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

特許第4755689号
(P4755689)

(45)発行日　平成23年8月24日(2011.8.24)　(24)登録日　平成23年6月3日(2011.6.3)

(51)Int.Cl.		F I		
G06F 13/00	(2006.01)	G06F	13/00	610S
G06F 1/00	(2006.01)	G06F	1/00	370E
G06F 3/16	(2006.01)	G06F	3/16	340A
H04L 9/32	(2006.01)	H04L	9/00	673D

請求項の数 13　(全 14 頁)

(21)出願番号　特願2008-523270 (P2008-523270)
(86)(22)出願日　平成18年4月27日(2006.4.27)
(65)公表番号　特表2009-503661 (P2009-503661A)
(43)公表日　平成21年1月29日(2009.1.29)
(86)国際出願番号　PCT/EP2006/061873
(87)国際公開番号　WO2007/014790
(87)国際公開日　平成19年2月8日(2007.2.8)
審査請求日　平成21年1月22日(2009.1.22)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100108501
弁理士　上野　剛史
(74)代理人　100112690
弁理士　太佐　種一
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】正規受信者への安全なファイル配信のためのシステムおよび方法

(57)【特許請求の範囲】

【請求項１】

生体認証音声識別を用いて、意図された受信者を認証し該受信者によるファイルの受信を確認するために、送信者および前記受信者のコンピュータとサービス・プロバイダ・サーバとを含むコンピュータ・ネットワーク中で前記受信者に送信される前記ファイルを符号化するための方法であって、

－　前記送信者のコンピュータが、暗号化鍵を選択するステップと、

－　前記送信者のコンピュータが、前記受信者の音声を取得するために該受信者に音読させるための音声チェック・テキストを含む音声チェック・チケットを前記暗号化鍵と関連付けるステップと、

－　前記サービス・プロバイダ・サーバが、少なくとも前記暗号化鍵を含む前記音声チェック・チケットのアドレスを決定するステップと、

－　前記サービス・プロバイダ・サーバが、送信される前記ファイルを、前記暗号化鍵を用いて暗号化するステップと、

－　前記サービス・プロバイダ・サーバが、前記音声チェック・チケット・アドレスを前記ファイルと関連付けるステップと、

を含む方法。

【請求項２】

前記音声チェック・チケット・アドレスを前記ファイルと関連付ける前記ステップが、前記音声チェック・チケット・アドレスを前記ファイルのファイル名中に符号化するステ

ップを含む、請求項１に記載の方法。
【請求項３】
暗号化鍵を選択する前記ステップが、前記暗号化鍵を生成するステップを含む、請求項１または２に記載の方法。
【請求項４】
暗号化鍵を選択する前記ステップが、前記暗号化鍵を別のコンピュータ・デバイスから受信するステップを含む、請求項１または２に記載の方法。
【請求項５】
少なくとも前記暗号化鍵を含む音声チェック・チケットの前記アドレスを決定する前記ステップが、前記音声チェック・チケットを生成するステップを含む、請求項１～４のいずれか１項に記載の方法。
【請求項６】
少なくとも前記暗号化鍵を含む音声チェック・チケットの前記アドレスを決定する前記ステップが、
－　前記暗号化鍵を送信し、少なくとも前記暗号化鍵を含む音声チェック・チケットを要求するステップと、
－　前記音声チェック・チケットのアドレスを受信するステップと、
を含む請求項１に記載の方法。
【請求項７】
請求項１～６のいずれか１項に記載の方法に従って符号化されたファイルを復号するための方法であって、
－　前記受信者のコンピュータが、音声チェック・チケットの前記アドレスを前記ファイルから抽出し、前記音声チェック・チケット・アドレスを復号するステップと、
－　前記受信者のコンピュータが、前記音声チェック・チケット・アドレスにおける前記音声チェック・チケットに関連付けられた音声チェック・テキストにアクセスするステップと、
－　前記受信者のコンピュータが、前記音声チェック・テキストの読み上げを送信するステップと、
－　前記受信者のコンピュータが、前記読み上げの声紋が前記音声チェック・チケットと関連付けられた声紋と一致すれば、解読鍵を受信するステップと、
－　前記受信者のコンピュータが、前記解読鍵を用いて前記ファイルを解読するステップと、
を含む方法。
【請求項８】
前記サービス・プロバイダ・サーバが、前記読み上げの前記声紋が前記音声チェック・チケットと関連付けられた前記声紋と一致し、前記読み上げの前記テキストが前記音声チェック・チケットと関連付けられた前記音声チェック・テキストと一致すると判断した場合、前記受信者のコンピュータへ前記暗号化鍵を送信する、請求項７に記載の方法。
【請求項９】
前記サービス・プロバイダ・サーバが、前記音声チェック・チケットの前記アドレスをファイルの名前の内部に符号化する、請求項７または８のいずれか１項に記載の方法。
【請求項１０】
請求項１～６のいずれか１項に記載の方法に従って符号化されたファイルの受信者を認証するための方法であって、
－　前記サービス・プロバイダ・サーバが、前記受信者からの要求があり次第、前記要求と共にアドレスが受信される前記音声チェック・チケットに関連付けられた音声チェック・テキストを前記受信者のコンピュータへ送信するステップと、
－　前記サービス・プロバイダ・サーバが、前記受信者からのテキスト読み上げが受信され次第、
－　前記テキスト読み上げから声紋を抽出するステップと、

－　前記抽出された声紋を前記受信者に関連付けられた前記声紋と比較するステップと、

－　前記抽出された声紋が前記受信者に関連付けられた前記声紋と一致すれば、前記音声チェック・チケットに関連付けられた前記暗号化鍵を前記受信者のコンピュータに送信するステップと、

を含む方法。

【請求項１１】

－　前記サービス・プロバイダ・サーバが、前記受信者からのテキスト読み上げが受信され次第、

－　前記テキスト読み上げをテキストに変換するステップと、

－　前記変換されたテキストを前記音声チェック・チケットと関連付けられた前記音声チェック・テキストと比較するステップと、

－　抽出された声紋が前記受信者と関連付けられた前記声紋と対応し、前記変換されたテキストが前記音声チェック・チケットと関連付けられた前記音声チェック・テキストと対応すれば、前記受信者のコンピュータに、前記音声チェック・チケットと関連付けられた前記暗号化鍵を送信するステップと、

