(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2016-71839
(P2016-71839A)
(43)公開日　平成28年5月9日(2016.5.9)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/62	(2013.01)	G06F	21/62	345

審査請求 有　請求項の数 20　ＯＬ　（全 18 頁）

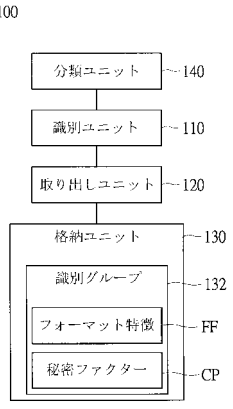
(21)出願番号　特願2015-20104(P2015-20104)
(22)出願日　平成27年2月4日(2015.2.4)
(31)優先権主張番号　103134231
(32)優先日　平成26年10月1日(2014.10.1)
(33)優先権主張国　台湾(TW)

(71)出願人　502003596
財団法人　資訊工業策進会
ＩＮＳＴＩＴＵＴＥ　ＦＯＲ　ＩＮＦＯＲＭＡＴＩＯＮ　ＩＮＤＵＳＴＲＹ
台湾台北市和平東路２段１０６号１１樓
１１Ｆ，　ＮＯ．１０６，　ＳＥＣ．２，　ＨＥＰＩＮＧ　Ｅ．　ＲＤ．，　ＴＡＩＰＥＩ，　ＴＡＩＷＡＮ，
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100110364
弁理士　実広　信哉
(74)代理人　100133400
弁理士　阿部　達彦

最終頁に続く

(54)【発明の名称】秘密データを識別する方法、電子装置及びコンピュータ読み取り可能な記録媒体

(57)【要約】　（修正有）
【課題】データの漏れを回避することができる秘密データを識別する方法、電子装置及びコンピュータ読み取り可能な記録媒体を提供する。
【解決手段】電子装置１００は、特定フォーマットを表すフォーマット特徴に基づいてデータにおいて特定フォーマットがあるか否かを判定し、特定フォーマットを秘密データとして表す複数の秘密ファクターＣＰに基づいて、データにおける特定フォーマットが秘密データであるか否かをさらに判定する。これにより、カウント数が多くないが機密記述が大量に含まれたデータの正しい機密レベルを提供するとともに特定フォーマットを有する秘密データを識別する。
【選択図】図１



【特許請求の範囲】
【請求項１】
特定フォーマットを表すフォーマット特徴と前記特定フォーマットを秘密データとして表す複数の機密ファクターとをそれぞれ有すると共に前記特定フォーマットにそれぞれ対応する複数の識別グループが格納された電子装置に適用される、秘密データを識別する方法であって、
複数のデータのいずれか１つを取り出し、それを取り出しデータと定義する工程と、
それらのフォーマット特徴のいずれか１つを取り出し、それを取り出し特徴と定義する工程と、
前記電子装置が、前記取り出し特徴に基づいて前記取り出しデータが対応する前記特定フォーマットを有するか否かを判定し、前記取り出しデータが対応する前記特定フォーマットを有すると判定した場合に、前記特定フォーマットに対応する複数の秘密ファクターが前記取り出しデータにおける出現頻度が秘密閾値以上であるかを判定し、前記出現頻度が前記秘密閾値以上であると判定した場合に、前記取り出しデータにおける前記特定フォーマットが前記秘密データであることを表し、前記出現頻度が前記秘密閾値よりも小さいと判定した場合に、前記取り出しデータにおける前記特定フォーマットが前記秘密データではないことを表すようにする工程と、
前記電子装置が、複数のフォーマット特徴において取り出されていない前記フォーマット特徴があるか否かを判定し、複数のフォーマット特徴において取り出されていない前記フォーマット特徴があると判定した場合に、取り出されていない前記フォーマット特徴を取り出し、取り出されていない前記フォーマット特徴を前記取り出し特徴と定義することで、改めて前記取り出し特徴に基づいて前記取り出しデータが対応する前記特定フォーマットを有するか否かを判定し、複数のフォーマット特徴において取り出されていない前記フォーマット特徴がないと判定した場合に、複数のデータの次のデータを取り出し、前記次のデータを前記取り出しデータと定義することで、改めて前記取り出しデータが対応する前記特定フォーマットを有するか否かを判定する工程と、
を備えることを特徴とする秘密データを識別する方法。
【請求項２】
前記電子装置は、前記取り出しデータが対応する前記特定フォーマットを有しないと判定した場合に、それらのフォーマット特徴において取り出されていない前記フォーマット特徴があるか否かを判定することを特徴とする請求項１に記載の秘密データを識別する方法。
【請求項３】
前記電子装置は、それらのフォーマット特徴において取り出されていない前記フォーマット特徴がないと判定した後に、さらに、それらの秘密ファクターとそれらの秘密ファクターがそれらのデータに出現する回数とに基づいて前記取り出しデータに対して分類を行うことを特徴とする請求項１に記載の秘密データを識別する方法。
【請求項４】
前記取り出し特徴に基づいて前記取り出しデータが対応する前記特定フォーマットを有するか否かを判定する工程において、前記取り出し特徴が同一列に２つの列終了位置を有し、かつ前記電子装置が前記特定フォーマットにおいて同一列に２つの列終了位置を有する数がフォーマット閾値以上であると判定した場合に、前記電子装置は前記取り出しデータが前記特定フォーマットを有すると判定することを特徴とする請求項１に記載の秘密データを識別する方法。
【請求項５】
前記取り出し特徴に基づいて前記取り出しデータが対応する前記特定フォーマットを有するか否かを判定する工程において、前記フォーマット特徴が特定鍵からのメッセージを含み、かつ前記特定フォーマットにおいて前記メッセージを有する数がフォーマット閾値以上である場合に、前記取り出しデータが前記特定フォーマットを有すると判定することを特徴とする請求項１に記載の秘密データを識別する方法。

