(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4479703号
(P4479703)
(45)発行日　平成22年6月9日(2010.6.9)　(24)登録日　平成22年3月26日(2010.3.26)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 673A
G09C 1/00 (2006.01)　　H04L 9/00 675A
　　G09C 1/00 640E

請求項の数 10　(全 28 頁)

(21)出願番号　特願2006-232002(P2006-232002)
(22)出願日　平成18年8月29日(2006.8.29)
(65)公開番号　特開2008-60671(P2008-60671A)
(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8日(2007.8.8)

(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　速水　雄太

最終頁に続く

(54)【発明の名称】通信システムと管理装置

(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管理装置とを備える通信システムであり、
管理装置は、
旧パスワードを入力する旧パスワード入力手段と、
新パスワードを入力する新パスワード入力手段と、
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、
旧パスワードをキーとして、所定のデータ量を単位データ量とするブロック単位でデータを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データを情報処理装置に出力するデータ出力手段とを有し、
暗号化手段は、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するとともに、新パスワードを少なくとも２つの分割所定データに分割し、
暗号化手段は、ブロック単位で暗号化されるべき前記データを構成する複数のブロックが、以下の（１）～（４）、即ち、
（１）前記複数のブロックが、第１種類のブロックと、２以上の第２種類のブロックとを含んでいる、

（２）前記第１種類のブロックが、分割チャレンジデータ及び分割所定データのそれぞれを特定するためのデータ特定情報を含んでいる、
（３）前記２以上の第２種類のブロックのそれぞれのブロックが、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つの分割所定データの両方を含んでいる、
（４）前記２以上の第２種類のブロックのうちの少なくとも１つのブロックが、ダミーデータをさらに含んでいる、
を満たすように前記データを作成し、
情報処理装置は、
旧パスワードを記憶するパスワード記憶手段と、
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データを入力するデータ入力手段と、
データ入力手段に入力された暗号化された前記データを、パスワード記憶手段に記憶されている旧パスワードをキーとして、ブロック毎に復号する復号手段と、
復号手段によって復号された前記第１種類のブロックに基づいて前記２以上の第２種類のブロックから再現される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、パスワード記憶手段に記憶されている旧パスワードを、復号手段によって復号された前記第１種類のブロックに基づいて前記２以上の第２種類のブロックから再現される新パスワードに更新し、両者が一致しない場合は、旧パスワードを更新することを禁止するデータ利用手段とを有する
ことを特徴とする通信システム。
【請求項２】
チャレンジ出力手段は、ハッシュ化されたチャレンジデータを作成し、そのハッシュ化されたチャレンジデータを管理装置に出力し、
チャレンジ記憶手段は、チャレンジ出力手段から出力されたハッシュ化されたチャレンジデータを記憶し、
チャレンジ入力手段は、情報処理装置から出力されたハッシュ化されたチャレンジデータを入力し、
暗号化手段は、新パスワードをハッシュ化してハッシュ化所定データを作成し、ハッシュ化されたチャレンジデータを少なくとも２つの分割ハッシュ化チャレンジデータに分割し、ハッシュ化所定データを少なくとも２つの分割ハッシュ化所定データに分割し、
前記第１種類のブロックに含まれるデータ特定情報は、分割ハッシュ化チャレンジデータ及び分割ハッシュ化所定データのそれぞれを特定するための情報であり、
前記２以上の第２種類のブロックのそれぞれのブロックに含まれる分割チャレンジデータは、分割ハッシュ化チャレンジデータであり、
前記２以上の第２種類のブロックのそれぞれのブロックに含まれる分割所定データは、分割ハッシュ化所定データである
ことを特徴とする請求項１の通信システム。
【請求項３】
暗号化手段は、前記２以上の第２種類のブロックのそれぞれについて、当該ブロックに含まれる分割ハッシュ化チャレンジデータのデータ量と、当該ブロックに含まれる分割ハッシュ化所定データのデータ量とを等しくする
ことを特徴とする請求項２の通信システム。
【請求項４】
前記単位データ量がＤＳであり、前記２以上の第２種類のブロックのブロック数がｎ（ｎは２以上の整数）であり、ハッシュ化されたチャレンジデータの全データ量とハッシュ化所定データの全データ量のそれぞれがＤＨである場合に、
暗号化手段は、
前記２以上の第２種類のブロックに含まれる（ｎ－１）個のブロック群のそれぞれにつ

いて、当該ブロックに含まれる分割ハッシュ化チャレンジデータのデータ量と当該ブロックに含まれる分割ハッシュ化所定データのデータ量とのそれぞれを（１／２）・ＤＳとし、
残りの１個のブロックに含まれる分割ハッシュ化チャレンジデータのデータ量と、その残りの１個のブロックに含まれる分割ハッシュ化所定データのデータ量のそれぞれを（ＤＨ－（ｎ－１）・（１／２）・ＤＳ）とし、
その残りの１個のブロックに、そのブロックのデータ量をＤＳにするためのダミーデータを含ませる
ことを特徴とする請求項３の通信システム。
【請求項５】
前記単位データ量がＤＳであり、前記２以上の第２種類のブロックのブロック数がｎ（ｎは２以上の整数）であり、チャレンジデータの全データ量がＣＡＬであり、新パスワードの全データ量がＤＡＬであり、ＣＡＬとＤＡＬが異なる場合に、
暗号化手段は、
前記２以上の第２種類のブロックに含まれる（ｎ－１）個のブロック群のそれぞれについて、当該ブロックに含まれる分割チャレンジデータのデータ量をＣＬとし、当該ブロックに含まれる分割所定データのデータ量をＤＬとし、ＣＬとＤＬの和をＤＳとし、
残りの１個のブロックに、（ＣＡＬ－（ｎ－１）・ＣＬ）のデータ量の分割チャレンジデータと、その分割チャレンジデータのデータ量との和がＣＬになる第１ダミーデータと、（ＤＡＬ－（ｎ－１）・ＤＬ）のデータ量の分割所定データと、その分割所定データのデータ量との和がＤＬになる第２ダミーデータとを含ませる
ことを特徴とする請求項１の通信システム。
【請求項６】
前記データ特定情報は、ＣＬとＤＬの比率を示すデータと、第１ダミーデータのデータ量を示すデータと、第２ダミーデータのデータ量を示すデータとを含んでいる
ことを特徴とする請求項５の通信システム。
【請求項７】
チャレンジデータの全データ量と新パスワードの全データ量が異なる場合に、前記データ特定情報は、チャレンジデータの全データ量を示すデータと新パスワードの全データ量を示すデータを含んでいる
ことを特徴とする請求項１の通信システム。
【請求項８】
暗号化手段は、
新パスワードの全データ量がチャレンジデータの全データ量より多い場合は、前記２以上の第２種類のブロックの少なくとも２つのブロックに、同じ分割所定データを重複して含ませるとともに、
チャレンジデータの全データ量が新パスワードの全データ量より多い場合は、前記２以上の第２種類のブロックの少なくとも２つのブロックに、同じ分割チャレンジデータを重複して含ませる
ことを特徴とする請求項１の通信システム。
【請求項９】
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管理装置であり、
旧パスワードを入力する旧パスワード入力手段と、
新パスワードを入力する新パスワード入力手段と、
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、
旧パスワードをキーとして、所定のデータ量を単位データ量とするブロック単位でデータを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データを情報処理装置に出力するデータ出力手段

とを備え、
暗号化手段は、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するとともに、新パスワードを少なくとも２つの分割所定データに分割し、
暗号化手段は、ブロック単位で暗号化されるべき前記データを構成する複数のブロックが、以下の（１）～（４）、即ち、
（１）前記複数のブロックが、第１種類のブロックと、２以上の第２種類のブロックとを含んでいる、
（２）前記第１種類のブロックが、分割チャレンジデータ及び分割所定データのそれぞれを特定するためのデータ特定情報を含んでいる、
（３）前記２以上の第２種類のブロックのそれぞれのブロックが、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つの分割所定データの両方を含んでいる、
（４）前記２以上の第２種類のブロックのうちの少なくとも１つのブロックが、ダミーデータをさらに含んでいる、
を満たすように前記データを作成する
ことを特徴とする管理装置。
【請求項１０】
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、
旧パスワードを入力する旧パスワード入力工程と、
新パスワードを入力する新パスワード入力工程と、
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、
旧パスワードをキーとして、所定のデータ量を単位データ量とするブロック単位でデータを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データを情報処理装置に出力するデータ出力工程とを実行させ、
暗号化工程では、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するとともに、新パスワードを少なくとも２つの分割所定データに分割し、
暗号化工程では、ブロック単位で暗号化されるべき前記データを構成する複数のブロックが、以下の（１）～（４）、即ち、
（１）前記複数のブロックが、第１種類のブロックと、２以上の第２種類のブロックとを含んでいる、
（２）前記第１種類のブロックが、分割チャレンジデータ及び分割所定データのそれぞれを特定するためのデータ特定情報を含んでいる、
（３）前記２以上の第２種類のブロックのそれぞれのブロックが、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つの分割所定データの両方を含んでいる、
（４）前記２以上の第２種類のブロックのうちの少なくとも１つのブロックが、ダミーデータをさらに含んでいる、
を満たすように前記データを作成する
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、その情報処理装置にデータを出力する管理装置を備える通信システムに関する。特に、暗号化されたデータが管理装置から情報処理装置に通信されるシステムに関する。
【背景技術】

