置６６（図２参照）に表示する（Ｓ４０）。

【００４０】

（複合機のチャレンジ発行処理）

続いて、複合機８０が実行するチャレンジ発行処理について詳しく説明する。図６は、チャレンジ発行処理のフローチャートを示す。以下の処理は、複合機８０の制御装置８４（図２参照）によって実行される。

複合機８０は、チャレンジデータを出力することを管理装置６０から要求されたのか否かを監視している（Ｓ５０）。この処理は、図４のＳ２８で管理装置６０から出力された指示を入力すると、ＹＥＳと判断される。

Ｓ５０でＹＥＳの場合、複合機８０は、乱数を生成して１つの乱数値を取得する（Ｓ５２）。この乱数値が、チャレンジデータ（チャレンジ値）である。複合機８０は、Ｓ５２の処理において、チャレンジデータをハッシュ化する。これにより、ハッシュ化されたチャレンジデータＨ（Ｃ）が生成される。また、複合機８０は、チャレンジデータＨ（Ｃ）を管理装置６０に出力する。Ｓ５２の処理は、図３のＡ５とＡ６に相当する。

次いで、複合機８０は、記憶装置８６のチャレンジ記憶領域８６ａ（図２参照）に記憶されているチャレンジデータの個数が上限（例えば１０個）に達しているのか否かを判断する（Ｓ５４）。ここでＹＥＳの場合、最も古いチャレンジデータをチャレンジ記憶領域８６ａから消去する（Ｓ５６）。

複合機８０は、Ｓ５２で生成されたチャレンジデータをチャレンジ記憶領域８６ａに記憶する（Ｓ５８）。

【００４１】

（複合機のパスワード変更処理）

続いて、複合機８０が実行するパスワード変更処理について詳しく説明する。図７は、パスワード変更処理のフローチャートを示す。以下の処理は、複合機８０の制御装置８４（図２参照）によって実行される。

複合機８０は、図４のＳ３６で管理装置６０から出力された組合せデータＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’））を入力すると、パスワード変更処理を実行する。複合機８０は、組合せデータＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’））を、パスワード記憶領域８６ｂに記憶されている旧パスワードＨ（Ｄ１）をキーとして復号する（Ｓ６０）。組合せデータＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’））は、複数のブロックデータ１００，１０２，１０４によって構成されている（図５（ｃ）参照）。複合機８０は、複数のブロックデータ１００，１０２，１０４のそれぞれを個別に復号する。上述したように、各ブロックデータ１００，１０２，１０４は、旧パスワードＨ（Ｄ１’）の先頭の１６バイトを利用して暗号化されている。このために、複合機８０は、パスワード記憶領域８６ｂに記憶されている旧パスワードＨ（Ｄ１）の先頭の１６バイトを利用して、各ブロックデータ１００，１０２，１０４を復号する。

【００４２】

複合機８０の再現ルール記憶領域８６ｃ（図２参照）は、以下の情報（チャレンジデータと新パスワードを再現するためのルール）を記憶している。

（１）１番目のブロックデータ１００の前半の８バイトは、チャレンジデータ（第１分割チャレンジデータ）である。後半の８バイトは、新パスワード（第１分割パスワードデータ）である。

（２）２番目のブロックデータ１０２の前半の８バイトは、チャレンジデータ（第２分割チャレンジデータ）である。後半の８バイトは、新パスワード（第２分割パスワードデータ）である。

（３）３番目のブロックデータ１０４の先頭から４バイトは、チャレンジデータ（第３分割チャレンジデータ）である。次の４バイトは、ダミーデータである。次の４バイトは、新パスワード（第３分割パスワードデータ）である。最後の４バイトは、ダミーデータである。

（４）１番目のブロックデータ１００のチャレンジデータを先頭とし、その次に２番目のブロックデータ１０２のチャレンジデータを並べ、最後に３番目のブロックデータ１０４のチャレンジデータを並べると、チャレンジデータＨ（Ｃ）を再現することができる。

（５）１番目のブロックデータ１００の新パスワードを先頭とし、その次に２番目のブロックデータ１０２の新パスワードを並べ、最後に３番目のブロックデータ１０４の新パスワードを並べると、新パスワードＨ（Ｄ２）を再現することができる。

【００４３】

上記の図７のＳ６０の処理では、組合せデータＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’））が復号された後に、上記のルールに従ってチャレンジデータと新パスワードが再現される。Ｓ６０の処理は、図３のＡ１１に相当する。