をさらに含む、請求項１０に記載の方法。

【請求項１２】

請求項１～１１のいずれか１項に記載の前記方法の各ステップを実行するよう適合された手段を含む、装置。

【請求項１３】

請求項１～１１のいずれか１項に記載の方法の各ステップをコンピュータに実行させる、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、電子文書の安全な配信に関し、より具体的には、自動音声認識および生体認証音声話者識別（biometric voice speaker identification）を用いて、意図された受信者（intended recipient）によるファイルの受信を検証および確認するための方法およびシステムに関する。

【背景技術】

【０００２】

電子メールにより、人（または自動ロボット機械）は、テキスト・メッセージならびに、例えば、写真のコレクション、録音物、および定様式文書のようなその他の情報を世界中どこの電子メール・ユーザへも迅速かつ容易に電子的に送信することが可能になる。例えば、ハード・ディスク・フォルダ中またはネットワーク共有フォルダ中のファイルとしてアクセスできるものは何でも、電子メール添付ファイルに含まれ得る。電子メール添付ファイルは、画像、文書、スプレッド・シート、ｍｐ３ファイル、プログラム等であり得る。ひとたびファイルが電子メールに添付されると、電子メールならびに添付ファイルは、通信ネットワーク（例えば、インターネット）上で他のコンピュータ・システムに送信され得る。添付ファイルにアクセスする受信ユーザまたは他のユーザは、そのファイルをさらなる処理のためにローカル・システム・ストレージに取り出すことができる。

【０００３】

開放されており安全ではないネットワーク上、特にインターネット上での電子情報の交換と関連した深刻なリスクは、詐欺師が電子通信を傍受、または電子メールのような情報の一部にアクセスして、当該電子通信の正規受信者になりすまし得るということである。

【０００４】

意図された受信者に電子文書を配信し、次に、別人ではなくその意図された受信者が文書を本当に受信したことを確認することが必要とされることがよくある。同様に、意図された受信者に電子文書を配信し、次に、その意図された受信者が、その文書を受信した後

、文書の内容を開いて閲覧したという確認を受信することが望ましいことがよくある。
【０００５】
意図された受信者への文書の配信を、そのような配信文書の受信をその意図された受信者が検証および確認することにより保証することは、例えば、様々な法的または安全関連用途において必要とされることがある。さらに、そのような種類の用途においては、受信者が、文書の受信および閲覧を容易に拒否できないことが一般に望ましい。
【０００６】
例えば、電子メールに添付された電子文書およびファイルの、意図された正規の受信者への配信を保証し、意図された受信者による受信確認を得るための以前の方法にはいくつかの欠点がある。第１の制限は、一般に、配信確認は、受信者が実際に、受信された文書の内容を閲覧するか、読むか、さもなければ気付かされたことを確実に証明できないことである。例えば、受信者の私的情報の提供、または確認メッセージへのデジタル署名に基づく従来技術の方法によれば、意図された受信者は後に、確認を拒否し、自分は確認を送らなかったと断言することがあり得る。例えば、意図された受信者は、パスワードのような私的情報が損なわれ、別の受信者によって提供されたと主張することがあり得る。また、電子メール送信者は、電子メールが受信者の電子メール・サーバにうまく配信されたこと、およびその電子メールが開かれたという自動確認を受信できるが、電子メールに添付されたファイルにアクセスして開く人物が、実際に意図された正規の受信者であるという検証および確認はなく、さらに、文書開披に関するどのような確認も、すなわち、意図された正規の受信者か別の人物である受信者が、配信された電子メールに送信者によって添付されたファイルまたは文書を実際に開きまたは読んだかどうかの確認もない。そのような状況において、意図された受信者は、電子メールが受信されたと確認するが、後に、電子メールの内容全体または電子メール添付ファイルの内容に受信者が気付いていたことを否定することがあり得る。
【０００７】
現代の電子メール・システムのほとんどは、受信者による（おそらく、意図された受信者による）電子メールの受信および開披を確認するメッセージを送信者に送る電子メールを構成することを可能にする一方で、電子メールに添付されたファイルが受信者により開かれたことを送信者に知らせる同等の機構は皆無である。さらに、電子メールに添付されたすべてのファイルが取り出されて将来の処理のために保存された後でさえ、当該ファイルの正規の意図された受信者によって開披およびアクセスされたことをその電子メールの送信者に保証および確認する機構は全く提供されていない。
【０００８】
結果として、電子メールに添付された電子文書およびファイルの送信者が、意図された受信者へのそれらの文書およびファイルの配信を、拒否できないやり方で保証、検証および確認できるようにする方法およびシステムが必要である。
【発明の開示】
【発明が解決しようとする課題】
【０００９】
従って、上記で説明されたような従来技術の欠点を改善することが本発明の大まかな目的である。
【課題を解決するための手段】
【００１０】
意図された受信者への電子文書およびファイルの配信を保証するための改善された方法およびシステムを提供することが、本発明の別の目的である。
【００１１】
あるファイルの内容へのアクセスを要求するユーザの身元を、そのユーザがそのファイルの内容にアクセスできるようにする前に検証するようにされた、意図された受信者への電子文書およびファイルの配信を保証するための改善された方法およびシステムを提供することも、本発明の別の目的である。