【０００２】
ネットワーク上に配置されているデバイス間でデータを通信することが広く行なわれている。デバイス間における認証のために、チャレンジ認証と呼ばれる技術が用いられることがある（例えば特許文献１）。
また、データを暗号化して通信することが広く行なわれている。所定のデータ量を単位データ量とするブロック単位でデータを暗号化する技術が知られている（例えば特許文献２参照）。
【０００３】
【特許文献１】特開２００３－１０１５７０号公報
【特許文献２】特開２００４－１８４５６７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
ネットワーク通信においては、データが通信される過程で、データが損傷することがある。例えば、データ通信中にデータが改ざんされる可能性がある。
本発明は、管理装置と情報処理装置の間で通信されるデータが改ざんされたのか否かを正確に知ることができる技術を提供することを目的とする。
【課題を解決するための手段】
【０００５】
本発明は、情報処理装置と、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管理装置とを備える通信システムである。管理装置は、旧パスワードを入力する旧パスワード入力手段と、新パスワードを入力する新パスワード入力手段と、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、旧パスワードをキーとして、所定のデータ量を単位データ量とするブロック単位でデータを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データを情報処理装置に出力するデータ出力手段とを有する。暗号化手段は、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するとともに、新パスワードを少なくとも２つの分割所定データに分割する。暗号化手段は、ブロック単位で暗号化されるべき前記データを構成する複数のブロックが、以下の（１）～（４）、即ち、（１）前記複数のブロックが、第１種類のブロックと、２以上の第２種類のブロックとを含んでいる、（２）前記第１種類のブロックが、分割チャレンジデータ及び分割所定データのそれぞれを特定するためのデータ特定情報を含んでいる、（３）前記２以上の第２種類のブロックのそれぞれのブロックが、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つの分割所定データの両方を含んでいる、（４）前記２以上の第２種類のブロックのうちの少なくとも１つのブロックが、ダミーデータをさらに含んでいる、を満たすように前記データを作成する。情報処理装置は、旧パスワードを記憶するパスワード記憶手段と、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データを入力するデータ入力手段と、データ入力手段に入力された暗号化された前記データを、パスワード記憶手段に記憶されている旧パスワードをキーとして、ブロック毎に復号する復号手段と、復号手段によって復号された前記第１種類のブロックに基づいて前記２以上の第２種類のブロックから再現される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、パスワード記憶手段に記憶されている旧パスワードを、復号手段によって復号された前記第１種類のブロックに基づいて前記２以上の第２種類のブロックから再現される新パスワードに更新し、両者が一致しない場合は、旧パスワードを更新することを禁止するデータ利用手段とを有する。
図１を参照して、本発明の別の形態の技術の内容を説明する。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、情報処理装置２５と、その情報処理装置２５に所定データ（以下では符号Ｄ２を用いる）を出力する管理装置１０とを備える。

【０００６】

管理装置１０は、チャレンジ入力手段１４と暗号化手段１６と組合せデータ出力手段１８を有する。

チャレンジ入力手段１４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。「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。

暗号化手段１６は、チャレンジ入力手段１４に入力されたチャレンジデータＣＤと上記の所定データＤ２との組合せのデータ（ＣＤ＋Ｄ２）を作成し、その組合せデータ（ＣＤ＋Ｄ２）を、所定のデータ量を単位データ量とするブロック単位で暗号化する。組合せデータの暗号化は、公知の暗号化手法を利用して実行される。また、上記の所定データは、ユーザによって管理装置１０に入力されたものであってもよいし、外部機器から管理装置１０に送られてきたものであってもよいし、管理装置１０に予め記憶されているものであってもよい。なお、以下では、暗号化された組合せデータをＥ（ＣＤ＋Ｄ２）と表現する。

上記の暗号化手段１６は、複数のブロックを利用して暗号化される組合せデータＥ（ＣＤ＋Ｄ２）の少なくとも１つのブロックに、チャレンジデータＣＤの少なくとも一部と所定データＤ２の少なくとも一部の両方を含ませるものである。図２は、組合せデータＥ（ＣＤ＋Ｄ２）の一例を示す。図２の例では、３つのブロック４０ａ，４０ｂ，４０ｃによって組合せデータが暗号化されている。ブロック４０ｂには、チャレンジデータＣＤの一部と所定データＤ２の一部の両方が含まれている。

組合せデータ出力手段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（ＣＤ＋Ｄ２）を情報処理装置２５に出力する。

【０００７】

情報処理装置２５は、チャレンジ出力手段３０とチャレンジ記憶手段３２と組合せデータ入力手段３４と復号手段３６とデータ利用手段３８を有する。

チャレンジ出力手段３０は、チャレンジデータＣＤを管理装置１０に出力する。情報処理装置２５は、例えば、ランダムに１つの数値を選択することによって、チャレンジデータＣＤを生成することができる。

チャレンジ記憶手段３２は、チャレンジ出力手段３０から出力されたチャレンジデータＣＤを記憶しておく。

組合せデータ入力手段３４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（ＣＤ＋Ｄ２）を入力する。

復号手段３６は、組合せデータ入力手段３４に入力された暗号化された組合せデータＥ（ＣＤ＋Ｄ２）をブロック毎に復号する。

データ利用手段３８は、復号手段３６によって復号された組合せデータ（ＣＤ＋Ｄ２）に含まれるチャレンジデータＣＤとチャレンジ記憶手段３２に記憶されているチャレンジデータＣＤとを比較する。データ利用手段３８は、両者が一致した場合は、復号手段３６によって復号された組合せデータ（ＣＤ＋Ｄ２）に含まれる所定データＤ２を利用する。一方において、データ利用手段３８は、両者が一致しない場合は、組合せデータ（ＣＤ＋Ｄ２）に含まれる所定データＤ２を利用することを禁止する。

【０００８】

組合せデータＥ（ＣＤ＋Ｄ２）が通信される過程で上記の所定データＤ２を改ざんしようとして無作為に攻撃が加えられることがある。本発明の通信システム２では、暗号化された組合せデータＥ（ＣＤ＋Ｄ２）の少なくとも１つのブロックに、チャレンジデータＣＤの少なくとも一部と所定データＤ２の少なくとも一部の両方が含まれている。図２の例

では、ブロック４０ｂにチャレンジデータＣＤと所定データＤ２が含まれている。ブロック４０ｂが改ざんされた場合、ブロック４０ｂに含まれるチャレンジデータＣＤが変化する。この場合、その変化したチャレンジデータＣＤ’は、チャレンジ記憶手段３２に記憶されているチャレンジデータＣＤと一致しない。これにより、情報処理装置２５は、組合せデータＥ（ＣＤ＋Ｄ２）が改ざんされたことを知ることができる。

本発明の通信システム２によると、管理装置１０と情報処理装置２５の間で送られるデータが改ざんされたのか否かを従来よりも正確に知ることができるようになることが期待できる。

【０００９】

図３は、組合せデータＥ（ＣＤ＋Ｄ２）の別の例を示す。図３の例では、３つのブロック４２ａ，４２ｂ，４２ｃによって組合せデータが暗号化されている。

暗号化手段１６は、チャレンジ入力手段１４に入力されたチャレンジデータＣＤを少なくとも２つの分割チャレンジデータに分割し、所定データＤ２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ことが好ましい。図３の例では、２つの分割チャレンジデータＣＤ（１），ＣＤ（２）の間に所定データＤ２の一部Ｄ２（１）が配置されている。また、２つの分割チャレンジデータＣＤ（２），ＣＤ（３）の間に所定データＤ２の一部Ｄ２（２）が配置されている。

このようにして組合せデータを作成すると、チャレンジデータＣＤが各ブロックに分散して配置されるようになることが期待できる。

【００１０】

図３に示されるように、暗号化手段１６は、組合せデータＥ（ＣＤ＋Ｄ２）の全てのブロック４２ａ，４２ｂ，４２ｃのそれぞれに、少なくとも１つの分割チャレンジデータＣＤ（１），ＣＤ（２），ＣＤ（３）を含ませることが好ましい。

情報処理装置２５は、いずれのブロック４２ａ，４２ｂ，４２ｃが改ざんされたとしても、組合せデータが改ざんされたことを知ることができる。

【００１１】

図４は、組合せデータＥ（ＣＤ＋Ｄ２）の別の例を示す。図４の例では、３つのブロック４４ａ，４４ｂ，４４ｃによって組合せデータが暗号化されている。

図４に示されるように、暗号化手段１６は、所定データＤ２を少なくとも２つの分割所定データＤ２（１），Ｄ２（２），Ｄ２（３）に分割し、組合せデータＥ（ＣＤ＋Ｄ２）の全てのブロック４４ａ，４４ｂ，４４ｃ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つの分割所定データの両方を含ませてもよい。