続いて、複合機８０は、Ｓ６０で復号されたチャレンジデータが、チャレンジ記憶領域８６ａ（図２参照）に含まれているのか否かを判断する（Ｓ６２）。これにより、復号されたチャレンジデータと、図６のＳ５８でチャレンジ記憶領域８６ａに記憶されたチャレンジデータが比較されることになる。Ｓ６２の処理は、図３のＡ１２に相当する。

Ｓ６２でＹＥＳの場合、複合機８０は、パスワード記憶領域８６ｂに記憶されている旧パスワードＨ（Ｄ１）を消去し、Ｓ６０で復号された新パスワードＨ（Ｄ２）を記憶する（Ｓ６４）。これにより、旧パスワードＨ（Ｄ１）から新パスワードＨ（Ｄ２）に変更されることになる。Ｓ６４の処理は、図３のＡ１３に相当する。一方において、Ｓ６２でＮＯの場合、複合機８０は、Ｓ６４をスキップしてＳ６６に進む。

複合機８０は、パスワード変更処理の結果を管理装置６０に出力する（Ｓ６６）。Ｓ６４を経由してＳ６６が実行される場合は、パスワード変更が成功した旨の情報が出力される。Ｓ６４をスキップしてＳ６６が実行される場合は、パスワード変更が失敗した旨の情報が出力される。管理装置６０は、パスワード変更処理結果を表示する（図４のＳ４０参照）。ユーザは、パスワード変更が成功したのか否かを知ることができる。

【００４４】

本実施例の管理装置６０は、複合機８０において過去に更新されたパスワードＨ（Ｄ１’）を利用して、新パスワードＤ２を暗号化する。複合機８０は、暗号化された新パスワードＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’）を、過去に更新された旧パスワードＨ（Ｄ１）をキーとして復号する。これにより、旧パスワードＨ（Ｄ１）が新パスワードＨ（Ｄ２）に更新される。

例えば、ユーザがパスワードＤ２を新パスワードＤ３に更新する場合は、パスワードＨ（Ｄ２’）をキーとして新パスワードＨ（Ｄ３）が暗号化される。複合機８０は、暗号化された新パスワードＥ（Ｈ（Ｃ）＋Ｈ（Ｄ３），Ｈ（Ｄ２’））をパスワードＨ（Ｄ２）をキーとして復号する。これにより、旧パスワードＨ（Ｄ２）が新パスワードＨ（Ｄ３）に更新される。

本実施例の通信システム５０によると、ユーザによって管理装置６０に過去に入力されて複合機８０で更新された旧パスワードがキーとなって新パスワードの暗号化及び復号化が行なわれる。このために、管理装置６０と複合機８０の間では、複合機８０で更新されるべきパスワードの他に、暗号化のためのキーを通信する必要がない。本実施例の通信システム５０は、従来にない斬新な手法で暗号キーの通信を実現している。

【００４５】

暗号化された組合せデータＥ（Ｈ（Ｃ）＋Ｈ（Ｄ２），Ｈ（Ｄ１’）が管理装置６０から複合機８０に送られる場合に、その組合せデータが改ざんされることがある。この場合、組合せデータに含まれるチャレンジデータが変わるために、組合せデータに含まれるチャレンジデータとチャレンジ記憶領域８６ａに記憶されているチャレンジデータが一致しない。この場合、パスワードが更新されない。改ざんされたパスワードに更新されることを防止することができる。

ユーザは、パスワードを更新する際に、旧パスワードＤ１’を管理装置６０に入力する。この旧パスワードＤ１’が正しく入力されなかった場合、暗号キーと復号キーが一致しないために、復号された組合せデータに含まれるチャレンジデータとチャレンジ記憶領域８６ａに記憶されているチャレンジデータが一致しない。この場合、パスワードが更新されない。本実施例によると、旧パスワードが正しく入力されなかった場合にパスワードが更新されることを防止することができる。

また、本実施例では、ハッシュ化された一定サイズのデータを利用する。この場合、２つのデバイス６０，８０の間でのデータ通信や各デバイス６０，８０でデータを利用する処理等を容易に実行することができるようになることが期待される。

【００４６】

以上、本発明の具体例を詳細に説明したが、これらは例示にすぎず、特許請求の範囲を限定するものではない。特許請求の範囲に記載の技術には、以上に例示した具体例を様々に変形、変更したものが含まれる。