【請求項６】
前記取り出し特徴に基づいて前記取り出しデータが対応する前記特定フォーマットを有するか否かを判定する工程において、前記フォーマット特徴がカスタマイズ特徴を含み、かつ前記特定フォーマットにおいて前記カスタマイズ特徴を有する数がフォーマット閾値よりも大きい場合に、前記取り出しデータが前記特定フォーマットを有すると判定することを特徴とする請求項１に記載の秘密データを識別する方法。
【請求項７】
各前記識別グループのそれらの秘密ファクターは、少なくとも１つのワード、少なくとも１つのストリング、少なくとも１つの符号、少なくとも１つの数字、少なくとも１つの実行指令、及び少なくとも１つのフォーマットのいずれか１つまたはそれらの組み合わせであることを特徴とする請求項１に記載の秘密データを識別する方法。
【請求項８】
各前記フォーマット特徴は、少なくとも１つのワード、少なくとも１つのストリング、少なくとも１つの符号、少なくとも１つの数字、少なくとも１つの実行指令、及び少なくとも１つのフォーマットのいずれか１つまたはそれらの組み合わせであることを特徴とする請求項１に記載の秘密データを識別する方法。
【請求項９】
特定フォーマットを表すフォーマット特徴と前記特定フォーマットを秘密データとして表す複数の機密ファクターとをそれぞれ有すると共に前記特定フォーマットにそれぞれ対応する複数の識別グループを格納するための格納ユニットと、
前記格納ユニットに電気的に接続され、それらのデータ及びそれらの識別グループを取り出すための取り出しユニットと、
前記取り出しユニットに電気的に接続される識別ユニットであって、
前記取り出しユニットを介して、それらのデータのいずれか１つを取り出し、それを取り出しデータと定義する工程と、
前記取り出しユニットを介して、それらのフォーマット特徴のいずれか１つを取り出し、それを取り出し特徴と定義する工程と、
前記取り出し特徴に基づいて前記取り出しデータが対応する前記特定フォーマットを有するか否かを判定し、前記取り出しデータが対応する前記特定フォーマットを有すると判定した場合に、前記特定フォーマットに対応するそれらの秘密ファクターが前記取り出しデータにおける出現頻度が秘密閾値以上であるかを判定し、前記出現頻度が前記秘密閾値以上であると判定した場合に、前記取り出しデータにおける前記特定フォーマットが前記秘密データであることを表し、前記出現頻度が前記秘密閾値よりも小さいと判定した場合に、前記取り出しデータにおける前記特定フォーマットが前記秘密データではないことを表すようにする工程と、
それらのフォーマット特徴において取り出されていない前記フォーマット特徴があるか否かを判定し、それらのフォーマット特徴において取り出されていない前記フォーマット特徴があると判定した場合に、前記取り出しユニットを介して取り出されていない前記フォーマット特徴を取り出し、取り出されていない前記フォーマット特徴を前記取り出し特徴と定義することで、改めて前記取り出し特徴に基づいて前記取り出しデータが対応する前記特定フォーマットを有するか否かを判定し、それらのフォーマット特徴において取り出されていない前記フォーマット特徴がないと判定した場合に、前記取り出しユニットを介して複数のデータの次のデータを取り出し、前記次のデータを前記取り出しデータと定義することで、改めて前記取り出しデータが対応する前記特定フォーマットを有するか否かを判定する工程と、を実行する識別ユニットと、
を備えることを特徴とする秘密データを識別する電子装置。
【請求項１０】
前記識別ユニットは、前記取り出しデータが対応する前記特定フォーマットを有しないと判定した場合に、複数のフォーマット特徴において取り出されていない前記フォーマット特徴があるか否かを判定することを特徴とする請求項９に記載の秘密データを識別する

電子装置。
【請求項１１】
前記識別ユニットに電気的に接続される分類ユニットであって、前記識別ユニットがそれらのフォーマット特徴において取り出されていない前記フォーマット特徴がないと判定した場合に、それらの秘密ファクターとそれらの秘密ファクターがそれらのデータに出現する回数とに基づいて前記取り出しデータに対して分類を行う分類ユニットをさらに備えることを特徴とする請求項９に記載の秘密データを識別する電子装置。
【請求項１２】
前記取り出し特徴が同一列に２つの列終了位置を有し、かつ前記識別ユニットが前記特定フォーマットにおいて同一列に２つの列終了位置を有する数がフォーマット閾値以上であると判定した場合に、前記識別ユニットは前記取り出しデータが前記特定フォーマットを有すると判定することを特徴とする請求項９に記載の秘密データを識別する電子装置。
【請求項１３】
前記フォーマット特徴が特定鍵からのメッセージを含み、かつ前記識別ユニットが前記特定フォーマットにおいて前記メッセージを有する数がフォーマット閾値以上であると判定した場合に、前記識別ユニットは前記取り出しデータが前記特定フォーマットを有すると判定することを特徴とする請求項９に記載の秘密データを識別する電子装置。
【請求項１４】
前記フォーマット特徴がカスタマイズ特徴を含み、かつ前記識別ユニットが前記特定フォーマットにおいて前記カスタマイズ特徴を有する数がフォーマット閾値よりも大きいと判定した場合に、前記識別ユニットは前記取り出しデータが前記特定フォーマットを有すると判定することを特徴とする請求項９に記載の秘密データを識別する電子装置。
【請求項１５】
各前記識別グループのそれらの秘密ファクターは、少なくとも１つのワード、少なくとも１つのストリング、少なくとも１つの符号、少なくとも１つの数字、少なくとも１つの実行指令、及び少なくとも１つのフォーマットのいずれか１つまたはそれらの組み合わせであることを特徴とする請求項９に記載の秘密データを識別する電子装置。
【請求項１６】
各前記フォーマット特徴は、少なくとも１つのワード、少なくとも１つのストリング、少なくとも１つの符号、少なくとも１つの数字、少なくとも１つの実行指令、及び少なくとも１つのフォーマットのいずれか１つまたはそれらの組み合わせであることを特徴とする請求項９に記載の秘密データを識別する電子装置。
【請求項１７】
ユーザコンピュータと遠隔サーバとの間に設けられ、前記ユーザコンピュータと前記遠隔サーバとの間に伝送される各前記データにおける前記特定フォーマットが秘密データであるか否かを識別することを特徴とする請求項９に記載の秘密データを識別する電子装置。
【請求項１８】
ユーザコンピュータに接続され、ネットワーク接続を介して前記ユーザコンピュータのそれらのデータを取り出し、各前記データにおける前記特定フォーマットが秘密データであるか否かを識別することを特徴とする請求項９に記載の秘密データを識別する電子装置。
【請求項１９】
ユーザコンピュータの内部に設けられ、前記ユーザコンピュータからそれらのデータが出力された場合に、それらのデータを取り出し、各前記データにおける前記特定フォーマットが秘密データであるか否かを識別することを特徴とする請求項９に記載の秘密データを識別する電子装置。
【請求項２０】
コンピュータによって実行可能なプログラムが記録され、プロセッサーによって読み取られた場合に、前記プロセッサーは、前記コンピュータによって実行可能なプログラムを

実行することで、請求項１に記載の秘密データを識別する方法を実施可能であることを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、秘密データを識別する方法、電子装置及びコンピュータ読み取り可能な記録媒体に関し、特にファイルにおける特定フォーマットが秘密データであるか否かを識別する方法、電子装置及びコンピュータ読み取り可能な記録媒体に関するものである。

【背景技術】

【０００２】

秘密データを識別する技術は、データ保護の関連分野に用いられる。秘密データの識別メカニズムを通じて、高機密性が潜在する秘密データをさらに識別することができる。

【０００３】

従来の秘密データ識別技術は、個人データまたは秘密ストリングに対してのみ分析識別するものであり、機密レベルが、見つけ出した類型またはカウント数に比例するのが一般的である。カウント数が多くないが機密記述が大量に含まれたデータ（例えば履歴、カルテ等）に対して、正しい機密レベルを提供することができない。また、従来の秘密データ識別技術は、大量の既知データ全体の内容について学習を行い、既知データの特徴を取得した後、上記特徴を識別すべきデータの特徴と比較対照することで、識別データが秘密データであるか否かを判定する。従って、従来の秘密データ識別技術は、既知データと同一または類似する秘密データしか見つけ出すことができず、既知データと同一のテンプレートまたはフォーマットを使用した秘密データを見つけ出すことができない。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

カウント数が多くないが機密記述が大量に含まれたデータの正しい機密程度を提供するとともに特定のテンプレートまたはフォーマットを有する秘密データを識別することによってデータの漏れを回避することができる秘密データを識別する方法、電子装置及びコンピュータ読み取り可能な記録媒体を提供する。