【００１２】

上記の通信システム２は、管理装置１０からの指示に応じて情報処理装置２５がパスワードを更新するシステムに好適に利用することができる。図１を参照しながら、このシステムの構成を説明する。

管理装置１０は、ユーザによって入力された新パスワード（これも符号「Ｄ２」で表現する）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パスワードＤ１を更新する。

管理装置１０は、旧パスワードＤ１を入力する旧パスワード入力手段２０と、新パスワードＤ２を入力する新パスワード入力手段２２とをさらに有する。上記の所定データＤ２は、新パスワードのことである。上記の旧パスワード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、旧パスワードＤ１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パスワードＤ１を新パスワードＤ２に更新する際に、自身が記憶している旧パスワードＤ１を管理装置１０に入力することができる。一方において、ユーザは、旧パスワードＤ１を新パスワードＤ２に更新する場合に、旧パスワードＤ１を管理装置１０に入力しなくてもよい。管理装置１０は、ユーザによって過去に入力された旧パスワードＤ１を継続して記憶しておいてもよい。なお、旧パスワード入力手段２０と新パスワード入力手段２２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、旧パスワード入力手段２０に入力された旧パスワードＤ１をキーとして組合せデータ（ＣＤ＋Ｄ２）を暗号化する。以下では、Ｄ１をキーとして暗号化された組合せデータをＥ（ＣＤ＋Ｄ２，Ｄ１）と表現する。
【００１３】
情報処理装置２５は、旧パスワードＤ１を記憶しているパスワード記憶手段４０をさらに有する。旧パスワード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。
復号手段３６は、暗号化された組合せデータＥ（ＣＤ＋Ｄ２，Ｄ１）を、パスワード記憶手段３０に記憶されている旧パスワードＤ１をキーとして復号する。
データ利用手段３８は、復号手段３６によって復号された組合せデータ（ＣＤ＋Ｄ２）に含まれるチャレンジデータＣＤとチャレンジ記憶手段３２に記憶されているチャレンジデータＣＤとを比較し、両者が一致した場合は、パスワード記憶手段３０に記憶されている旧パスワードＤ１を復号手段３６によって復号された組合せデータ（ＣＤ＋Ｄ２）に含まれる新パスワードＤ２に更新し、両者が一致しない場合は、旧パスワードＤ１を更新することを禁止する。
【００１４】
上記の通信システム２では、ハッシュ化されたデータを利用してもよい。データをハッシュ化すると、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。ハッシュ化されたデータを利用する場合、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。
【００１５】
チャレンジ出力手段３０は、ハッシュ化されたチャレンジデータ（以下ではＨ（ＣＤ）と表現する）を作成し、そのハッシュ化されたチャレンジデータＨ（ＣＤ）を管理装置１０に出力する。以下では、ハッシュ化されたチャレンジデータのことを「ハッシュ化チャレンジデータ」と呼ぶ。
チャレンジ記憶手段３２は、チャレンジ出力手段３０から出力されたハッシュ化チャレンジデータＨ（ＣＤ）を記憶しておく。
チャレンジ入力手段１４は、情報処理装置２５から出力されたハッシュ化チャレンジデータＨ（ＣＤ）を入力する。
暗号化手段１６は、所定データＤ２をハッシュ化してハッシュ化所定データ（以下ではＨ（Ｄ２）と表現する）を作成し、そのハッシュ化所定データＨ（Ｄ２）とチャレンジ入力手段１４に入力されたハッシュ化チャレンジデータＨ（ＣＤ）とから上記の組合せデータ（Ｈ（ＣＤ）＋Ｈ（Ｄ２））を作成する。なお、図１では、組合せデータ（Ｈ（ＣＤ）＋Ｈ（Ｄ２））が暗号化されたものをＥ（Ｈ（ＣＤ）＋Ｈ（Ｄ２））と表現している。
データ利用手段３８は、復号手段３６によって復号された組合せデータ（Ｈ（ＣＤ）＋Ｈ（Ｄ２））に含まれるハッシュ化チャレンジデータＨ（ＣＤ）とチャレンジ記憶手段３２に記憶されているハッシュ化チャレンジデータＨ（ＣＤ）とを比較し、両者が一致した場合は、復号手段３６によって復号された組合せデータ（Ｈ（ＣＤ）＋Ｈ（Ｄ２））に含まれるハッシュ化所定データＨ（Ｄ２）を利用し、両者が一致しない場合は、組合せデータ（Ｈ（ＣＤ）＋Ｈ（Ｄ２））に含まれるハッシュ化所定データＨ（ＣＤ）を利用することを禁止する。
【００１６】
暗号化手段１６は、ハッシュ化チャレンジデータＨ（ＣＤ）を少なくとも２つの分割ハッシュ化チャレンジデータに分割してもよい。暗号化手段１６は、ハッシュ化所定データＨ（Ｄ２）を少なくとも２つの分割ハッシュ化所定データに分割してもよい。暗号化手段１６は、組合せデータＥ（Ｈ（ＣＤ）＋Ｈ（Ｄ２））の全てのブロックのそれぞれに、少なくとも１つの分割ハッシュ化チャレンジデータと少なくとも１つの分割ハッシュ化所定データの両方を含ませてもよい。

この場合、暗号化手段１６は、組合せデータＥ（Ｈ（ＣＤ）＋Ｈ（Ｄ２））の全てのブロックのそれぞれについて、当該ブロックに含まれる分割ハッシュ化所定データのデータ量と、当該ブロックに含まれる分割ハッシュ化チャレンジデータのデータ量とを等しくしてもよい。

このようにすると、組合せデータの構成を単純化することができる。組合せデータを作成して暗号化するための処理が容易になることが期待できる。組合せデータを復号してチャレンジデータと所定データを再現するための処理が容易になることが期待できる。

【００１７】

図５は、組合せデータＥ（Ｈ（ＣＤ）＋Ｈ（Ｄ２））の別の例を示す。図５の例では、ｎ個のブロック４６－１～４６－ｎによって組合せデータが暗号化されている。ここでは、暗号化の単位となる単位データ量をＤＳとし、組合せデータのブロック数をｎ（ｎは２以上の整数）とし、ハッシュ化チャレンジデータＨ（ＣＤ）の全データ量とハッシュ化所定データＨ（Ｄ２）の全データ量のそれぞれをＤＨとする。

この場合、暗号化手段１６は、（ｎ－１）個のブロック群のそれぞれについて、当該ブロック（例えば４６－１）に含まれる分割ハッシュ化チャレンジデータ（例えばＣＤ（１））のデータ量と、当該ブロック（例えば４６－１）に含まれる分割ハッシュ化所定データ（例えばＤ２（１））のデータ量のそれぞれを（１／２）・ＤＳとしてもよい。

また、暗号化手段１６は、残りの１個のブロック（図５の例では４６－ｎ）に含まれる分割ハッシュ化チャレンジデータＣＤ（ｎ）のデータ量と、その残りの１個のブロック４６－ｎに含まれる分割ハッシュ化所定データＤ２（ｎ）のデータ量のそれぞれを（ＤＨ－（ｎ－１）・（１／２）・ＤＳ）としてもよい。

暗号化手段１６は、その残りの１個のブロック４６－ｎに、そのブロック４６－ｎのデータ量をＤＳにするためのダミーデータＰ（１），Ｐ（２）を含ませてもよい。

この構成は、ハッシュ化されたデータＨ（Ｄ２），Ｈ（ＣＤ）のデータ量が、単位データ量Ｄ２の整数倍にならない場合に、有効に利用することができる。

【００１８】

図６（ａ）は、組合せデータＥ（ＣＤ＋Ｄ２）の別の例を示す。図６（ａ）の例では、ｎ個のブロック４８－１～４８－ｎによって組合せデータが暗号化されている。この例では、チャレンジデータＣＤと所定データＤ２がハッシュ化されていない。ここでは、単位データ量をＤＳとし、組合せデータのブロック数をｎ（ｎは２以上の整数）とし、チャレンジデータＣＤの全データ量をＣＡＬとし、所定データＤ２の全データ量をＤＡＬとする。ＣＡＬとＤＡＬは、異なるデータ量である。

この場合、暗号化手段１６は、（ｎ－１）個のブロック群のそれぞれについて、当該ブロックに含まれる分割チャレンジデータのデータ量をＣＬとし、当該ブロックに含まれる分割所定データのデータ量をＤＬとし、ＣＬとＤＬの和をＤＳとする。例えば、ブロック４８－１に含まれるＣＤ（１）がＣＬであり、Ｄ２（１）がＤＬである。