また、本明細書または図面に説明した技術要素は、単独であるいは各種の組合せによって技術的有用性を発揮するものであり、出願時請求項記載の組合せに限定されるものではない。また、本明細書または図面に例示した技術は複数目的を同時に達成するものであり、そのうちの一つの目的を達成すること自体で技術的有用性を持つものである。

【図面の簡単な説明】

【００４７】

【図１】本発明の通信システムの構成図を示す。

【図２】実施例の通信システムを示す。

【図３】パスワード変更処理のタイムチャートを示す。

【図４】管理装置のパスワード変更処理のフローチャートを示す。

【図５】（ａ）ハッシュ化されたチャレンジデータを示す。（ｂ）ハッシュ化された新パスワードを示す。（ｃ）組合せデータを示す。端末装置のメイン処理のフローチャートを示す。

【図６】複合機のチャレンジ発行処理のフローチャートを示す。

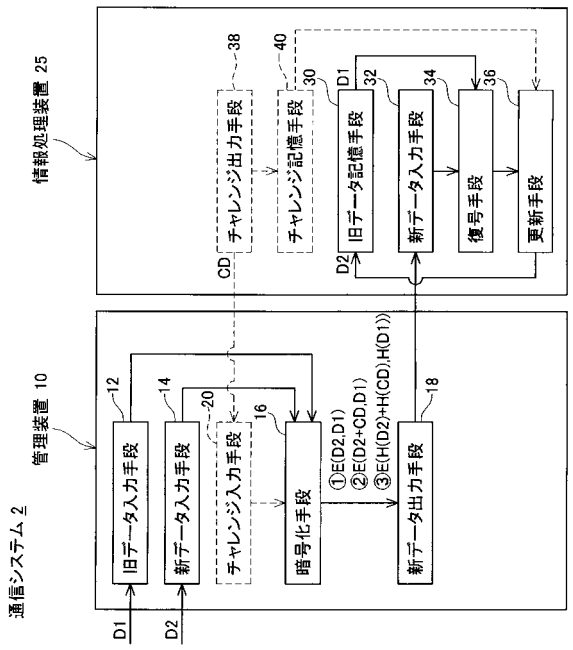
【図７】複合機のパスワード変更処理のフローチャートを示す。

【符号の説明】

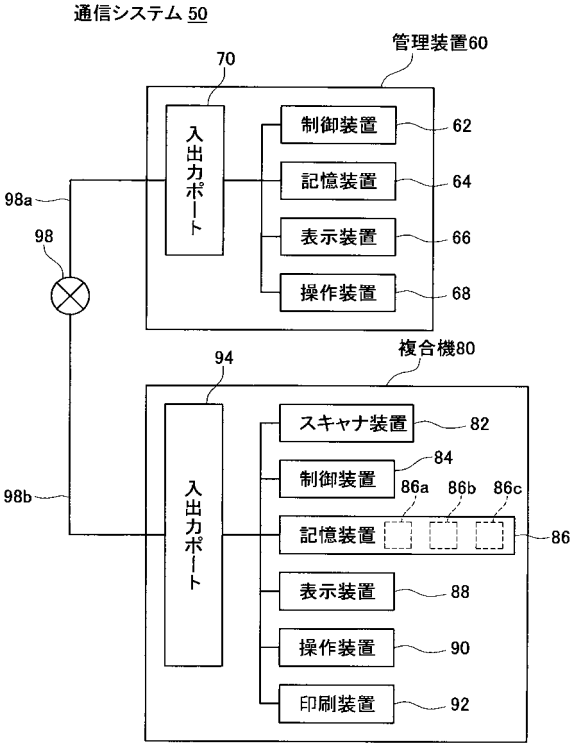
【００４８】

２：通信システム
１０：管理装置
１２：管理装置側旧データ入力手段
１４：管理装置側新データ入力手段
１６：暗号化手段
１８：新データ出力手段
２０：チャレンジ入力手段
２５：情報処理装置
３０：旧データ記憶手段
３２：処理装置側新データ入力手段
３４：復号手段
３６：更新手段
３８：チャレンジ出力手段
４０：チャレンジ記憶手段
５０：通信システム
６０：管理装置
８０：複合機