【００１２】
ファイルの送信者に、意図された受信者によるそのファイルの内容へのアクセスの拒絶できない確認を提供するようにされた、意図された受信者への電子文書およびファイルの配信を保証するための改善された方法およびシステムを提供することが、本発明のさらなる目的である。
【００１３】
意図された受信者への電子文書およびファイルの配信を、声紋（voiceprint）を用いて保証するための改善された方法およびシステムを提供することが本発明のさらなる目的である。
【００１４】
これらおよびその他の関連付けられた目的の遂行は、生体認証音声識別を用いて、受信者を認証し該受信者によるファイルの受信を確認するために、コンピュータ・ネットワーク中で意図された受信者に送信されるファイルを符号化するための方法であって、以下のステップ、
－　暗号化鍵（encryption key）を選択するステップと、
－　音声チェック・チケット（voice check ticket）を前記暗号化鍵と関連付けるステップと、
－　少なくとも前記暗号化鍵を含む前記音声チェック・チケットのアドレスを決定するステップと、
－　送信されるファイルを、前記暗号化鍵を用いて暗号化するステップと、
－　前記音声チェック・チケット・アドレスを前記ファイルと関連付けるステップと、を含む方法、
上記の方法に従って符号化されたファイルを復号するための方法であって、以下のステップ、
－　音声チェック・チケットのアドレスを前記ファイルから抽出し、前記音声チェック・チケット・アドレスを復号するステップと、
－　前記音声チェック・チケット・アドレスにおける前記音声チェック・チケットに関連付けられた音声チェック・テキスト（voice check text）にアクセスするステップと、
－　前記音声チェック・テキストの読み上げを送信するステップと、
－　前記読み上げの声紋が前記音声チェック・チケットと関連付けられた声紋と一致すれば、解読鍵を受信するステップと、
－　前記解読鍵を用いて前記ファイルを解読するステップと、を含む方法、
ならびに
上記の方法に従って符号化されたファイルの受信者を認証するための方法であって、以下のステップ、
－　前記受信者からの要求があり次第、前記要求と共にアドレスが受信される音声チェック・チケットに関連付けられた音声チェック・テキストを送信するステップと、
－　前記受信者からのテキスト読み上げが受信され次第、
　－　前記テキスト読み上げから声紋を抽出するステップと、
　－　前記抽出された声紋を前記受信者に関連付けられた声紋と比較するステップと、
　－　前記抽出された声紋が前記受信者に関連付けられた声紋と一致すれば、前記音声チェック・チケットに関連付けられた暗号化鍵を前記受信者に送信するステップと、を含む方法、
により達成される。
【００１５】
本発明のさらなる利点は、図面および詳細な説明を考察すれば当業者にとり明白になる。どのような付加的な利点も本明細書に組み込まれることが意図される。
【発明を実施するための最良の形態】
【００１６】
本発明によれば、電子的に送信されたファイルへのアクセスを保証し、他の誰かではな

く、意図された受信者がそのファイルを受信し開披したことを検証および確認するための方法およびシステムが開示される。主な原理は、暗号化鍵を、暗号化ファイルがその暗号化鍵を用いてのみ解読されるように受信者声紋と組み合わせることにあり、暗号化鍵は、受信者が所定のテキストを読んだ後に、もしこの読み上げの声紋が受信者声紋と一致すれば、受信者に送信される。

【００１７】

一般に知られているように、ほとんどの音声生体認証方式は、ユーザの声紋、すなわち、ユーザがシステムに登録する際に生成されるその人物に特有の音声特性のテンプレートを生成する。システムにアクセスにしようとするその後の全ての試みは、ユーザの生の音声サンプルが事前記録されたテンプレートと比較されるように、ユーザに話すことを要求する。例えば、この件に関する参考資料は、「Apparatus and method for speakerverification/identification/classification employing non-acoustic and/oracoustic models and databases」と題されたKanevskyの米国特許第６，５２９，８７１号である。

【００１８】

図１は、あるユーザが、本発明の方法に従って文書を送付したい別の人物の音声をどのように記録できるかを示す例を例示する。この例において、電話会話の一部が音声記録のデータベース中に記録される。示されるように、電話１０５を有するユーザ１００は、標準の公衆交換電話網（ＰＳＴＮ）１２０を介して電話１１５を有するユーザ１１０に電話をかけることができる。そのような場合、ユーザ１１０は受信者と呼ばれ、ユーザ１００は送信者と呼ばれる。通話の間、送信者１００は、後に受信者１１０の声紋を決定するために、会話の一部を記録できる。好ましい実施形態において、送信者１００は、受信者音声記録を音声記録のデータベース中に格納する。さらに好ましい実施形態において、各受信者音声記録は、参照符号１２５により例示されるように、受信者名、受信者声紋識別子および受信者音声記録を含む。音声記録のデータベースは、送信者のコンピュータまたはハンドヘルド・デバイス１３０あるいは公的ネットワーク、例えば、インターネット、または私的ネットワークを通してアクセス可能なリモート・サーバ（図示せず）に局所的に格納できる。

【００１９】

受信者の音声サンプルを記録した後、送信者は受信者の声紋を決定しなければならない。これは、一般サーバ上または特定の音声チェック・サーバ上で局所的に行われ得る。例示のため、声紋の決定および声紋の格納は、図２に示されるように、特定の音声チェック・サーバ上で行われる。送信者１００が、受信者の音声サンプルを受信者音声記録として格納した後、そのサンプルは、完全にまたは部分的に、私的または公的ネットワーク２００、例えば、インターネットを通して特定の音声チェック・サーバ２０５へ送信される。さらに好ましい実施形態において、音声サンプルは、匿名のオーディオ・ファイルとして送信される。音声チェック・サーバ２０５は、音声サンプルを処理し、受信者の声紋を計算おおび格納し、その声紋に識別子（ＩＤ）を割り当てる。声紋および関連付けられたＩＤは、声紋データベース２１０中に局所的に格納される。声紋ＩＤは次に、それが局所的に格納される送信者のコンピュータ１３０に送信される。例えば、声紋ＩＤは、上記で論じられたように、受信者音声記録１２５内に格納され得る。

【００２０】

送付されるファイルを暗号化するために、送信者１００は最初に、上記で開示されたように、受信者の音声サンプルおよび声紋ＩＤを取得しければならない。次に、送信者は好ましくは、音声チェック・チケットを作成する。送信者は、音声チェック・サーバまたはサード・パーティ・サーバに音声チェック・チケットを要求することもできる。音声チェック・チケットは主に、声紋ＩＤ、暗号化鍵および音声チェック・テキストから成る。音声チェック・チケットに関連付けられた暗号化鍵は、送信されるファイル暗号化するために送信者により使用される。音声チェック・チケットは次に、音声チェック・サーバに送られ、この音声チェック・サーバは、音声チェック・チケットのアドレスまたはＵＲＬ、すなわち、音声チェック・チケットをダウンロードできるアドレスを返送する。音声チェ