暗号化手段１６は、残りの１個のブロック（図６の例では４８－ｎ）に、（ＣＡＬ－（ｎ－１）・ＣＬ）のデータ量の分割チャレンジデータＣＤ（ｎ）と、その分割チャレンジデータＣＤ（ｎ）のデータ量との和がＣＬになる第１ダミーデータＰ（１）と、（ＤＡＬ－（ｎ－１）・ＤＬ）のデータ量の分割所定データＤ２（ｎ）と、その分割所定データＤ２（ｎ）のデータ量との和がＤＬになる第２ダミーデータＰ（２）とを含ませてもよい。

【００１９】

図６（ａ）に例示された構成を採用する場合、組合せデータ出力手段１８は、図６（ｂ）に例示されるデータを情報処理装置２５に出力してもよい。即ち、組合せデータ出力手段１８は、ＣＬとＤＬの比率αを示すデータ（Ｄ（α））と、第１ダミーデータＰ（１）のデータ量を示すデータＤ（Ｐ（１））と、第２ダミーデータＰ（２）のデータ量を示すデータＤ（Ｐ（２））を、組合せデータとは別に情報処理装置２５に出力する。

上記の「組合せデータとは別に」という記載は、各ブロック４８－１～４８－ｎの中に上記の情報データ（Ｄ（α）等）を含ませないことを意味している。この記載は、情報データと組合せデータを一連のデータ列として出力することを排除しているものではない。

また、上記の情報データは、図６（ｂ）に示されるように、１つのブロック５０として暗号化されてもよい。

また、Ｄ（α）は、１つのブロックに含まれる分割所定データのデータ量を示すデータと、１つ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を示すデータに分かれていてもよい。

上記の情報データが情報処理装置２５に出力されるために、情報処理装置２５は、組合せデータ（ＣＤ＋Ｄ２）からチャレンジデータＣＤと所定データＤ２を再現することができる。この構成によると、チャレンジデータＣＤの全データ量と所定データＤ２の全データ量が異なる場合でも、情報処理装置２５がチャレンジデータＣＤと所定データＤ２を再現することができる。

【００２０】

なお、組合せデータ出力手段１８は、上記の情報データのＤ（Ｐ１）とＤ（Ｐ２）の代わりに、チャレンジデータＣＤの全データ量ＣＡＬを示すデータと所定データＤ２の全データ量ＤＡＬを示すデータを情報処理装置２５に出力してもよい。

この場合も、情報処理装置２５がチャレンジデータＣＤと所定データＤ２を再現することができる。

【００２１】

図７は、組合せデータＥ（ＣＤ＋Ｄ２）の別の例を示す。図７の例では、ｎ個のブロック５２－１～５２－ｎによって組合せデータが暗号化されている。ここでは、チャレンジデータＣＤの全データ量と所定データＤ２の全データ量が異なるものとする。

この場合、暗号化手段１６は、組合せデータＥ（ＣＤ＋Ｄ２）の全てのブロック５２－１～５２－ｎのそれぞれに、当該ブロック（例えば５２－１）に含まれる分割チャレンジデータ（例えばＣＤ（１））のデータ量を示すデータ（例えばＣＬ（１））と、当該ブロック（例えば５２－１）に含まれる分割所定データ（例えばＤ２（１））のデータ量を示すデータ（例えばＤＬ（１））とを含ませてもよい。

情報処理装置２５は、ＣＬ（１）～ＣＬ（ｎ）を読み込むことによって、各ブロックに含まれる分割チャレンジデータＣＤ（１）～ＣＤ（ｎ）のデータ量を知ることができる。このために、各ブロックからチャレンジデータＣＤを再現することができる。情報処理装置２５は、ＤＬ（１）～ＤＬ（ｎ）を読み込むことによって、各ブロックに含まれる分割所定データＤ２（１）～Ｄ２（ｎ）のデータ量を知ることができる。このために、各ブロックから所定データＤ２を再現することができる。

【００２２】

また、暗号化手段１６は、組合せデータＥ（ＣＤ＋Ｄ２）の少なくとも１つのブロックに、ダミーデータと、そのダミーデータのデータ量を示すデータとを含ませてもよい。

この場合、情報処理装置２５は、ダミーデータが含まれていることと、そのダミーデータのデータ量を知ることができる。

【００２３】

チャレンジデータＣＤの全データ量と所定データＤ２の全データ量が異なる場合に、組合せデータ出力手段１８は、チャレンジデータＣＤの全データ量を示すデータと、所定データＤ２の全データ量を示すデータとを情報処理装置２５に出力してもよい。

情報処理装置２５は、チャレンジデータＣＤの全データ量と所定データＤ２の全データ量を知ることができる。情報処理装置２５は、これらの情報からチャレンジデータＣＤと所定データＤ２を再現することができる。

なお、全データ量を示すデータは、組合せデータの中に含ませてもよいし（即ちブロックの中に含ませてもよいし）、組合せデータとは別に出力されてもよい。

【００２４】

暗号化手段１６は、所定データＤ２の全データ量がチャレンジデータＣＤの全データ量より多い場合は、組合せデータＥ（ＣＤ＋Ｄ２）の少なくとも２つのブロックに、同じ分割所定データを重複して含ませてもよい。また、暗号化手段１６は、チャレンジデータＣＤの全データ量が所定データＤ２の全データ量より多い場合は、組合せデータＥ（ＣＤ＋

Ｄ２）の少なくとも２つのブロックに、同じ分割チャレンジデータを重複して含ませてもよい。

この構成は、所定データＤ２の全データ量とチャレンジデータＣＤの全データ量が異なる場合に有効に利用することができる。

【００２５】

本発明の管理装置は、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。この管理装置は、旧パスワードを入力する旧パスワード入力手段と、新パスワードを入力する新パスワード入力手段と、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、旧パスワードをキーとして、所定のデータ量を単位データ量とするブロック単位でデータを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データを情報処理装置に出力するデータ出力手段とを備える。暗号化手段は、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するとともに、新パスワードを少なくとも２つの分割所定データに分割する。暗号化手段は、ブロック単位で暗号化されるべき前記データを構成する複数のブロックが、以下の（１）～（４）、即ち、（１）前記複数のブロックが、第１種類のブロックと、２以上の第２種類のブロックとを含んでいる、（２）前記第１種類のブロックが、分割チャレンジデータ及び分割所定データのそれぞれを特定するためのデータ特定情報を含んでいる、（３）前記２以上の第２種類のブロックのそれぞれのブロックが、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つの分割所定データの両方を含んでいる、（４）前記２以上の第２種類のブロックのうちの少なくとも１つのブロックが、ダミーデータをさらに含んでいる、を満たすように前記データを作成する。

次の管理装置１０も有用である。この管理装置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、その情報処理装置２５に所定データを出力する。

この管理装置１０は、図１に例示されるチャレンジ入力手段１４と暗号化手段１６と組合せデータ出力手段１８を有する。この暗号化手段１８は、複数のブロックを利用して暗号化される組合せデータＥ（ＣＤ＋Ｄ２）の少なくとも１つのブロックに、チャレンジデータＣＤの少なくとも一部と所定データＤ２の少なくとも一部の両方を含ませる。

【００２６】

本発明のコンピュータプログラムは、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管理装置を実現するためのものである。このコンピュータプログラムは、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、旧パスワードを入力する旧パスワード入力工程と、新パスワードを入力する新パスワード入力工程と、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、旧パスワードをキーとして、所定のデータ量を単位データ量とするブロック単位でデータを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データを情報処理装置に出力するデータ出力工程とを実行させる。暗号化工程では、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するとともに、新パスワードを少なくとも２つの分割所定データに分割する。暗号化工程では、ブロック単位で暗号化されるべき前記データを構成する複数のブロックが、以下の（１）～（４）、即ち、（１）前記複数のブロックが、第１種類のブロックと、２以上の第２種類のブロックとを含んでいる、（２）前記第１種類のブロックが、分割チャレンジデータ及び分割所定データのそれぞれを特定するためのデータ特定情報を含んでいる、（３）前記２以上の第２種類のブロックのそれぞれのブロックが、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つの分割所定データの両方を含んでいる、（４）前記２以上の第２種類のブロックのうちの少なくとも１つのブロックが、ダミーデータをさらに含んでいる、を満たすように前記データを作成する。

上記の管理装置１０のためのコンピュータプログラムも、本発明の別の形態の創作物の１つである。このコンピュータプログラムは、管理装置１０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）情報処理装置２５からのチャレンジデータＣＤと所定データＤ２との組合せのデータ（ＣＤ＋Ｄ２）を作成し、その組合せデータ（ＣＤ＋Ｄ２）を、所定のデータ量を単位データ量とするブロック単位で暗号化する暗号化工程。
この暗号化工程では、複数のブロックを利用して暗号化される組合せデータＥ（ＣＤ＋Ｄ２）の少なくとも１つのブロックに、チャレンジデータＣＤの少なくとも一部と所定データＤ２の少なくとも一部の両方を含ませる。
（２）暗号化工程で暗号化された組合せデータＥ（ＣＤ＋Ｄ２）を情報処理装置２５に出力する組合せデータ出力工程。
【発明を実施するための最良の形態】
【００２７】
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機能を実行することを許容する。
（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。
（形態５）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所定データを再現（特定）するためのルールを記憶している。
【実施例】
【００２８】
（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８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。
【００２９】
（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８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。