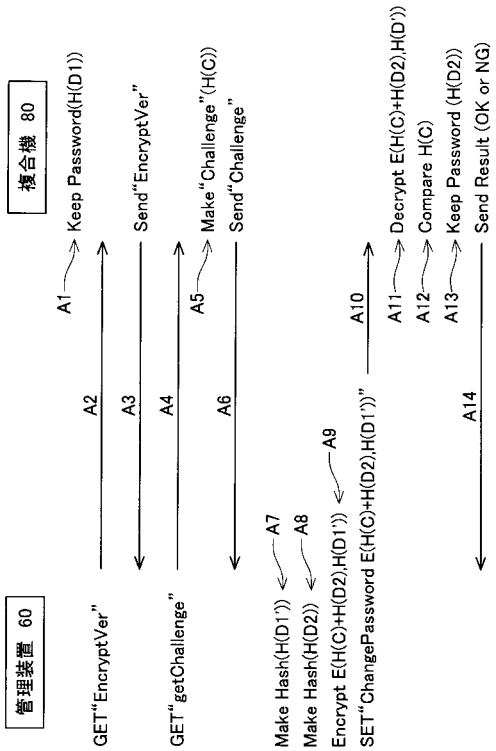
【図１】


通信システム 2
管理装置 10
情報処理装置 25
旧データ入力手段
新データ入力手段
チャレンジ入力手段
暗号化手段
新データ出力手段
チャレンジ出力手段
チャレンジ記憶手段
旧データ記憶手段
新データ入力手段
復号手段
更新手段
①E(D2,D1)
②E(D2+CD,D1)
③E(H(D2)+H(CD),H(D1))
D1
D2
CD

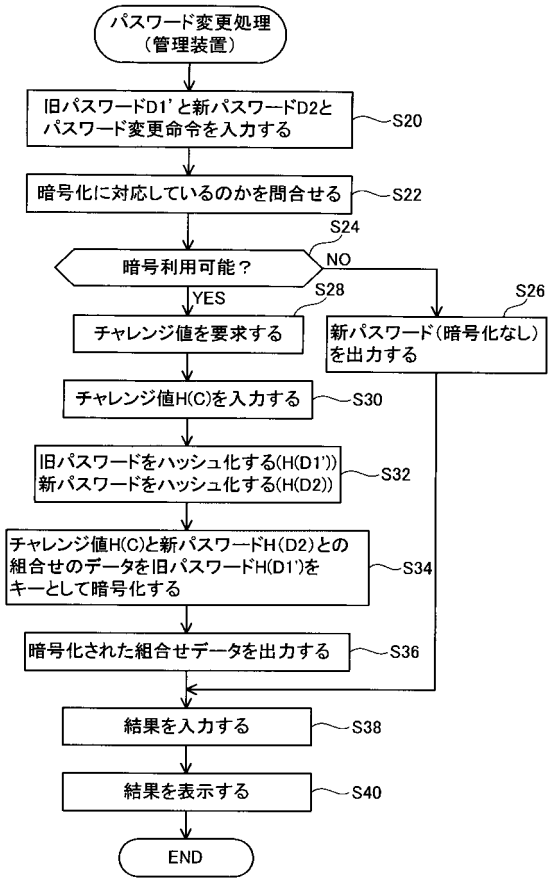
【図２】


通信システム 50
管理装置60
入出力インターフェース
制御装置
記憶装置
表示装置
操作装置
複合機80
スキャナ装置
印刷装置
98a
98
98b

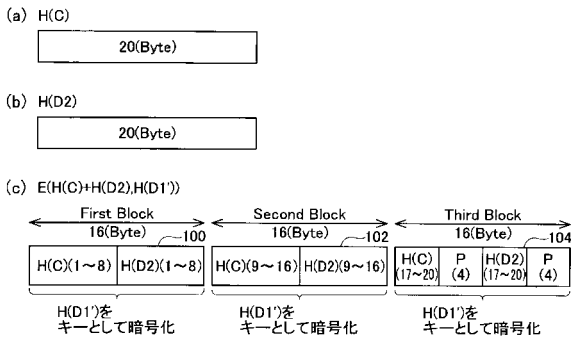
【図３】


複合機 80
管理装置 60
Keep Password(H(D1))
Send"EncryptVer"
Make "Challenge"(H(C))
Send"Challenge"
Decrypt E(H(C)+H(D2),H(D'))
Compare H(C)
Keep Password (H(D2))
Send Result (OK or NG)
GET"EncryptVer"
GET"getChallenge"
Make Hash(H(D1'))
Make Hash(H(D2))
Encrypt E(H(C)+H(D2),H(D1'))
SET"ChangePassword E(H(C)+H(D2),H(D1'))"