【課題を解決するための手段】

【０００５】

本発明は、特定フォーマットを表すフォーマット特徴と前記特定フォーマットを秘密データとして表す複数の機密ファクターとをそれぞれ有すると共に前記特定フォーマットにそれぞれ対応する複数の識別グループが格納された電子装置に適用される、秘密データを識別する方法であって、複数のデータのいずれか１つを取り出し、それを取り出しデータと定義する工程と、複数のフォーマット特徴のいずれか１つを取り出し、それを取り出し特徴と定義する工程と、電子装置が、取り出し特徴に基づいて取り出しデータが対応する特定フォーマットを有するか否かを判定し、取り出しデータが対応する特定フォーマットを有すると判定した場合に、特定フォーマットに対応する複数の秘密ファクターの取り出しデータにおける出現頻度が秘密閾値以上であるかを判定し、出現頻度が秘密閾値以上であると判定した場合に、取り出しデータにおける特定フォーマットが秘密データであることを表し、出現頻度が秘密閾値よりも小さいと判定した場合に記取り出しデータにおける特定フォーマットが秘密データではないことを表すようにする工程と、電子装置が、複数のフォーマット特徴において取り出されていないフォーマット特徴があるか否かを判定し、複数のフォーマット特徴において取り出されていないフォーマット特徴があると判定した場合に、取り出されていないフォーマット特徴を取り出し、取り出されていないフォーマット特徴を取り出し特徴と定義することで、改めて取り出し特徴に基づいて取り出しデータが対応する特定フォーマットを有するか否かを判定し、複数のフォーマット特徴において取り出されていないフォーマット特徴がないと判定した場合に、複数のデータの次のデータを取り出し、次のデータを取り出しデータと定義することで、改めて取り出しデー

タが対応する特定フォーマットを有するか否かを判定する工程と、を備えることを特徴とする秘密データを識別する方法を提供する。

【０００６】

また、本発明は、特定フォーマットを表すフォーマット特徴と特定フォーマットを秘密データとして表す複数の機密ファクターとをそれぞれ有すると共に特定フォーマットにそれぞれ対応する複数の識別グループを格納するための格納ユニットと、格納ユニットに電気的に接続され、複数のデータ及び複数の識別グループを取り出すための取り出しユニットと、取り出しユニットに電気的に接続される識別ユニットであって、取り出しユニットを介して、複数のデータのいずれか１つを取り出し、それを取り出しデータと定義する工程と、取り出しユニットを介して、複数のフォーマット特徴のいずれか１つを取り出し、それを取り出し特徴と定義する工程と、取り出し特徴に基づいて取り出しデータが対応する特定フォーマットを有するか否かを判定し、取り出しデータが対応する特定フォーマットを有すると判定した場合に、特定フォーマットに対応する複数の秘密ファクターの取り出しデータにおける出現頻度が秘密閾値以上であるかを判定し、出現頻度が秘密閾値以上であると判定した場合に、取り出しデータにおける特定フォーマットが秘密データであることを表し、出現頻度が秘密閾値よりも小さいと判定した場合に、取り出しデータにおける特定フォーマットが秘密データではないことを表すようにする工程と、複数のフォーマット特徴において取り出されていないフォーマット特徴があるか否かを判定し、複数のフォーマット特徴において取り出されていないフォーマット特徴があると判定した場合に、取り出しユニットを介して取り出されていないフォーマット特徴を取り出し、取り出されていないフォーマット特徴を取り出し特徴と定義することで、改めて取り出し特徴に基づいて取り出しデータが対応する特定フォーマットを有するか否かを判定し、複数のフォーマット特徴において取り出されていないフォーマット特徴がないと判定した場合に、取り出しユニットを介して複数のデータの次のデータを取り出し、次のデータを取り出しデータと定義することで、改めて取り出しデータが対応する特定フォーマットを有するか否かを判定する工程と、を実行する識別ユニットと、を備えることを特徴とする秘密データを識別する電子装置を提供する。

【０００７】

また、本発明は、コンピュータによって実行可能なプログラムが記録され、プロセッサーによって読み取られた場合に、プロセッサーは、上記秘密データを識別する方法における工程を実行可能であることを特徴とするコンピュータ読み取り可能な記録媒体を提供する。

【発明の効果】

【０００８】

上記のように、本発明に係る秘密データを識別する方法、電子装置及びコンピュータ読み取り可能な記録媒体によれば、特定フォーマットを有するデータが秘密データであるか否かを判定することができる。これにより、本発明に係る秘密データを識別する方法、電子装置及びコンピュータ読み取り可能な記録媒体は、カウント数が多くないが機密記述が大量に含まれたデータの正しい機密レベルを提供するとともに特定フォーマットを有する秘密データを識別することができ、データの漏れを回避することができる。

【図面の簡単な説明】

【０００９】

【図１】本発明の一実施例に係る秘密データを識別する電子装置の模式図である。

【図２Ａ】本発明の一実施例に係る秘密データを識別する方法のフロー図である。

【図２Ｂ】本発明の一実施例に係る秘密データを識別する方法のフロー図である。

【図３Ａ】本発明の一実施例に係る電子装置が取り出しデータにフォームがあると判定した様子を示す模式図である。

【図３Ｂ】本発明の一実施例に係る電子装置が取り出しデータにフォームがあると判定した様子を示す模式図である。

【図４Ａ】本発明の他の実施例に係る電子装置が取り出しデータにリストがあると判定し

た様子を示す模式図である。
【図４Ｂ】本発明の他の実施例に係る電子装置が取り出しデータにリストがあると判定した様子を示す模式図である。
【図５Ａ】本発明の他の実施例に係る電子装置が取り出しデータにパターンがあると判定した様子を示す模式図である。
【図５Ｂ】本発明の他の実施例に係る電子装置が取り出しデータにパターンがあると判定した様子を示す模式図である。
【図６】本発明の他の実施例に係る電子装置が受信したデータにおける特定フォーマットの内容が秘密データであるか否かを判定する。
【発明を実施するための形態】
【００１０】
以下、本発明の各種の例示性実施例について、添付図面を参照しながら詳しく説明する。ここで説明しておきたいのは、本発明の概念は、異なる形式で表現されるため、明細書に述べた例示性実施例に限定されるものではない。また、図面における同一素子には、同一符号を付す。
【００１１】
本発明の実施例に係る秘密データを識別する電子装置は、特定フォーマットを表すフォーマット特徴に基づいてデータにおいて特定フォーマットがあるか否かを判定し、次に、さらに特定フォーマットを秘密データとして表す複数の秘密ファクターに基づいて、データにおける特定フォーマットが秘密データであるか否かを判定する。また、本発明の実施例に係る電子装置に対応して実行される秘密データを識別する方法において、ファームウェア、ソフトウェアまたはハードウェア回路の方法により電子装置に実施可能である。
【００１２】
まず、図１は、本発明の一実施例に係る秘密データを識別する電子装置の模式図である。図１に示すように、秘密データを識別する電子装置１００は、電子装置１００によって受信されたデータにおける特定フォーマットの内容が秘密データであるか否かを識別し、データの漏れを回避するためのものである。この実施例において、電子装置１００は、スマートフォン、デスクトップコンピュータ、ノードブックコンピュータ、またはその他データを受信可能な電子装置であってもよい。
【００１３】
電子装置１００は、ユーザコンピュータと遠隔サーバとの間（図示せず）に設けられており、ユーザコンピュータと遠隔サーバとの間に伝送されるデータにおける特定フォーマットが秘密データであるか否かを識別することができる。また、電子装置１００は、ユーザコンピュータ（図示せず）に電気的に接続されることで、ネットワーク接続を介してユーザコンピュータにおけるデータを取り出すとともに、取り出されたデータにおける特定フォーマットが秘密データであるか否かを識別することもできる。さらに、電子装置１００は、ユーザコンピュータの内部（図示せず）に設けられることで、ユーザコンピュータからデータが出力された場合に、出力されたデータにおける特定フォーマットが秘密データであるか否かを識別することができる。本発明は、電子装置の設置位置について何ら制限するものではない。これにより、電子装置１００は、秘密データが窃取意図のある者によって取得されることを防止し、データの漏れを回避することができる。
【００１４】
電子装置１００は、演算処理ユニットとしての識別ユニット１１０と、取り出しユニット１２０と、格納ユニット１３０とを含む。格納ユニット１３０には複数の識別グループ１３２が格納されている。各識別グループ１３２は、特定フォーマットに対応し、かつ対応する特定フォーマットを表すフォーマット特徴ＦＦを有する。つまり、各識別グループ１３２がフォーマット特徴ＦＦを有することで、演算処理ユニットとしての識別ユニット１１０は、データにおける内容が対応する特定フォーマットを有するか否かを識別することができる。１つの例として、特定フォーマットがフォーム（ＦＯＲＭ）である場合、フォームのフォーマット特徴ＦＦは、複数の列において２つの列終了位置（Ｅｎｄ－ｏｆ－