ック・チケットのアドレスまたはＵＲＬは、送信される符号化ファイルの名前の内部に符号化される。

【００２１】

図３は、本発明に従って、送付される暗号化ファイルに関連付けられた音声チェック・チケットが、送信者のコンピュータ１３０から音声チェック・サーバ２０５にどのようにアップロードされるかを例示する。送信者のコンピュータが音声チェック・チケットを音声チェック・サーバに送信した後、音声チェック・チケットは、好ましくは、音声チェック・サーバ２０５の音声チェック・チケット・データベース３００に格納される。示されるように、音声チェック・サーバ２０５は、音声チェック・チケットのアドレスまたはＵＲＬ、すなわち音声チェック・チケットをダウンロードできるアドレスまたはＵＲＬを送信することにより、送信者のコンピュータ１３０に応答する。アドレスまたはＵＲＬは、好ましくは、送信者のコンピュータ１３０中の音声チェック・チケットのローカル・コピーの予約フィールドに格納される。

【００２２】

図４は、送信者であるLewis Carrollが、音声チェック・サーバに格納された音声チェック・チケットにリンクされた暗号化ファイルを電子メールに添付する、本発明の応用の一例を示す。その電子メールが受信されると、音声チェック・チケットは、受信者の身元を検証し、ファイルの受信を確認し、ファイルを解読するために、受信者（Jane R. Friday）によりアクセスされなければならない。この図は、音声チェック・チケットのアドレスまたはＵＲＬ（例えば、ハイパーリンク「http://www.voicecheck.com/R7KWW56T.vct」）が、特定の辞書編集を用いて添付ファイルのファイル名にどのように符号化され得るかも例示している。例えば、特定の辞書編集は、「://」、および「/」などのＵＲＬの辞書編集において有効な文字または文字グループを、「;」および「,」などのファイル名の辞書編集において有効な文字でそれぞれ置き換えることにある。本発明によれば、電子メール受信者が音声チェック・チケットにリンクされたファイル添付のアイコンをクリックすると、添付ファイルのファイル名が構文解析され、音声チェック・チケットのＵＲＬがその同じファイル名から抽出および復号される。意図された受信者によるファイル受信を検証するために必要とされる音声識別および音声チェック・チケット妥当性検査操作に音声チェック・サーバ上でアクセスおよび実行し、受信ファイルを解読するために必要とされる暗号化鍵を音声チェック・サーバから取り出すために、抽出されたＵＲＬを用いてハイパーリンクがトリガされる。

【００２３】

図５は、音声チェック・チケットのアドレスまたはＵＲＬを埋め込む暗号化ファイルを受信者が受信する場合の音声チェック・チケット処理の例を示す。音声チェック・サーバ２０５の音声チェック・チケット・データベース３００において音声チェック・チケットが受信者１１０によりアクセスされると、音声チェック・チケットの音声チェック・テキストが抽出され、音声チェック・サーバから受信者のコンピュータまたはハンドヘルド・デバイス４００に送信される。受信された音声チェック・テキストが表示され、受信者１１０は、ファイル受信確認および受信者身元検証を実行するために、このテキストを音読するよう促される。上記で論じられたように、受信者は、音声認識および音声識別によって、その受信者がそのファイルを開くことを許可された人物であることを検証するために、音声チェック・テキストを音読するよう促される。受信された音声チェック・テキストを受信者が音読すると、受信者１１０の発話（utterance）は、好ましくは、受信者のコンピュータ４００上に記録され、音声チェック・サーバ２０５に送信される。音声チェック・サーバ２０５において受信された発話は、音声認識により復号され、音声チェック・チケットの音声チェック・テキスト成分と比較される。加えて、受信された発話の声紋が計算され、同じ声紋ＩＤに対応する記録された声紋ファイルと比較される。もし両方のチェックの結果がポジティブであれば、意図された受信者の同一性が立証され、ファイルを解読するために、暗号化鍵が受信者のコンピュータ４００に送信される。音声チェック・サーバ２０５上に格納された音声チェック・チケットにアクセスしてこれを取り出すこと

により、送信者１００は、意図された受信者によるファイルの受信の拒絶できない確認を得るか、あるいは正規ではない受信者または詐欺師によるファイル開披の試みが成功しなかったことに気付き得る。

【００２４】

図６は、送信される文書を暗号化するための一般的なアルゴリズムの例を例示する。その実装に応じて、アルゴリズムは、１つまたは異なるコンピュータまたはサーバ上で走るいくつかのモジュールに分割できる。図６の例によれば、アルゴリズムは、３つの異なる部分、すなわち送信者のコンピュータ・モジュール６００（または、送信者がアクセス可能なネットワーク・サーバ）、セキュリティ・サーバ・モジュール６０５、および音声チェック・サーバ・モジュール６１０に分割される。受信者名をタイプすることにより、文書またはファイルが送信されるべき受信者名を選択し、その氏名をリスト中からまたは同様の既知のインタフェース方法に従って選択した後（ステップ６１５）、送信者のコンピュータ・モジュール６００は、選択された受信者の声紋がすでに存在するかどうかを決定する（ステップ６２０）。例えば、送信者のコンピュータ・モジュール６００は、受信者名が受信者識別子（ＩＤ）に関連付けられて、音声チェック・サーバ中に格納された声紋データベース中の特定の声紋を選択するためにそのようなＩＤが使用され得るテーブルをホストすることができる。そのような例によれば、受信者声紋が存在するかどうかのチェックは、テーブル中の受信者名の存在をチェックすることにある。選択された受信者についての声紋が全く存在しなければ、送信者のコンピュータ・モジュール６００は、ネットワーク・インタフェース、電話システム、または任意の同等なシステムを通して受信者記録を受信する（ステップ６２５）。受信者記録は、音声チェック・サーバ・モジュール６１０に送信され、そこから対応するＩＤを送信者のコンピュータ・モジュール６００が受信する（ステップ６３０）。音声チェック・サーバ・モジュール６１０は、受信された受信者記録から声紋を抽出し、ＩＤを決定し、この声紋を対応するＩＤと共に声紋データベース中に格納する（ステップ６３５）。もう一つの選択肢として、受信者が自分の声のオーディオ記録を音声チェック・サーバ・モジュール６１０に直接送り得ることに注目するべきである。