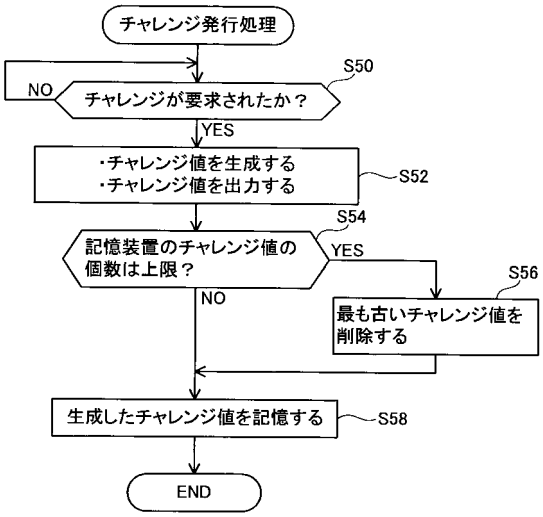
【図４】


パスワード変更処理
（管理装置）
旧パスワードD1'と新パスワードD2と
パスワード変更命令を入力する
S20
暗号化に対応しているのかを問合せる
S22
S24
暗号利用可能？
NO
YES
S28
S26
チャレンジ値を要求する
新パスワード（暗号化なし）
を出力する
チャレンジ値H(C)を入力する
S30
旧パスワードをハッシュ化する(H(D1'))
新パスワードをハッシュ化する(H(D2))
S32
チャレンジ値H(C)と新パスワードH(D2)との
組合せのデータを旧パスワードH(D1')を
キーとして暗号化する
S34
暗号化された組合せデータを出力する
S36
結果を入力する
S38
結果を表示する
S40
END

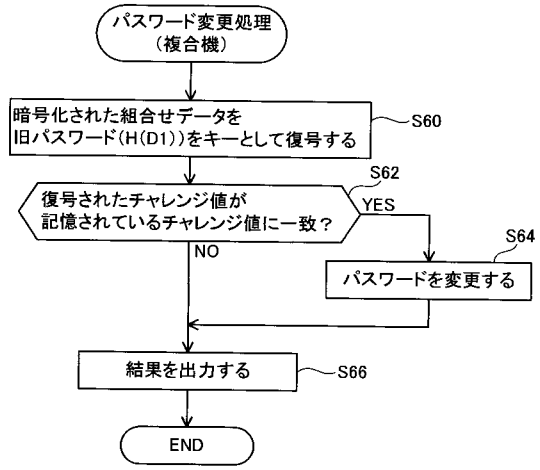
【図５】


(a) H(C)
20(Byte)
(b) H(D2)
20(Byte)
(c) E(H(C)+H(D2),H(D1'))
First Block
16(Byte)
100
Second Block
16(Byte)
102
Third Block
16(Byte)
104
H(C)(1～8)
H(D2)(1～8)
H(C)(9～16)
H(D2)(9～16)
H(C) (17～20)
P (4)
H(D2) (17～20)
P (4)
H(D1')を キーとして暗号化
H(D1')を キーとして暗号化
H(D1')を キーとして暗号化

【図６】


チャレンジ発行処理
S50
NO
チャレンジが要求されたか？
YES
・チャレンジ値を生成する
・チャレンジ値を出力する
S52
S54
記憶装置のチャレンジ値の個数は上限？
YES
S56
NO
最も古いチャレンジ値を削除する
生成したチャレンジ値を記憶する
S58
END

【図７】


パスワード変更処理（複合機）
暗号化された組合せデータを旧パスワード(H(D1))をキーとして復号する
S60
S62
復号されたチャレンジ値が記憶されているチャレンジ値に一致？
YES
NO
S64
パスワードを変更する
結果を出力する
S66
END

フロントページの続き

(56)参考文献 特開平０８－３２０８４７（ＪＰ，Ａ）
特表２００５－５０９９３８（ＪＰ，Ａ）
特開２００１－２６５７３１（ＪＰ，Ａ）
特開２００１－２６５７３５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｈ０４Ｌ　９／３２