Ｌｉｎｅ）を有する特徴であってもよい。さらに例を挙げれば、特定フォーマットがリスト（ＬＩＳＴ）である場合、リストのフォーマット特徴ＦＦは、複数の「ＴＡＢ」鍵からのメッセージを有する特徴であってもよい。さらに例を挙げれば、特定フォーマットがユーザ自身によって定義されたテンプレート（ＴＥＭＰＬＡＴＥ）である場合、テンプレートのフォーマット特徴ＦＦは、ユーザ自身によって定義された特徴であってもよい。この実施例において、各フォーマット特徴ＦＦは、少なくとも１つのワード、少なくとも１つのストリング、少なくとも１つの符号、少なくとも１つの数字、少なくとも１つの実行指令、及び少なくとも１つのフォーマットのいずれか１つまたはそれらの組み合わせであってもよく、これらに限定されるものではない。

【００１５】

また、各識別グループ１３２は、対応する特定フォーマットを秘密データとして表す複数の秘密ファクターＣＰを有する。つまり、各識別グループ１３２が複数の秘密ファクターＣＰを有することで、演算処理ユニットとしての識別ユニット１１０は、データにおける特定フォーマットの内容が秘密データであるか否かを識別することができる。１つの例として、特定フォーマットが履歴フォーム（図３Ａを参照）である場合、秘密ファクターＣＰは、「名前」、「身分証明書」、「携帯電話」、及び「連絡住所」等の名詞であってもよい。さらに例を挙げれば、特定フォーマットが住所録リスト（図４Ａを参照）である場合、秘密ファクターＣＰは、「生年月日」、「身長」、「体重」、「住所」、及び「電話」等の名詞であってもよい。さらに例を挙げれば、特定フォーマットがユーザ自身によって定義されたテンプレート（図５Ａを参照）である場合、秘密ファクターＣＰは、「計画目的」、及び「お客様要求」等、ユーザ自身によって定義された名詞であってもよい。この実施例において、各識別グループ１３２に対応する複数の秘密ファクターＣＰは、少なくとも１つのワード、少なくとも１つのストリング、少なくとも１つの符号、少なくとも１つの数字、少なくとも１つの実行指令、及び少なくとも１つのフォーマットのいずれか１つまたはそれらの組み合わせであってもよく、これらに限定されるものではない。

【００１６】

電子装置１００において複数の識別グループ１３２が格納ユニット１３０に格納される方法は、従来の格納方法である。当業者は、電子装置１００において複数の識別グループ１３２が格納ユニット１３０に格納される方法を理解することができるため、ここでは詳しい説明を省略する。この実施例において、格納ユニット１３０は、フラッシュメモリチップ、リードオンリーメモリチップまたはランダムアクセスメモリチップ等、揮発性または非揮発性の記憶チップであってもよく、好ましくは非揮発性メモリである。

【００１７】

また、電子装置１００は、ユーザが識別インタフェースにおいて識別しようとする特定フォーマット（例えばユーザ自身によって定義された名詞）を設定し、かつ受信されたデータにおける特定フォーマットの内容が秘密データであるか否かを識別できるように、識別インタフェース（図示せず）を表示するための表示ユニットをさらに有する。当然ながら、識別しようとする特定フォーマット及びそれに対応する識別グループ１３２が予め格納ユニット１３０に設定された場合には、表示ユニットを設けなくてもよく、本発明はこれに限定されるものではない。

【００１８】

取り出しユニット１２０は、識別ユニット１１０が受信されたデータをさらに識別できるように、格納ユニット１３０に電気的に接続されるとともに、複数のデータ及び複数の識別グループ１３２を取り出すものである。識別ユニット１１０は、取り出しユニット１２０に電気的に接続され、電子装置１００の主要な演算中心としての演算処理ユニットであり、各分析、演算及び制御を行うものである。この実施例において、識別ユニット１１０は、中央処理器、マイクロ制御器または埋め込み型制御器等の処理チップであってもよい。識別ユニット１１０及び取り出しユニット１２０は、中央処理器、マイクロ制御器または埋め込み型制御器等の処理チップに統合されてもよく、本発明は、それに限定されるものではない。

【００１９】
識別ユニット１１０は、下記の工程を実行することで、受信されたデータにおける特定フォーマットの内容が秘密データであるか否かを識別する。
【００２０】
図１、図２Ａを同時に参照すると、まず、識別ユニット１１０は、取り出しユニット１２０を介して複数のデータのいずれか１つを取り出し、それを取り出しデータと定義することで、取り出しデータにおける特定フォーマットの内容が秘密データであるか否かをさらに識別する（ステップＳ２１０）。識別ユニット１１０は、取り出しユニット１２０を介して外部装置から上記複数のデータを取り出すか、または格納ユニット１３０に予め格納された複数のデータを取り出すことができ、本発明はそれに限定されるものではない。
【００２１】
次に、識別ユニット１１０は、取り出しユニット１２０を介して格納ユニット１３０に格納された複数のフォーマット特徴ＦＦのいずれか１つを取り出し、それを取り出し特徴（ステップＳ２２０）と定義する。この場合の取り出し特徴は、ある特定フォーマット（例えばフォームまたはリスト等の特定フォーマット）を表す。さらに、識別ユニット１１０は、取り出し特徴に基づいて取り出しデータが対応する特定フォーマットを有するか否かを判定する（ステップＳ２３０）。即ち、識別ユニット１１０は、取り出しデータに所定の数量の取り出し特徴があるか否かを判定することにより、取り出しデータに現在取り出されたフォーマット特徴ＦＦの特定フォーマットがあるか否かを判定する。この実施例において、特定フォーマットは、フォーム、リスト、ユーザ自身によって定義されたテンプレート、またはその他規則性特徴を有する特定フォーマットであってもよく、本発明はそれに限定されるものではない。特定フォーマットに対応するフォーマット特徴ＦＦは、特定フォーマットにおいてのみ出現する特徴、例えば特定鍵からのメッセージ、連続ブランク等の特徴から選択されてもよく、本発明はそれに限定されるものではない。
【００２２】
識別ユニット１１０が取り出しデータにおいて対応する特定フォーマットがあると判定した場合には、取り出しデータにおいて取り出し特徴に対応する特定フォーマットがあることを表す。この場合、識別ユニット１１０は、取り出しデータにおける特定フォーマットの内容が秘密データであるか否かをさらに判定する（ステップＳ２４０）。逆に、識別ユニット１１０が、取り出しデータにおいて対応する特定フォーマットがないと判定した場合には、取り出しデータにおいて取り出し特徴に対応する特定フォーマットがないことを表す。この場合、識別ユニット１１０は、複数のフォーマット特徴ＦＦにおいて取り出されていないフォーマット特徴ＦＦがあるか否かをさらに判定する（ステップＳ２７０）。
【００２３】
１つの例として、特定フォーマットがフォームである場合、そのフォーマット特徴ＦＦは、図３Ａに示すように、同一列に少なくとも２つの列終了位置を有するものである。従って、取り出しユニット１２０がフォームを表すフォーマット特徴ＦＦを取り出した場合に、識別ユニット１１０は、フォームの内容において、その同一列に少なくとも２つの列終了位置を有する数がフォーマット閾値以上であるか否かを判定する。ＹＥＳ（はい）と判定した場合に、識別ユニット１１０は、取り出しデータにフォームを表す特定フォーマットがあると認定する。逆に、識別ユニット１１０は、取り出しデータにフォームを表す特定フォーマットがないと認定する。上記フォーマット閾値は、実際のフォームに応じて設定することができ、本発明はそれに限定されるものではない。識別ユニット１１０は、取り出しデータにフォームを表す特定フォーマットがあるか否かを識別した後、取り出しユニット１２０を介してフォームにおける内容（図３Ｂを参照）を取り出し、フォームにおける内容が秘密データであるか否かをさらに判定する。
【００２４】
さらに例を挙げれば、特定フォーマットがリストである場合、そのフォーマット特徴ＦＦは、図４Ａに示すように、複数の「ＴＡＢ」からのメッセージである。従って、取り出