【００２５】

もし声紋が選択された受信者と関連付けられていれば、送信者のコンピュータ・モジュール６００は、暗号化鍵および音声チェック・チケット（ＶＣＴ）の要求をセキュリティ・サーバ・モジュール６０５に送る（ステップ６４０）。上記で言及されたように、セキュリティ・サーバ・モジュール６０５は、送信者のコンピュータ・モジュール６００と一体化させることができ、その結果、暗号化鍵は送信者のコンピュータにおいて生成され、音声チェック・チケットも送信者のコンピュータにより作成される。セキュリティ・サーバ・モジュール６０５は、標準の所定の暗号化アルゴリズム、例えばＲＳＡのような公開鍵アルゴリズムにより用いられる暗号化鍵を生成する（ステップ６４５）。暗号化鍵は、送信者のコンピュータ・モジュール６００により受信され（ステップ６５０）、送信者のコンピュータ・モジュール６００は、送信するファイルを暗号化するためにその暗号化鍵を用いる（ステップ６５５）。加えて、セキュリティ・サーバ・モジュール６０５は、音声チェック・チケットを生成する（ステップ６６０）。上記で論じられたように、各音声チェック・チケットは好ましくは、声紋ＩＤ、暗号化鍵および音声チェック・テキストを含む。声紋ＩＤは、選択された受信者に従って送信者のコンピュータ・モジュール６００によって決定されるのに対して、暗号化鍵および音声チェック・テキストは、セキュリティ・サーバ・モジュール６０５によって決定される。暗号化鍵は、標準の鍵生成アルゴリズムに従って無作為に生成される。音声チェック・テキストは、種々の方法で生成できる。例えば、音声チェック・テキストは、受信者による暗号化ファイルの受信の宣言確認のように、送信者によって書かれ得る。音声チェック・テキストは、例えば、暗号化ファイルが添付されている電子メールテキストの一部をコピーすることによって、送信者より選択され得る。代わりに、音声チェック・テキストは、音声チェック・サーバ・モジュール６１０によって、例えば、前記サーバに格納またはそれからアクセスされる文書のライブ

ラリからテキストを無作為に選択することにより自動的に生成され得る。

【００２６】

音声チェック・チケットは次に、音声チェック・サーバ・モジュール６１０に送られ（ステップ６６５）、音声チェック・チケット・データベース中に格納される（ステップ６７０）。音声チェック・サーバ・モジュール６１０は、格納された音声チェック・チケットのアドレスまたはＵＲＬをセキュリティ・サーバ・モジュール６０５に返し（ステップ６７５）、次にセキュリティ・サーバ・モジュール６０５が、格納された音声チェック・チケットのアドレスまたはＵＲＬを送信者のコンピュータ・モジュール６００に送信する（ステップ６６５）。格納された音声チェック・チケットのアドレスまたはＵＲＬは次に、送信者のコンピュータ・モジュール６００において、送信されるファイルの名前内に符号化される（ステップ６８０）。ファイルは、送信される状況にある。なぜならば、そのファイルは符号化されており、意図された受信者がそれを解読できるようにする情報を含んでいるからである。

【００２７】

図７は、意図された受信者によるファイルの受信を確認し、受信者の身元を検証し、暗号化鍵を正規の受信者に配信するための、本発明による方法の主なステップを例示する。好ましい実施形態において、そのようなアルゴリズムは、２つの異なる部分を含む。すなわち、受信者のコンピュータまたはハンドヘルド・デバイス内部に実装される７００で示される第１の部分および音声チェック・サーバ内部に実装される７０５で示される第２の部分である。図６に関連して説明された方法のような本発明の方法に従って暗号化されたファイル、例えば電子メールの添付ファイルを受信した後、ファイル名が構文解析され（ステップ７１０）、構文解析されたファイル名から音声チェック・チケットのアドレスまたはＵＲＬが抽出され、復号される（ステップ７１５）。構文解析されたファイル名からの抽出およびアドレスまたはＵＲＬの復号は、符号化ステップで使われた辞書編集に依存する。辞書編集、符号化および復号の例を、以下説明する。ひとたびアドレスまたはＵＲＬが復元されると、音声チェック・チケットがアクセスされ（ステップ７２０）、この音声チェック・チケットに含まれている音声チェック・テキストを受信する（ステップ７２５）。音声チェック・テキストは、受信者がテキストを音読できるように、受信者コンピュータ・ディスプレイに表示される。受信者の読み上げは、アナログかデジタルのオーディオ信号として音声チェック・サーバに送信される（ステップ７３０）。受信されたオーディオ信号は、標準の音声認識エンジンに従って音声チェック・サーバによってテキストに変換され（ステップ７３５）、変換されたテキストと音声チェック・テキストとを比較するためにテストが行われる（ステップ７４０）。もし変換されたテキストが音声チェック・テキストと異なれば、受信者の要求は拒絶され、もし変換されたテキストが音声チェック・テキストと同一であれば、受信されたオーディオ信号の声紋計算される（ステップ７４５）。この声紋は次に、音声チェック・サーバの声紋データベース中に格納されている受信者識別子に関連付けられた声紋と比較される（ステップ７５０）。例えば、受信者識別子は、受信者自身によりオーディオ記録と共に送信され得る。もし声紋が異なれば、受信者の要求は拒絶され、音声チェック・サーバは、暗号化鍵を受信者のコンピュータまたはハンドヘルド・デバイスに送信し（ステップ７５５）、その結果、受信ファイルは、受信者のコンピュータにより解読される（ステップ７６０）。本発明の特定の実施形態において、音声チェック・チケットの音声チェック・テキストは、音声チェック・サーバによって異なるテキストに自動的に修正され、その結果、そのファイルにアクセスしようとする各試みについて、異なる音声チェック・テキストが識別のために受信者に送信される。この実施形態によれば、受信者が識別されて、解読鍵が受信者に送信された場合に、音声チェック・テキストが修正される。代わりに、本発明の別の実施形態において、ひとたび受信者が識別され、解読鍵が初めて受信者に送信されると、音声チェック・チケットは自動的に詳記され、音声チェック・サーバから破棄され、その結果、ひとたびファイルが初めて解読されると、その同じファイルを解読しようとするさらなる試みは、失敗するであろう。