【００３０】

（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。

【００３１】

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。この場合、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。

【００３２】

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。

【００３３】

（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９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８参照）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８参照）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。

【００３４】

（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。

【００３５】

（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８参照）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８参照）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。
【００３６】
（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１０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８参照）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８参照）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９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。複合機８０は、ユーザによって入力された旧パスワードＤ１’がパスワード記憶領域８６ｂ（図８参照）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。
【００３７】
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９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９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。次いで、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９のＡ９に相当する。

【００３８】

図１１を参照して、Ｓ３４の処理の内容を詳しく説明する。

図１１（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１１（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１１（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。

【００３９】

（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バイト目から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。

【００４０】

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が等しい。

【００４１】

図１０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９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８参照）に表示する（Ｓ４０）。

【００４２】

（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１２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８参照）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１０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９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８参照）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）。

【００４３】

（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１３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８参照）によって実行される。

複合機８０は、図１０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（図１１（ｃ）参照）によって構成されている。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８６

ｂ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。

【００４４】

複合機８０の再現ルール記憶領域８６ｃ（図８参照）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。

【００４５】

上記の図１３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９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８参照）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１２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９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９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１０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。

【００４６】

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。

【００４７】

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。特に、本実施例では、全てのブロック１００，１０２，１０４（図１１（ｃ）参照）に分割チャレンジデータが含まれている。このために、いずれのブロック１００，１０２，１０４が改ざんされても、パスワードが更新されない。

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。

【００４８】

（第２実施例）

上記の第１実施例では、ハッシュ化されたチャレンジデータＨ（Ｃ）とハッシュ化された新パスワードＨ（Ｄ２）から組合せデータ（Ｈ（Ｃ）＋Ｈ（Ｄ２））が作成される。ハッシュ化チャレンジデータＨ（Ｃ）とハッシュ化新パスワードＨ（Ｄ２）は、データ量が等しい。このために、第１実施例では、組合せデータのデータ構造を簡略化することができると言える。これに対し、以下の各実施例では、ハッシュ化されたデータが利用されない。このために、チャレンジデータのデータ量と新パスワードのデータ量が異なる可能性が高い。以下の各実施例では、チャレンジデータのデータ量と新パスワードのデータ量が異なるものとして説明する。

【００４９】

図９を参照しながら、第１実施例と異なる点を以下に列挙する。図９の各処理の中で第１実施例と異なるものをダッシュを付けて説明する。

（Ａ１’）複合機８０のパスワード記憶領域８６ｂ（図８参照）は、ハッシュ化されていないパスワードＤ１を記憶している。

（Ａ５’）複合機８０は、チャレンジデータ（以下では「ＣＤ」と記載する）を生成するが、チャレンジデータＣＤをハッシュ化しない。複合機８０のチャレンジ記憶領域８６ａ（図８参照）は、ハッシュ化されていないチャレンジデータＣＤを記憶する。

（Ａ７’）管理装置６０は、ユーザによって入力された旧パスワードＤ１’をハッシュ化しない。

（Ａ８’）管理装置６０は、ユーザによって入力された新パスワードＤ２をハッシュ化しない。

（Ａ９’）管理装置６０は、ハッシュ化されていないチャレンジデータＣＤとハッシュ化されていない新パスワードＤ２から組合せデータ（ＣＤ＋Ｄ２）を生成する。組合せデータ（ＣＤ＋Ｄ２）は、ハッシュ化されていない旧パスワードＤ１’によってブロック単位で暗号化される。暗号化された組合せデータをＥ（ＣＤ＋Ｄ２，Ｄ１’）と表現する。

【００５０】

図１４を参照して、上記のＡ９’の処理の内容を詳しく説明する。図１４（ａ）は、チャレンジデータＣＤを示す。図１４（ｂ）は、新パスワードＤ２を示す。チャレンジデータＣＤと新パスワードＤ２は、データ量が異なる。

図１４（ｃ）は、情報ブロック１３０と、暗号化された組合せデータＥ（ＣＤ＋Ｄ２，Ｄ１’）を示す。組合せデータＥ（ＣＤ＋Ｄ２，Ｄ１’）は、ｎ個のブロック１３２，１３４等によって構成されている。

ｎ番目のブロック１３４以外の各ブロックは、データ量ＣＬの分割チャレンジデータと、データ量ＤＬの分割パスワードデータを含んでいる。例えば、ブロック１３２に含まれる分割チャレンジデータＣＤ（１）のデータ量はＣＬであり、分割パスワードデータＤ２（１）のデータ量はＤＬである。ｎ番目のブロック１３４以外の各ブロックには、分割チャレンジデータと分割パスワードデータのみが含まれている。即ち、ダミーデータが含まれていない。

ｎ番目のブロック１３４は、分割チャレンジデータＣＤ（ｎ）とチャレンジ用ダミーデータＣＰと分割パスワードデータＤ２（ｎ）とパスワード用ダミーデータＤＰを含んでいる。ＣＤ（ｎ）とＣＰの和はＣＬである。Ｄ２（ｎ）とＤＰの和はＤＬである。

【００５１】

情報ブロック１３０は、４種類のデータＣＬ，ＣＰＬ，ＤＬ，ＤＰＬを含んでいる。ＣＬは、１ブロックに含まれる分割チャレンジデータのデータ量（即ちＣＤ（１）のデータ量）を示す。ＣＰＬは、チャレンジ用ダミーデータＣＰのデータ量を示す。ＤＬは、１ブロックに含まれる分割パスワードデータのデータ量（即ちＤ２（１）のデータ量）を示す。ＤＰＬは、パスワード用ダミーデータＤＰのデータ量を示す。

情報ブロック１３０とｎ個のブロック１３２，１３４等のそれぞれは、旧パスワードＤ１’をキーとして暗号化される。

【００５２】

（Ａ１０’）図１４（ｃ）に示される一連のデータ列（情報ブロック１３０と組合せデータ（ＣＤ＋Ｄ２））が、複合機８０に出力される。

（Ａ１１’）複合機８０は、パスワード記憶領域８６ｂ（図８参照）に記憶されている旧パスワードＤ１をキーとして、暗号化されたデータ列をブロック毎に復号する。複合機８０は、復号された組合せデータ（ＣＤ＋Ｄ２）からチャレンジデータＣＤと新パスワードＤ２を再現する。複合機８０の再現ルール記憶領域８６ｃは、以下の再現ルールを記憶している。

（１）情報ブロック１３０を読み込むことによって、ＣＬ，ＣＰＬ，ＤＬ，ＤＰＬがわかる。

（２）１番目から（ｎ－１）番目までの各ブロックに含まれる分割チャレンジデータのデータ量はＣＬである。

（３）１番目から（ｎ－１）番目までの各ブロックに含まれる分割パスワードデータのデータ量はＤＬである。

（４）ｎ番目のブロックに含まれる分割チャレンジデータＣＤ（ｎ）のデータ量は、ＣＬからＣＰＬを減算した値である。

（５）ｎ番目のブロックに含まれる分割パスワードデータＤ２（ｎ）のデータ量は、ＤＬからＤＰＬを減算した値である。

（６）各ブロック１３２，１３４等に含まれる分割チャレンジデータを順に並べれば、チャレンジデータＣＤを再現することができる。

（７）各ブロック１３２，１３４等に含まれる分割パスワードデータを順に並べれば、新パスワードＤ２を再現することができる。

【００５３】

（Ａ１２’）上記のＡ１１’で再現されたチャレンジデータＣＤは、ハッシュ化されたものではない。複合機８０は、再現されたチャレンジデータＣＤが、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ＣＤと一致するのか否かを判断する。

（Ａ１３’）複合機８０は、Ａ１２’において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に記憶されているパスワードＤ１をＡ１１’で再現された新パスワードＤ２に更新する。

【００５４】

本実施例では、（ｎ－１）個のブロック群については、分割チャレンジデータのデータ量がＣＬである。また、ｎ番目のブロック１３４については、分割チャレンジデータＣＤ（ｎ）のデータ量とチャレンジ用ダミーデータＣＰのデータ量の和がＣＬである。ｎ個のブロック群は、チャレンジデータＣＤのためのデータ量（分割チャレンジデータとチャレンジ用ダミーデータの和）が一定化されていると言える。同様に、ｎ個のブロック群は、新パスワードＤ２のためのデータ量（分割パスワードデータとパスワード用ダミーデータの和）が一定化されていると言える。本実施例では、チャレンジデータＣＤのデータ量と新パスワードＤ２のデータ量が異なる場合であっても、組合せデータの各ブロックを規則的なデータ構成にすることができる。この場合、管理装置６０が組合せデータを作成し易い。また、複合機８０がチャレンジデータＣＤや新パスワードＤ２を再現し易くなる。