しユニット１２０がリストを表すフォーマット特徴ＦＦを取り出した場合に、識別ユニット１１０は、リストにおける内容に上記メッセージを有する数がフォーマット閾値以上であるかを判定する。ＹＥＳと判定した場合に、識別ユニット１１０は、取り出しデータにリストを表す特定フォーマットがあると認定する。逆に、識別ユニット１１０は、取り出しデータにリストを表す特定フォーマットがないと認定する。上記フォーマット閾値は、実際のリストに基づいて設定してもよく、本発明はそれに限定されるものではない。識別ユニット１１０は、取り出しデータにリストを表す特定フォーマットがあるか否かを識別した後、取り出しユニット１２０を介してリストにおける内容を取り出し（図４Ｂを参照）、リストにおける内容が秘密データであるか否かをさらに判定する。

【００２５】

さらに例を挙げれば、特定フォーマットがユーザ自身によって定義されたテンプレートである場合、そのフォーマット特徴ＦＦは、カスタマイズ特徴である。即ち、フォーマット特徴ＦＦは、ユーザ自身によって定義されてなるものである。図５Ａに示すように、カスタマイズ特徴は、「計画目的」及び「お客様要求」等の特徴である。従って、取り出しユニット１２０がカスタマイズ特徴を表すフォーマット特徴ＦＦを取り出した場合に、識別ユニット１１０は、テンプレートの内容に上記カスタマイズ特徴を有する数がフォーマット閾値以上であるかを判定する。ＹＥＳと判定した場合に、識別ユニット１１０は、取り出しデータにテンプレートを表す特定フォーマットがあると認定する。逆に、識別ユニット１１０は、取り出しデータにテンプレートを表す特定フォーマットがないと認定する。上記フォーマット閾値は、実際のテンプレートに基づいて設定してもよく、本発明はそれに限定されるものではない。識別ユニット１１０は、取り出しデータにテンプレートを表す特定フォーマットがあるか否かを識別した後、取り出しユニット１２０を介してテンプレートにおける内容を取り出し（図５Ｂを参照）、テンプレートにおける内容が秘密データであるか否かをさらに判定する。

【００２６】

上記の３つの例において、当業者は、識別ユニット１１０が取り出しユニット１２０を介して特定フォーマット（例えばフォーム、リスト、テンプレート）における内容を取り出す実施方法を理解することができるため、ここでは詳しい説明を省略する。

【００２７】

ステップＳ２４０に戻り、識別ユニット１１０は、この特定フォーマットに対応する複数の秘密ファクターＣＰの取り出しデータにおける出現頻度が秘密データ閾値以上であるかを判定することにより、取り出しデータにおける特定フォーマットの内容が秘密データであるか否かを判定する。秘密ファクターＣＰは、対応する特定フォーマットが秘密データである確率を表すものである。従って、特定フォーマットにおいて秘密ファクターＣＰが多く出現するほど、特定フォーマットが秘密データである確率が高いことを表す。秘密ファクターＣＰの設定について、前の実施例に記載された通りであるため、ここでは詳しい説明を省略する。これにより、識別ユニット１１０が、秘密ファクターＣＰの出現頻度が秘密閾値以上であると判定した場合に、取り出しデータにおける特定フォーマットが秘密データであることを表す（ステップＳ２５０）。逆に、識別ユニット１１０が、秘密ファクターＣＰの出現頻度が秘密閾値よりも小さいと判定した場合に、取り出しデータにおける特定フォーマットが秘密データではないことを表す（ステップＳ２６０）。上記秘密閾値は、実際の複数の秘密ファクターＣＰの取り出しデータにおける出現頻度に基づいて設定されたものであり、本発明はそれに限定されるものではない。

【００２８】

１つの例として、図３Ａ～図３Ｂに示すように、特定フォーマットがフォームであるとする。このうち、フォームは、秘密ファクターＣＰの名詞として、「名前」、「身分証明書」、「携帯電話」、及び「連絡住所」を有する。各名詞には、例えば「名前」と同義である「名字」、「名称」、「人名」、「Ｎａｍｅ」等の同義字が現れる可能性がある。従って、判定の過程において、識別ユニット１１０は、同義字を同一の字句と見なす。この実施例において、識別ユニット１１０は、同義字関数ＳＴＦ（ｉ）を介して各字句がフォ

ームに出現する重要性を算出することで、各字句とフォームとの間の関連性を得ることができる。本実施例における同義字関数ＳＴＦ（ｉ）は、以下のように示すことができる。

【００２９】

【数１】

$$STF(i) = \frac{n_{ij}}{\sum_k N_{kj}} \times \omega_i$$

【００３０】

ここで、n_{ij}は、第ｉ種の字句が第ｊ個のフォームに出現する回数を表す。ω_iは第ｉ種の字句の重みを表す。$\Sigma_k N_{kj}$は第ｊ個のフォームにおけるすべてのｋ個の字句を表し、かつ且ｋ≧０。

【００３１】

ここで注意すべき点は、識別ユニット１１０が同義字を同一の字句と見なす点である。即ち、識別ユニット１１０がフォームにおける「連絡住所」、「名前」、「名称」、「人名」、及び「身分証明書」を見つけ出した場合、識別ユニット１１０は、「連絡住所」を第１種の名詞として見なし、「名前」、「名称」、「人名」を第２種の字句として見なし、「身分証明書」を第３種の字句として見なす。各種の字句の重みについて、ω_1が０．５であり、ω_2が０．２であり、ω_3が０．３であるとする場合、識別ユニット１１０は、同義字関数ＳＴＦを介して各字句がフォームに出現する重要性を算出する。第１種の字句としては、ＳＴＦ（１）＝１／５＊０．５＝０．１であり、第２種の字句としては、ＳＴＦ（２）＝３／５＊０．２＝０．１２であり、第３種の字句としては、ＳＴＦ（３）＝１／５＊０．３＝０．０６である。