【００２８】
送信するファイルの名前内にアドレスまたはＵＲＬを符号化するために、ファイル・システムにより禁止されることがある特定の文字、例えば、Microsoft Windowsシステム（Windowsは、マイクロソフト・コーポレーションの商標である）における「¥」を回避するように、またはそれらのサイズを減らすようにアドレスを符号化するように、あるいはその両方を行うように、特定の辞書編集が決定される。符号化されるアドレスは、任意の形態、例えば、ローカル・アドレス、私的ネットワーク内のアドレスまたはインターネット・アドレスであり得るが、例示のため、以下の説明において示される例は、ＵＲＬタイプのアドレスに基づく。

【００２９】
図８は、ファイル名中にアドレスを符号化するために用いられるアルゴリズムの例を例示する。図８ａに示されるように、第１のステップは、ファイルの一次ファイル名を得ること（ステップ８００）、すなわち、ファイルのファイル名、および音声チェック・チケットのアドレスまたはＵＲＬを得ること（ステップ８０５）にある。次に、アドレスは符号化され（ステップ８１０）、一次ファイル名および符号化されたアドレスを含むファイル名でリネームされる（ステップ８２０）前に、特定の区切り記号を用いてファイルの一次ファイル名とマージされる（ステップ８１５）。

【００３０】
図８ｂは、図８ａにおいてステップ８１０と呼ばれる符号化アルゴリズムの例を示す。変数ｉが０に設定され（ステップ８２５）、ｉ番目の文字が、アドレス文字列から抽出される（ステップ８３０）。抽出された文字が有効であるか、そうでなければユーザのデバイスのファイル・システムによって課されるファイル名構文規則によって禁止されるかを決定するために試験が実行される（ステップ８３５）。もし抽出された文字がファイル名有効文字であれば、変数ｉは、１だけ増分され（ステップ８５０）、変数ｉがその最大値に達したかどうか、すなわち、アドレス文字列の全ての文字が処理されたかどうか決定するために試験が実行される（ステップ８５５）。もし変数ｉがその最大値に達していなければ、アルゴリズムの最後の４ステップが繰り返される（ステップ８３０～８５０）。他に、もし変数ｉがその最大値に達していれば、プロセスは停止される。もしアドレス文字列から抽出された文字がファイル名構文規則により禁止されれば、対応する有効な文字、または文字グループが、辞書編集テーブル８４５の中から選択され、この選択された文字、または文字グループは、禁止された文字に取って代わる（ステップ８４０）。次に、変数ｉは１だけ増分され、変数ｉがその最大値に達したかどうかを決定するために前に説明されものと同じ試験が実行される。

【００３１】
上述のアルゴリズムの例示として、「Biometri.txt」と名付けられたテキスト・ファイルのケースを考えて見よう。これは、暗号化された電子メール添付ファイルとしてユーザが他の誰かに送付したいテキスト・ファイルであり、この目的のため、音声チェック・チケット・アドレス文字列をファイル名に符号化するための辞書編集テーブルが使用され、そこでは、
「://」は「;」に関連付けられ、
「/」は「,」に関連付けられる。

【００３２】
ファイルの開披を可能にする音声チェック・チケットを取得するためには、このファイルに対応する音声チェック・チケットにアクセスすることが必要とされる。例示のため、この音声チェック・チケットが以下のＵＲＬからダウンロードできると考えることができる：
http://www.voicecheck.com/tickets/R7KWW56.vct

【００３３】
送信者が文書「Biometric.txt」を送付またはファイルに添付する前、ファイルを暗号化して音声チェック・チケットを生成し、この音声チェック・チケットのアドレスまたは

ＵＲＬを得るために、「ファイルを暗号化する（encrypt file）」のようなオプションが選択され得る。

【００３４】

ファイル名は、図８に例示されるアルゴリズムに従って修正される。第一に、前の辞書編集テーブルを用いて、アドレスは以下のように符号化される：

http;www.voicecheck.com,tickets,R7KWW56.vct

【００３５】

次に、符号化されたアドレスはファイル名とマージされる。この例において、符号化されたアドレスは、区切り記号として用いられる括弧で囲まれる。符号化されたアドレスは、一次ファイル名の拡張子ドットの前に以下のように挿入され：

Biometric(http;www.voicecheck.com,tickets,R7KWW56.vct).txt

ファイルは、この修正ファイル名を用いてリネームされる。

【００３６】

例示のために、この符号化アルゴリズムが意図的に非常に単純であることに注目しなければならない。好ましいアルゴリズムは、一連の禁止文字を単一の文字で置き換えること、および文字の集合をよりコンパクトな符号で置き換えること、例えば、「http://」を「H!」で置き換えることになるであろう。

【００３７】

本発明の利点のうち、

－　送信者は、受信者に送付されたファイルを、それらのファイルが意図された受信者のみにより開披されことを保証および確認することにより、保護し、

－　ファイルの送信者は、意図された受信者によるファイル受信の拒絶できない確認を得、正規ではない受信者または詐欺師によるそのファイルを開披しようとする試みが成功しなかったことを知らされ、

－　自分自身の声を記録することにより、どのユーザも、他人による不正アクセスから任意のファイルを選択的に保護できる、

ことが認められるはずである。

【００３８】

当然、ローカルおよび特定の要件を満たすため、当業者は、上記で説明された解決策に、多くの修正および変更を適用し得るが、それらの修正および変更はすべて、以下の特許請求の範囲により定義される本発明の保護範囲内に含まれる。

【図面の簡単な説明】

【００３９】

【図１】あるユーザが、本発明の方法に従って文書を送付したい別の人物の音声をどのように記録できるかを示す例を例示する。

【図２】声紋を決定し格納するためのシステムの例を例示する。

【図３】本発明に従って、送付される暗号化ファイルに関連付けられた音声チェック・チケットが、送信者のコンピュータから音声チェック・サーバにどのようにアップロードされるかを例示する。