なお、上記の情報ブロック１３０は、ＣＰＬの代わりに、チャレンジデータＣＤの全データ量を示すデータを含んでいてもよい。また、情報ブロック１３０は、ＤＰＬの代わりに、新パスワードＤ２の全データ量を示すデータを含んでいてもよい。

【００５５】

（第３実施例）

本実施例では、組合せデータ（ＣＤ＋Ｄ２）のデータ構成が第２実施例と異なる。図１５は、本実施例の組合せデータ（ＣＤ＋Ｄ２）を示す。

本実施例では、ｎ個のブロック１４０，１４２，１４４等によって組合せデータ（ＣＤ＋Ｄ２）が暗号化されている。分割チャレンジデータ（例えばＣＤ（１））のデータ量と、分割パスワードデータ（例えばＤ２（１））のデータ量は、ブロック毎に異なる。

各ブロック１４０，１４２，１４４等は、分割チャレンジデータと分割パスワードデータの他に、４種類の情報データを含んでいる。例えば、第１ブロック１４０は、ＣＬ１とＣＰＬ１とＤＬ１とＤＰＬ１を含んでいる。ＣＬ１は、第１ブロック１４０に含まれる分割チャレンジデータＣＤ（１）のデータ量を示す。ＣＰＬ１は、第１ブロック１４０に含まれるチャレンジ用ダミーデータのデータ量を示す。ＤＬ１は、第１ブロック１４０に含まれる分割パスワードデータＤ２（１）のデータ量を示す。ＤＰＬ１は、第１ブロック１４０に含まれるパスワード用ダミーデータのデータ量を示す。なお、第１ブロック１４０にはチャレンジ用ダミーデータとパスワード用ダミーデータが含まれていないために、ＣＰＬ１とＤＰＬ１は、ゼロというデータ量を示すデータである。

他のブロック１４２，１４４等も、ブロック１４０と同様のデータ構成を有する。

【００５６】

複合機８０は、各ブロックに含まれている情報データ（ＣＬ，ＣＰＬ，ＤＬ，ＤＰＬ）に基づいて、チャレンジデータＣＤとパスワードＤ２を再現することができる。

本実施例では、最後のブロック１４４のみがダミーデータＣＰ，ＤＰを含んでいる。他のブロック１４０，１４２等は、ダミーデータを含んでいないにもかかわらず、ダミーデータのデータ量（即ちゼロ）を示すデータ（例えばＣＰＬ１，ＤＰＬ１等）を含んでいる。このようにすると、全てのブロックに同じ種類の情報データ（ＣＬ，ＣＰＬ，ＤＬ，ＤＰＬ）を含ませることができる。この場合、複合機８０が同じ手順で各ブロック１４０，１４４等を読み込むことによって、チャレンジデータＣＤや新パスワードＤ２を再現することができる。複合機８０が各データを容易に再現することができるものと思われる。

なお、本実施例では、最後のブロック１４４のみがダミーデータＣＰ，ＤＰを含んでいる。しかしながら、他のブロック１４２，１４４等にもダミーデータＣＰ，ＤＰを含ませてもよい。また、ダミーデータが含まれていないブロックは、ＣＰＬやＤＰＬを含んでいなくてもよい。

【００５７】

（第４実施例）

図１６は、本実施例の組合せデータ（ＣＤ＋Ｄ２）を示す。

本実施例では、（ｍ＋１０）個のブロック１５２，１５４，１５６等によって組合せデータ（ＣＤ＋Ｄ２）が暗号化されている。情報ブロック１５０が生成される点は、第２実施例と同様である。

情報ブロック１５０は、第２実施例で説明した４種類のデータ（ＣＬ，ＣＰＬ，ＤＰ，ＤＰＬ）に加えて、ＣＡＬとＤＡＬを含んでいる。ＣＡＬは、チャレンジデータＣＤの全データ量を示すデータである。ＤＡＬは、新パスワードＤ２の全データ量を示すデータである。

１番目から（ｍ－１）番目までの各ブロックに含まれる分割チャレンジデータのデータ量は一定である（即ちＣＬである）。ｍ番目の分割チャレンジデータＣＤ（ｍ）のデータ量は、ＣＬではない。ＣＤ（ｍ）のデータ量とチャレンジ用ダミーデータＣＰのデータ量の和はＣＬである。（ｍ＋１）番目から（ｍ＋１０）番目までの各ブロックに含まれる分割チャレンジデータのデータ量も一定である（即ちＣＬである）。

１番目から（ｍ＋９）番目までの各ブロックに含まれる分割パスワードデータのデータ量は一定である（即ちＤＬである）。（ｍ＋１０）番目の分割パスワードデータＤ２（ｍ＋１０）のデータ量は、ＤＬではない。Ｄ２（ｍ＋１０）とパスワード用ダミーデータＤＰの和はＤＬである。

【００５８】

本実施例では、新パスワードＤ２は、（ｍ＋１０）個の分割パスワードデータに分割されている。１つのブロックは、１つの分割パスワードデータを含んでいる。新パスワードＤ２を再現するためには、１番目から（ｍ＋１０）番目までのブロックが必要となる。一方において、チャレンジデータＣＤは、ｍ個の分割チャレンジデータに分割されている。従って、１番目からｍ番目までのブロックに含まれている分割チャレンジデータからチャレンジデータＣＤを再現することができる。（ｍ＋１）番目から（ｍ＋１０番目）までには、１番目から１０番目のブロックに含まれている分割チャレンジデータが含まれている。例えば、（ｍ＋１）番目には、ＣＤ（１）が含まれている。また、例えば、（ｍ＋１０）番目には、ＣＤ（１０）が含まれている。

【００５９】

複合機８０は、情報ブロック１５０に含まれているＣＬとＣＰＬとＣＡＬからチャレンジデータＣＤを再現することができる。複合機８０は、１番目からｍ番目までのブロックに含まれている分割チャレンジデータからチャレンジデータＣＤを再現する。このチャレンジデータＣＤが、チャレンジデータ記憶領域８６ａ（図８参照）に記憶されているチャレンジデータＣＤと比較される。また、複合機８０は、（ｍ＋１）番目から（ｍ＋１０）番目までのブロックに含まれている分割チャレンジデータからチャレンジデータＣＤの一部を再現する。複合機８０は、この再現された部分が、チャレンジデータ記憶領域８６ａに記憶されているチャレンジデータＣＤの一部に含まれているのか否かを比較する。

また、複合機８０は、情報ブロック１５０に含まれているＤＰとＤＰＬとＤＡＬから新パスワードＤ２を再現することができる。複合機８０は、１番目からｍ＋１０番目までのブロックに含まれている分割パスワードデータから新パスワードＤ２を再現する。

なお、実際には、ＣＬとＣＡＬが少なくともあれば、チャレンジデータＣＤを再現することができる。即ち、チャレンジ用ダミーデータＣＰのデータ量ＣＰＬがなくても、チャレンジデータＣＤを再現することができる。また、ＤＬとＤＡＬが少なくともあれば、新パスワードＤ２を再現することができる。即ち、パスワード用ダミーデータＤＰのデータ量ＤＰＬがなくても、新パスワードＤ２を再現することができる。情報ブロック１５０は、ＣＰＬとＤＰＬを含んでいなくてもよい。

【００６０】

（第５実施例）

図１７は、本実施例の組合せデータ（ＣＤ＋Ｄ２）を示す。

本実施例では、（ｍ＋１０）個のブロック１６０，１６２，１６４，１６６等によって組合せデータ（ＣＤ＋Ｄ２）が暗号化されている。分割チャレンジデータ（例えばＣＤ（１））のデータ量と、分割パスワードデータ（例えばＤ２（１））のデータ量は、ブロッ

ク毎に異なる。この点は、第３実施例と同様である。各ブロック１６０，１６２，１６４，１６６等には、６種類の情報データ（ＣＬ，ＣＰＬ，ＣＡＬ，ＤＬ，ＤＰＬ，ＤＡＬ）が含まれている。これらの情報データの内容は、第３実施例や第４実施例と同様である。

本実施例では、新パスワードＤ２は、（ｍ＋１０）個の分割パスワードデータに分割されている。新パスワードＤ２を再現するためには、１番目から（ｍ＋１０）番目までのブロックが必要となる。一方において、チャレンジデータＣＤは、ｍ個の分割チャレンジデータに分割されている。従って、１番目からｍ番目までのブロックに含まれている分割チャレンジデータからチャレンジデータＣＤを再現することができる。（ｍ＋１）番目から（ｍ＋１０番目）までには、１番目から１０番目のブロックに含まれている分割チャレンジデータが含まれている。この点は、第４実施例と同様である。