【００３２】

次に、この実施例における識別ユニット１１０は、さらに、情報関数ＰＩＦを介してフォームにおいて秘密ファクターＣＰの字句として出現する確率を算出する。この実施例における情報関数ＰＩＦは、以下の通りである。

【００３３】

【数２】

$$PIF = \frac{P_n}{P_t}$$

【００３４】

ここで、Ｐｔは、現在秘密ファクターＣＰとしての名句の数を表す。Ｐｎは、フォームにおいて秘密ファクターＣＰの字句として出現する数を表す。上記の例としては、フォームには、秘密ファクターＣＰの名詞として、「名前」、「身分証明書」、「携帯電話」、及び「連絡住所」の４つの名詞がある。識別ユニット１１０は、フォームにおいて「連絡住所」、「名前」、「名称」、「人名」、及び「身分証明書」の５つの名詞を見つけ出し、見つけ出した５つの名詞を３種の字句に分類する。この場合、演算処理ユニットとしての識別ユニット１１０がＰＩＦ＝３／４として算出したため、フォームにおいて秘密ファクターＣＰの名詞として出現する確率が７５％であることを表す。

【００３５】

次に、識別ユニット１１０は、秘密データ関数ＰＩＦＶを介して、フォームに対応する４つの秘密ファクターＣＰの取り出しデータにおける出現頻度を算出する。この実施例における秘密データ関数ＰＩＦＶは、以下の通りである。

【００３６】

【数３】

$$PIFV = \left(\sum\nolimits_{n} STF(i)\right) \times PIF$$

【００３７】

ここで、ΣｎＳＴＦ（ｉ）は、各字句がフォームにおいて出現する重要性の総計を表す。ＰＩＦは、フォームにおいて秘密ファクターの字句として出現する確率を表す。上記の例に続き、ＰＩＦＶ＝（０．１＋０．１２＋０．０６）＊０．７５＝０．２１であることは、フォームに対応する４つの秘密ファクターＣＰの取り出しデータにおける出現頻度が０．２１であることを表す。

【００３８】

最後に、識別ユニット１１０は、出現頻度が秘密閾値以上であるかを判定する。上記の例に続き、この実施例における秘密閾値は０．１とする。従って、識別ユニット１１０は、秘密ファクターＣＰの出現頻度（０．２１である）が秘密閾値（０．１である）よりも大きいと判定し、取り出しデータにおけるフォームの内容が秘密データであることを表す。これにより、識別ユニット１１０は、ステップＳ２１０～Ｓ２６０を介して、取り出されたデータにおける特定フォーマットが秘密データであるか否かを判定することができる。

【００３９】

これにより、識別ユニット１１０は、特定フォーマットを表す秘密ファクターＣＰを介して取り出しデータにおける特定フォーマットの秘密性を識別することができ、高秘密性のデータの漏れを回避することができる。

【００４０】

次に、識別ユニット１１０は、複数のフォーマット特徴ＦＦにおいて取り出されていないフォーマット特徴ＦＦがあるか否かを判定する（ステップＳ２７０）。即ち、識別ユニット１１０は、取り出しデータにその他の特定フォーマットがあるか否かをさらに判定する。識別ユニット１１０が、取り出されていないフォーマット特徴ＦＦがあると判定した場合に、ステップＳ２２０に戻り、取り出しユニット１２０を介して取り出されていないフォーマット特徴ＦＦを取り出す。この場合、識別ユニット１１０は、取り出されていないフォーマット特徴ＦＦを取り出し特徴と定義することで、改めて定義された取り出し特徴に基づいて取り出しデータに対応する特定フォーマットがあるか否かを改めて判定する。上記の例に続き、フォームのフォーマット特徴ＦＦを判定した後、識別ユニット１１０がリストを表すフォーマット特徴ＦＦが取り出されていないと判定した場合に、識別ユニット１１０は、リストを表すフォーマット特徴ＦＦ（即ちフォーマット特徴ＦＦが複数の「ＴＡＢ」鍵からのメッセージである）を取り出し特徴として定義することで、改めて取り出し特徴に基づいて取り出しデータにリストのフォーマットがあるか否かを判定する。

【００４１】

逆に、識別ユニット１１０が、取り出されていないフォーマット特徴がないと判定した場合に、取り出しデータに判定すべき特定フォーマットがないことを表す。この場合、識別ユニット１１０は、ステップＳ２１０に戻り、複数のデータにおける次のデータを取り出す。さらに、識別ユニット１１０は、次のデータを取り出しデータとして定義することで、取り出しデータに対応する特定フォーマットがあるか否かを改めて判定する。

【００４２】

また、図１、図２Ａ、図２Ｂを同時に参照すると、電子装置１００は、分類ユニット１４０をさらに含む。分類ユニット１４０は、識別ユニット１１０に電気的に接続され、現在の取り出しデータに対して分類を行うものである。さらに詳しくは、識別ユニット１１０が、取り出されたフォーマット特徴ＦＦがないと判定した場合に、分類ユニット１４０は、現在の取り出しデータに対してさらに分類することで、取り出しデータにおける特定フォーマットがどの種類であるかをさらに判定することができる（ステップＳ２７５）。識別ユニット１１０は、分類ユニット１４０が現在の取り出しデータの分類を終了した後

に、ステップＳ２１０に戻り、複数のデータにおける次のデータを取り出す。１つの例として、分類ユニット１４０は、フォームを有する取り出しデータを履歴表、給料表、カルテ表、またはその他高秘密性のフォームに分類する。若しくは、分類ユニット１４０は、リストを有する取り出しデータを住所録、内線表、またはその他高秘密性のリストに分類する。

【００４３】

この実施例において、すべてのデータを関連性を有するため、分類ユニット１４０は、特定フォーマットにおける複数の秘密ファクターＣＰと、上記秘密ファクターＣＰがすべてのデータにおいて出現する回数とに基づいて現在の取り出しデータに対して分類を行う。例えば、分類ユニット１４０は、「履歴」、「名前」、「身分証明書」、「携帯電話」、及び「連絡住所」の５つの字句を秘密ファクターＣＰとする。分類ユニット１４０は、上記の５つの字句と、上記の５つの字句がすべてのデータにおいて出現する回数とに基づいて現在の取り出しデータに対して分類を行う。当然ながら、すべてのデータの間に関連性がない場合には、分類ユニット１４０は、特定フォーマットの複数の秘密ファクターＣＰにのみ基づいて現在の取り出しデータに対して分類を行うこともでき、本発明はそれに限定されるものではない。

【００４４】

また、本実施例における分類ユニット１４０は、例えばＴＦＩＤＦ（ｔｅｒｍ　ｆｒｅｑｕｅｎｃｙ－ｉｎｖｅｒｓｅ　ｄｏｃｕｍｅｎｔ　ｆｒｅｑｕｅｎｃｙ）、サポートベクトル　マシン（ｓｕｐｐｏｒｔ　ｖｅｃｔｏｒ　ｍａｃｈｉｎｅｓ、ＳＶＭ）、ベイジアン分類法（ｂａｙｅｓｉａｎ　ｃｌａｓｓｉｆｉｃａｔｉｏｎ）、またはバックプロパゲーションニューラルネットワーク（ｂａｃｋ　ｐｒｏｐａｇａｔｉｏｎｎｅｕｒａｌ（ＢＰＮ）ｎｅｔｗｏｒｋ）等の分類アルゴリズムにより、現在の取り出しデータに対して分類を行うことで、取り出しデータの分類をより正確に行う。当業者は、分類ユニット１４０が分類アルゴリズムにより現在の取り出しデータに対して分類を行う実施及び運用方法を理解することができるため、ここでは詳しい説明を省略する。