【図４】送信者が、電子メールに、音声チェック・サーバに格納さられた音声チェック・チケットにリンクされた暗号化ファイルを添付する、本発明の特定の例を示す。

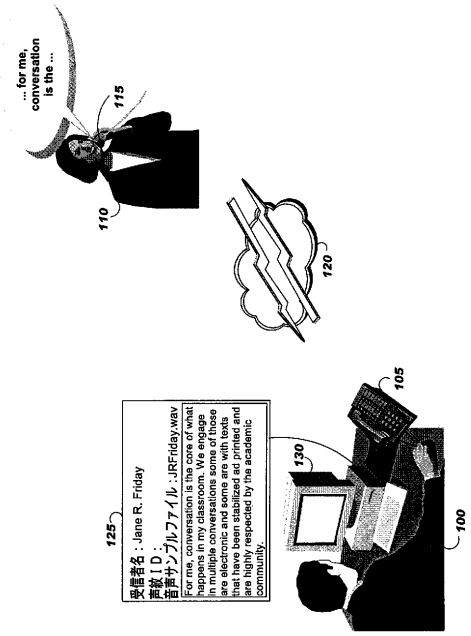
【図５】音声チェック・チケットのアドレスまたはＵＲＬを埋め込む暗号化ファイルを受信者が受信する場合の音声チェック・チケット処理の例を例示する。

【図６】送信される文書を暗号化するための一般的なアルゴリズムの例を例示する。

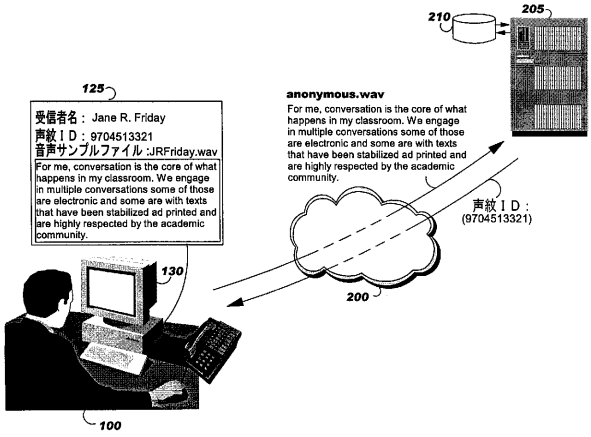
【図７】意図された受信者によるファイルの受信を確認し、受信者の身元を検証し、暗号化鍵を正規の受信者に配信するための、本発明による方法の主ステップを例示する。

【図８】ファイル名中にアドレスを符号化するために用いられるアルゴリズムの例を例示する。

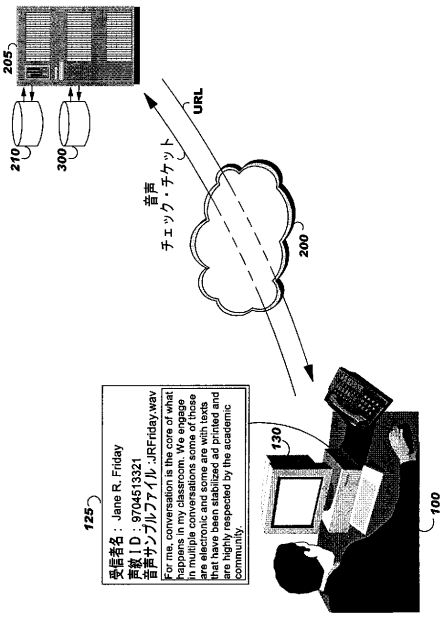
【図１】


... for me, conversation is the ...
115
110
120
105
130
100
125
受信者名：Jane R. Friday
声紋ＩＤ：
音声サンプルファイル：JRFriday.wav
For me, conversation is the core of what happens in my classroom. We engage in multiple conversations some of those are electronic and some are with texts that have been stabilized ad printed and are highly respected by the academic community.

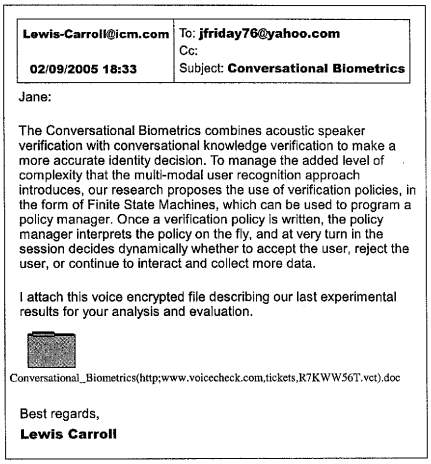
【図２】


210
205
125
受信者名： Jane R. Friday
声紋ＩＤ： 9704513321
音声サンプルファイル：JRFriday.wav
For me, conversation is the core of what happens in my classroom. We engage in multiple conversations some of those are electronic and some are with texts that have been stabilized ad printed and are highly respected by the academic community.
anonymous.wav
For me, conversation is the core of what happens in my classroom. We engage in multiple conversations some of those are electronic and some are with texts that have been stabilized ad printed and are highly respected by the academic community.
声紋ＩＤ：
(9704513321)
130
200
100

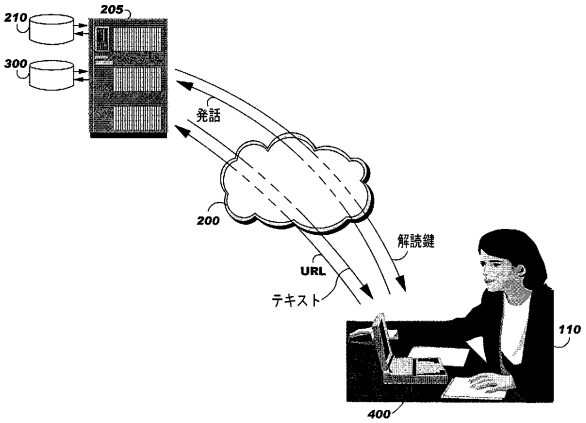
【図３】


205
210
300
URL
音声
チェック・チケット
200
130
100
125
受信者名： Jane R. Friday
声紋ＩＤ： 9704513321
音声サンプルファイル：JRFriday.wav
For me, conversation is the core of what happens in my classroom. We engage in multiple conversations some of those are electronic and some are with texts that have been stabilized ad printed and are highly respected by the academic community.