【００６１】

複合機８０は、各ブロックに含まれているＣＬとＣＰＬとＣＡＬからチャレンジデータＣＤを再現することができる。複合機８０は、１番目からｍ番目までのブロックに含まれている分割チャレンジデータからチャレンジデータＣＤを再現する。また、複合機８０は、各ブロックに含まれているＤＰとＤＰＬとＤＡＬから新パスワードＤ２を再現することができる。複合機８０は、１番目からｍ＋１０番目までのブロックに含まれている分割パスワードデータから新パスワードＤ２を再現する。

本実施例のデータ構成によっても、複合機８０がチャレンジデータＣＤと新パスワードＤ２を再現することができる。

【００６２】

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。

例えば、ダミーデータのデータ量を示すＣＰＬ，ＤＰＬに固有のＩＤを割り振ることができる。複合機８０は、それらのＩＤがブロックに含まれている場合は、予め決められているデータ量のダミーデータがそのブロックに含まれているものとしてデータを再現する。また、複合機８０は、それらのＩＤがブロックに含まれていない場合は、ダミーデータがそのブロックに含まれていないものとして扱う。

【００６３】

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】

【００６４】

【図１】本発明の通信システムの構成図を示す。

【図２】暗号化された組合せデータの一例を示す。

【図３】暗号化された組合せデータの一例を示す。

【図４】暗号化された組合せデータの一例を示す。

【図５】暗号化された組合せデータの一例を示す。

【図６】（ａ）暗号化された組合せデータの一例を示す。（ｂ）データ量を示すデータの一例を示す。

【図７】暗号化された組合せデータの一例を示す。

【図８】実施例の通信システムを示す。

【図９】パスワード変更処理のタイムチャートを示す。

【図１０】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。

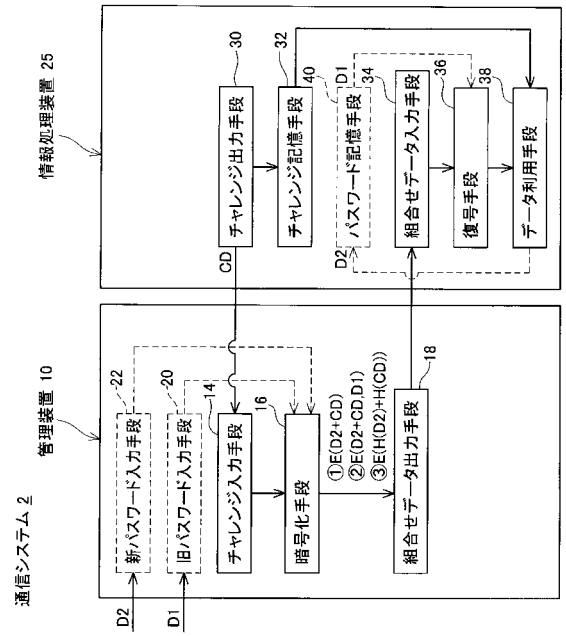
【図１１】（ａ）ハッシュ化されたチャレンジデータを示す。（ｂ）ハッシュ化された新パスワードを示す。（ｃ）組合せデータを示す。

【図１２】複合機のチャレンジ発行処理のフローチャートを示す。

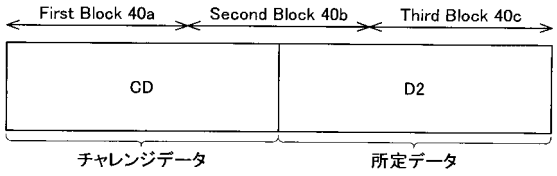
【図１３】複合機のパスワード変更処理のフローチャートを示す。

【図１４】（ａ）チャレンジデータの一例を示す。（ｂ）新パスワードの一例を示す。（ｃ）暗号化された組合せデータの一例を示す（第２実施例）。
【図１５】暗号化された組合せデータの一例を示す（第３実施例）。
【図１６】暗号化された組合せデータの一例を示す（第４実施例）。
【図１７】暗号化された組合せデータの一例を示す（第５実施例）。
【符号の説明】
【００６５】
２：通信システム
１０：管理装置
１４：チャレンジ入力手段
１６：暗号化手段
１８：組合せデータ出力手段
２０：旧パスワード入力手段
２２：新パスワード入力手段
２５：情報処理装置
３０：チャレンジ出力手段
３２：チャレンジ記憶手段
３４：組合せデータ入力手段
３６：復号手段
３８：データ利用手段
３８：チャレンジ出力手段
４０：パスワード記憶手段
５０：通信システム
６０：管理装置
８０：複合機