【００４５】

これにより、分類ユニット１４０は、特定フォーマットの取り出しデータに対して分類を行うことができる。従って、すべてのデータの識別が終了した場合に、ユーザは、すべてのデータにおける特定フォーマットがどの種類であるかを理解することができ、すべてのデータに対して制御を行うことができる。

【００４６】

以下、ユーザがユーザコンピュータ１０を介して１つのデータＤＡを遠隔サーバ２０に伝送することを例にして説明する。図６に示すように、電子装置１００は、ユーザコンピュータ１０と遠隔サーバ２０との間に設けられることで、ユーザコンピュータ１０からのデータＤＡにおける特定フォーマットの内容が秘密データであるか否かを判定する。説明の簡単化のために、本実施例におけるデータＤＡは、図３Ａに示すフォームを有し、この場合に取り出されたフォーマット特徴ＦＦは、フォームを表す特定フォーマットである。

【００４７】

図１、図３Ａ、図６を同時に参照すると、ユーザがユーザコンピュータ１０を介してデータＤＡを遠隔サーバ２０に伝送する過程において、電子装置１００における識別ユニット１１０は、取り出しユニット１２０を介してデータＤＡを取り出す。この場合、電子装置１００は、データＤＡにおける特定フォーマットの内容が秘密データであるか否かを判定し、かつ、秘密データの漏れを回避するために、しばらくの間、データＤＡを遠隔サーバ２０に伝送しない。

【００４８】

まず、電子装置１００における識別ユニット１１０は、現在取り出されたフォーマット特徴ＦＦ（即ちフォームを表す特定フォーマット）に基づいてデータＤＡにおいてフォームを表す特定フォーマットがあると判定する。識別ユニット１１０がデータＤＡにおいてフォームを表す特定フォーマットがあるか否かを判定する方法について、上記の実施例に

記載された通りであるため、ここでは詳しい説明を省略する。

【００４９】

次に、電子装置１００における識別ユニット１１０は、フォームを表す特定フォーマットに対応する複数の秘密ファクターＣＰのデータＤＡにおける出現頻度に基づいて、データＤＡにおけるフォームの内容が秘密データであると判定する。識別ユニット１１０がデータＤＡにおいてフォームを表す特定フォーマットの内容が秘密データであるか否かを判定する方法について、上記の実施例に記載された通りであるため、ここでは詳しい説明を省略する。

【００５０】

さらに、電子装置１００における識別ユニット１１０は、まだ識別していないフォーマット特徴ＦＦがあるか否かをさらに判定する。この実施例において、この場合の識別ユニット１１０には取り出されていないフォーマット特徴ＦＦが既にない。即ち、識別ユニット１１０は、データＤＡにおける特定フォーマットを既に判定した。次に、電子装置１００における分類ユニット１４０は、複数の秘密ファクターＣＰに基づいてデータＤＡに対して分類を行うとともに、データＤＡを履歴データに分類する。分類ユニット１４０がデータＤＡを履歴データに分類する方法について、上記の実施例に記載された通りであるため、ここでは詳しい説明を省略する。

【００５１】

この場合、電子装置１００は、ユーザコンピュータ１０からのデータＤＡにおけるフォームが履歴データであり、かつこの履歴データが秘密データであると判定する。電子装置１００は、データＤＡにおけるフォームが秘密データであると判定した後、実際の情報安全防護に基づいて後続の処理を行うことができる。例えば、電子装置１００は、データＤＡが遠隔サーバ２０に伝送されることを許可しないと同時に、システム管理者に対してユーザコンピュータ１０が秘密データを遠隔サーバ２０に伝送中であることを通知する。これにより、電子装置１００は、出力されたデータＤＡにおける特定フォーマットが秘密データであるか否かを識別することができ、秘密データが窃取意図のある者によって取得されることを防止し、データの漏れを回避することができる。

【００５２】

また、本発明は、コンピュータ読み取り可能な記録媒体により、上記秘密データを識別する方法におけるコンピュータプログラムを格納することで上記の工程を行うこともできる。このコンピュータ読み取り可能な記録媒体は、フロッピー(登録商標)ディスク、ハードディスク、光ディスク、ＵＳＢドライブ、磁気テープ、ネットワークを介してアクセス可能なデータベース、または当業者が容易に想到し得る同一機能を有する記録媒体であってもよい。

【００５３】

上記のように、本発明の実施例に係る秘密データを識別する方法、電子装置及びコンピュータ読み取り可能な記録媒体は、特定フォーマットを有するデータが秘密データであるか否かを判定することができる。これにより、本発明の実施例に係る秘密データを識別する方法、電子装置及びコンピュータ読み取り可能な記録媒体は、カウント数が多くないが機密記述が大量に含まれたデータの正しい機密レベルを提供するとともに特定フォーマットを有する秘密データを識別することができ、データの漏れを回避することができる。

【００５４】

上述したものは、本発明の好ましい実施例に過ぎず、本発明の実施の範囲を限定するためのものではない。

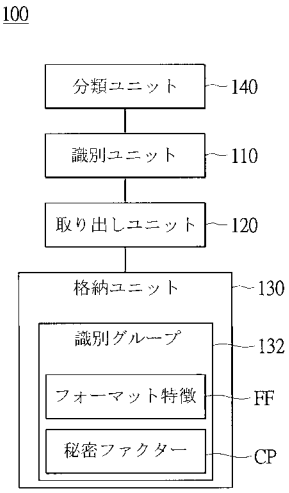
【符号の説明】

【００５５】

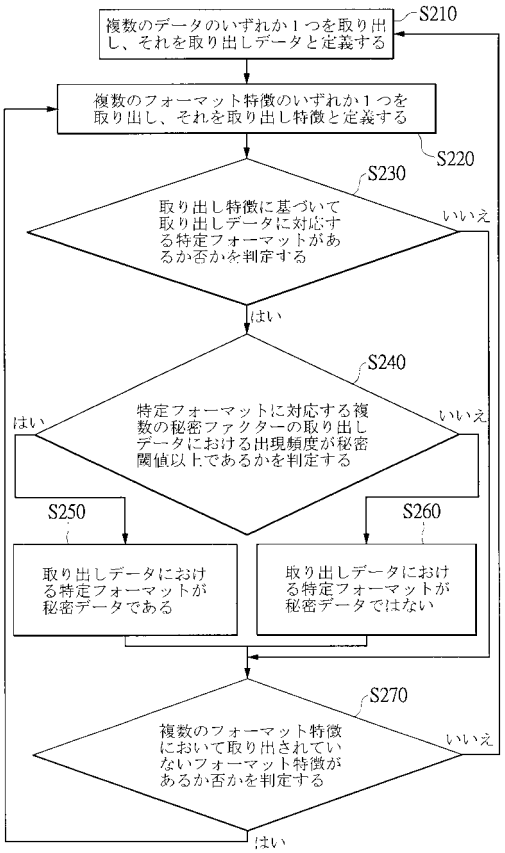
１００　電子装置
１１０　識別ユニット
１２０　取り出しユニット
１３０　格納ユニット

１３２　識別グループ
１４０　分類ユニット

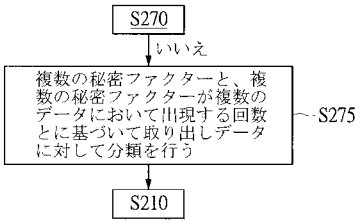
【図１】



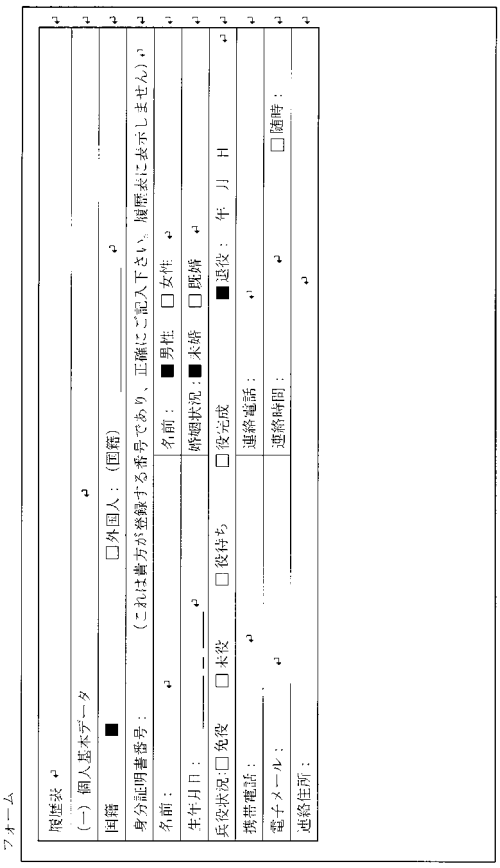
【図２Ａ】



【図２Ｂ】



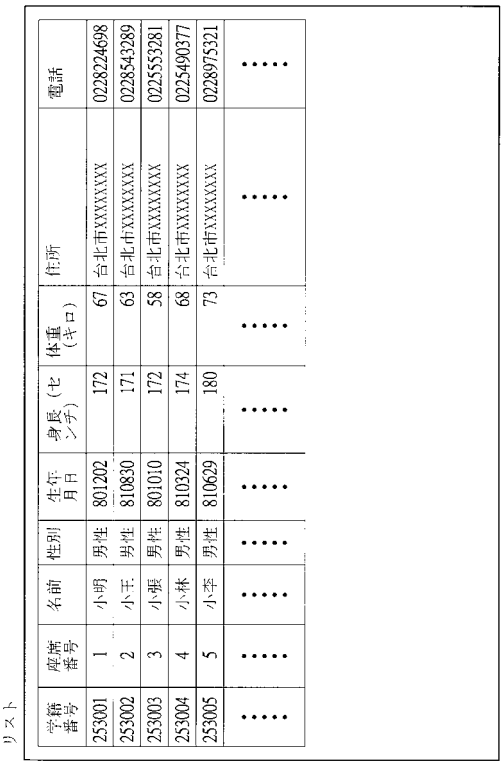
【図３Ａ】



【図３Ｂ】

履歴表
(一) 個人基本データ
国籍： ■ □外国人：(国籍)
身分証明書番号：(これは貴方が登録する番号であり、正確にご記入下さい。履歴表に表示しません)
名前：
性別：■男性 □女性
生年月日：
婚姻状況：■未婚 □既婚
兵役状況：□免役 □未役 □役待ち ■役完成 □退役：年 月 日
携帯電話：
連絡電話：
電子メール：
連絡時間： □随時：
連絡住所：

【図４Ａ】



学籍番号	座席番号	名前	性別	生年月日	身長（センチ）	体重（キロ）	住所	電話
253001	1	小明	男性	801202	172	67	台北市XXXXXXXX	0228224698
253002	2	小王	男性	810830	171	63	台北市XXXXXXXX	0228543289
253003	3	小張	男性	801010	172	58	台北市XXXXXXXX	0225553281
253004	4	小林	男性	810324	174	68	台北市XXXXXXXX	0225490377
253005	5	小李	男性	810629	180	73	台北市XXXXXXXX	0228975321
.....	.....	.....	.....	.....	.....	.....	.....	.....

【図４Ｂ】

学籍番号	座席番号	名前	性別	生年月日	身長（センチ）	体重（キロ）	住所	電話
253001	1	小明	男性	801202	172	67	台北市XXXXXXXX	0228224698
253002	2	小王	男性	810830	171	63	台北市XXXXXXXX	0228543289
253003	3	小張	男性	801010	172	58	台北市XXXXXXXX	0225553281
253004	4	小林	男性	810324	174	68	台北市XXXXXXXX	0225490377
253005	5	小李	男性	810629	180	73	台北市XXXXXXXX	0228975321

【図５Ａ】

テンプレート

一、計画目的

本計画は、ネットワークバージョン個人情報検出システム（以下、本システムという）［１］を強化することを目的とする。当該ソフトウェアは、主に、企業秘密データの自動化検索収集に用いられる。

二、お客様要求：

本プロジェクトのお客様要求の説明には、以下の「応用情景」、「システム要求」、及び「クラウド演算」の３つの部分が含まれる。

１、応用情景：

２、システム機能：

本プロジェクトのシステム機能は、それぞれ「機能性要求」及び「非機能性要求」の２つの部分について説明する。

【図５Ｂ】

計画目的

本計画は、ネットワークバージョン個人情報検出システム（以下、本システムという）［１］を強化することを目的とする。当該ソフトウェアは、主に、企業秘密データの自動化検索収集に用いられる。

お客様要求：

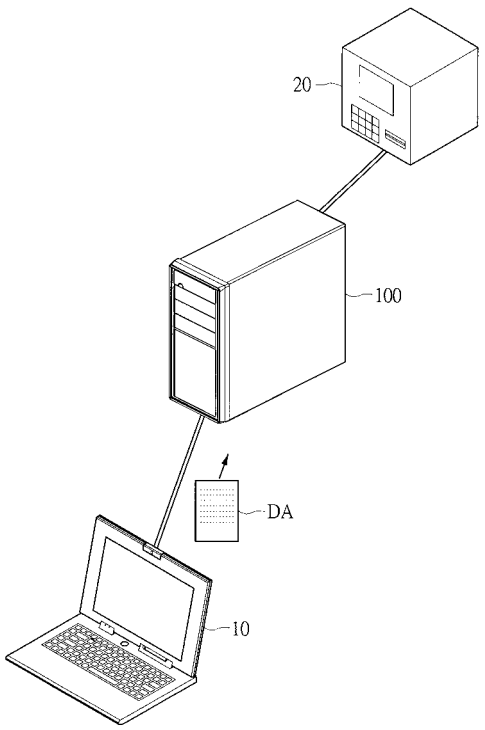
本プロジェクトのお客様要求の説明には、以下の「応用情景」、「システム要求」、及び「クラウド演算」の３つの部分が含まれる。

応用情景：

お客様要求：

本プロジェクトのシステム機能は、それぞれ「機能性要求」及び「非機能性要求」の２つの部分について説明する。

【図６】



フロントページの続き

(72)発明者　葉　信延
台湾新北市三重區三和路四段２９２巷３號３エフ
(72)発明者　劉　建宗
台湾新北市中和區國光街１１２巷２弄１０號１エフ