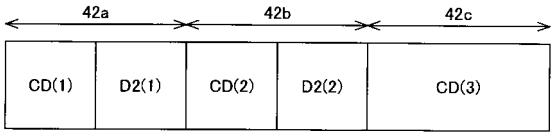
【図１】



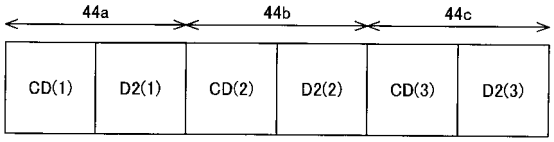
【図２】



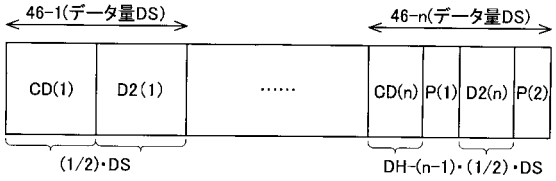
【図３】



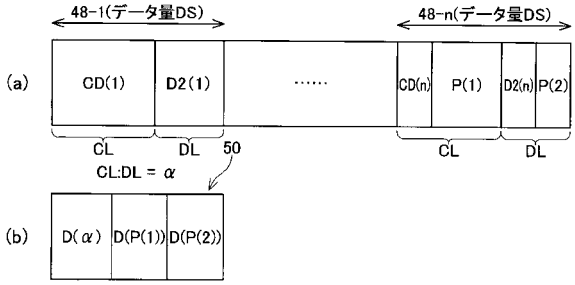
【図４】



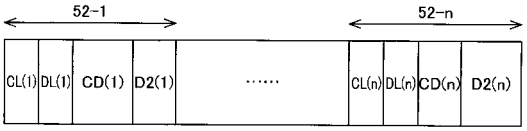
【図５】



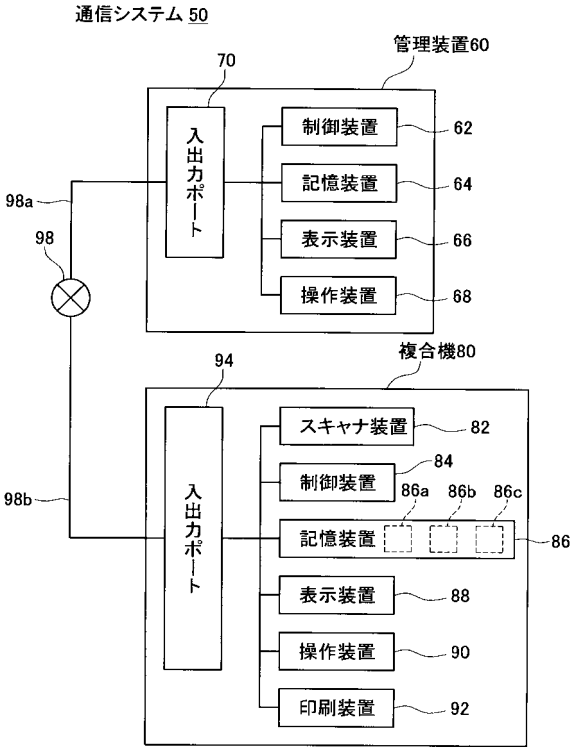
【図６】



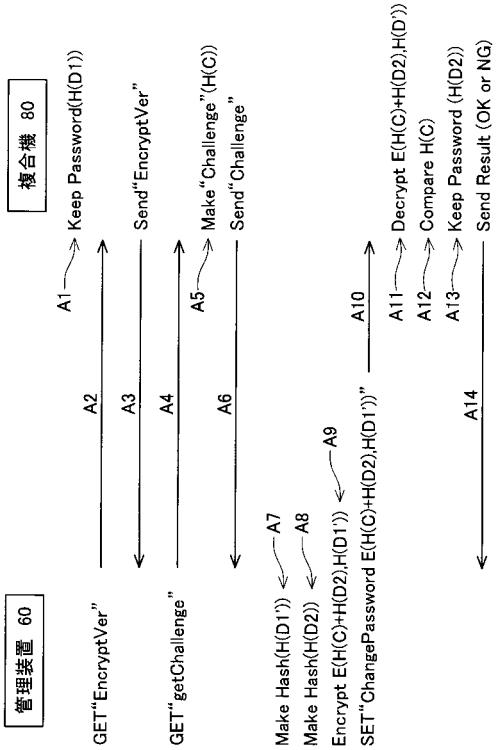
【図７】



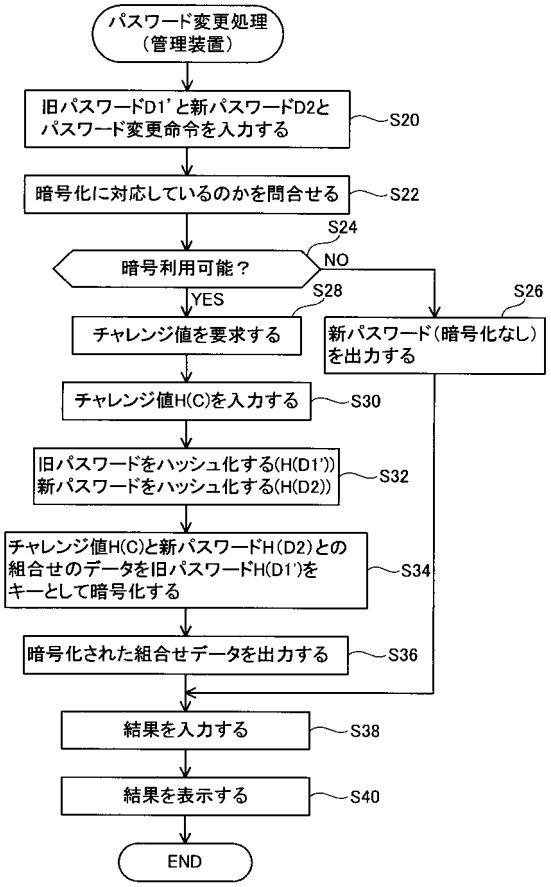
【図８】



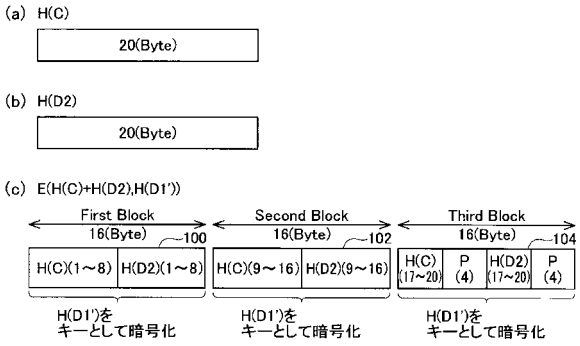
【図９】



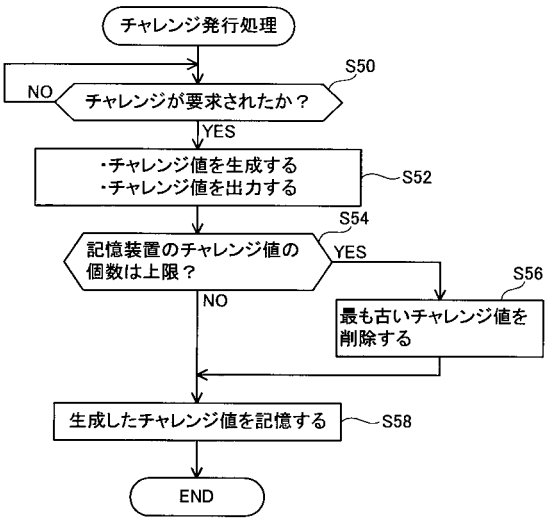
【図１０】



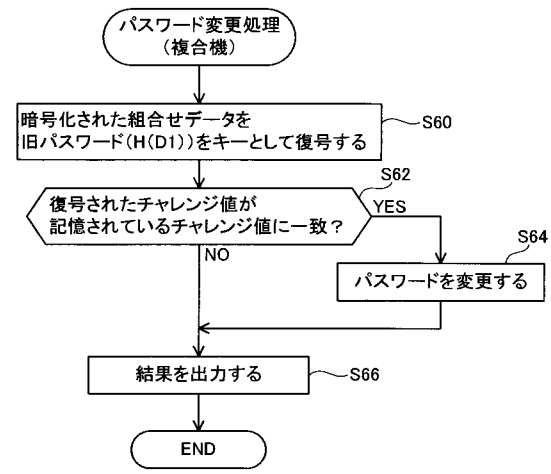
【図１１】



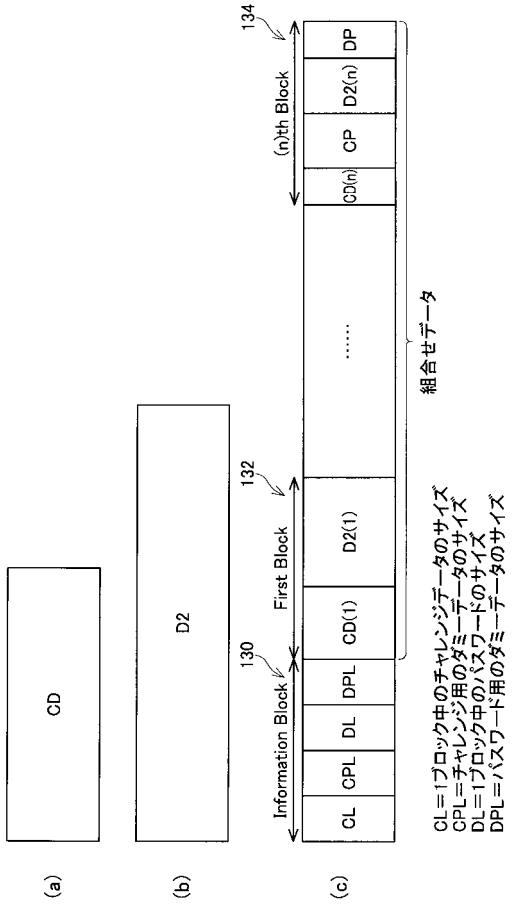
【図１２】



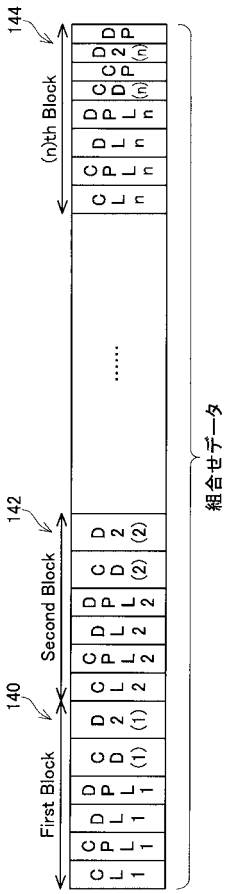
【図１３】



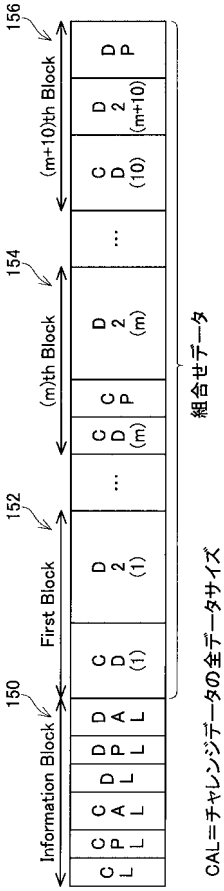
【図１４】



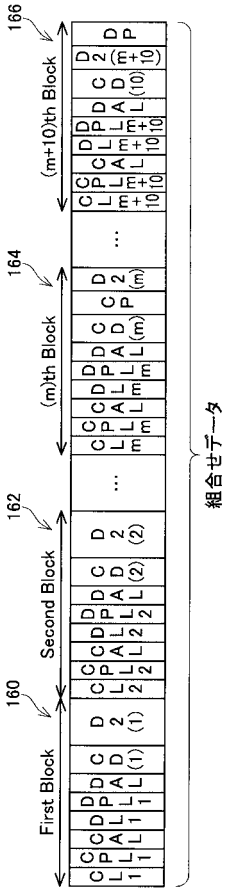
【図１５】


144
(n)th Block
142
Second Block
140
First Block
組合せデータ

【図１６】


156
(m+10)th Block
154
(m)th Block
152
First Block
150
Information Block
組合せデータ
CAL＝チャレンジデータの全データサイズ
DAL＝パスワードの全データサイズ

【図１７】


166
(m+10)th Block
164
(m)th Block
162
Second Block
160
First Block
組合せデータ

フロントページの続き

(56)参考文献 特開２００５－１１４８７０（ＪＰ，Ａ）
特開２００２－３３０１２２（ＪＰ，Ａ）
特開２００５－２５２３４７（ＪＰ，Ａ）
米国特許第０６７６９０６０（ＵＳ，Ｂ１）
特開平０９－２３１１７４（ＪＰ，Ａ）
特開平０８－３２０８４７（ＪＰ，Ａ）
特表２００５－５０９９３８（ＪＰ，Ａ）
特開２０００－０５９３５５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０９Ｃ　　１／００