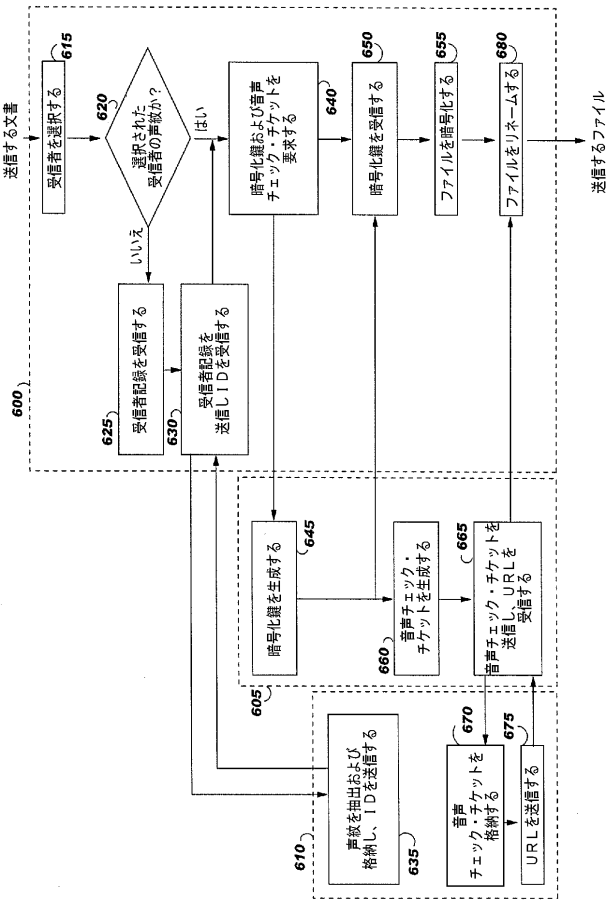
【図４】


Lewis-Carroll@icm.com
02/09/2005 18:33
To: jfriday76@yahoo.com
Cc:
Subject: Conversational Biometrics
Jane:
The Conversational Biometrics combines acoustic speaker verification with conversational knowledge verification to make a more accurate identity decision. To manage the added level of complexity that the multi-modal user recognition approach introduces, our research proposes the use of verification policies, in the form of Finite State Machines, which can be used to program a policy manager. Once a verification policy is written, the policy manager interprets the policy on the fly, and at very turn in the session decides dynamically whether to accept the user, reject the user, or continue to interact and collect more data.
I attach this voice encrypted file describing our last experimental results for your analysis and evaluation.
Conversational_Biometrics(http;www.voicecheck.com,tickets,R7KWW56T.vct).doc
Best regards,
Lewis Carroll

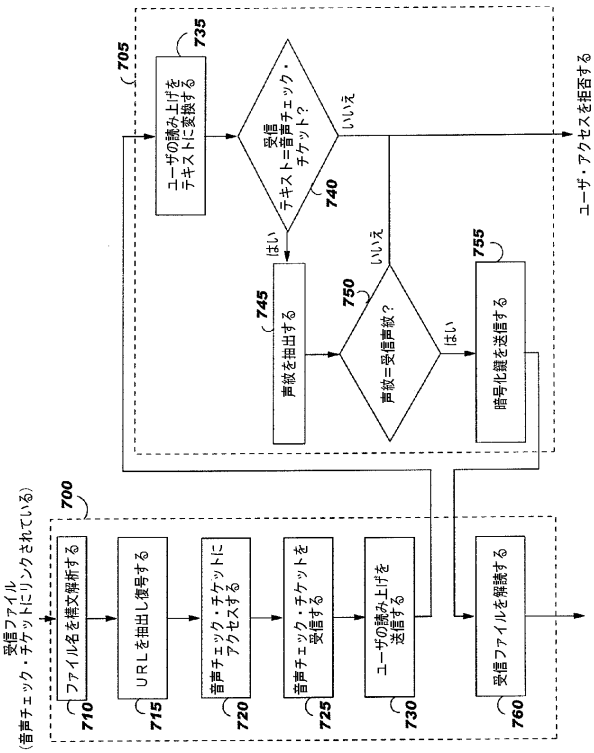
【図５】


210
205
300
発話
200
解読鍵
URL
テキスト
110
400

【図６】


送信する文書
受信者を選択する
615
620
選択された受信者の声紋か？
はい
いいえ
暗号化鍵および音声チェック・チケットを要求する
640
650
暗号化鍵を受信する
655
ファイルを暗号化する
680
ファイルをリネームする
送信するファイル
600
受信者記録を受信する
625
受信者記録を送信ＵＩＤを受信する
630
暗号化鍵を生成する
645
605
音声チェック・チケットを生成する
660
665
音声チェック・チケットを送信 URLを受信する
声紋を抽出および格納し、ＩＤを送信する
635
610
670
音声チェック・チケットを格納する
675
ＵＲＬを送信する

【図７】


受信ファイル
(音声チェック・チケットにリンクされている)
700
ファイルを構文解析する
710
ＵＲＬを抽出し復号する
715
音声チェック・チケットにアクセスする
720
音声チェック・チケットを受信する
725
ユーザの読み上げを送信する
730
受信ファイルを解読する
760
705
ユーザの読み上げをテキストに変換する
735
受信テキスト＝音声チェック・チケット？
740
いいえ
はい
ユーザ・アクセスを拒否する
声紋を抽出する
745
声紋＝受信声紋？
750
いいえ
はい
暗号化鍵を送信する
755

【図８】

a
一次ファイルを得る
800
アドレスを得る
805
アドレスを符号化する
810
一次ファイル名および符号化されたアドレスをマージする
815
ファイルをリネームする
820
b
i = 0
825
addr[i]を抽出する
830
禁止文字か？
835
いいえ
はい
addr[i] = Tab[addr[i]]
840
i++
850
i = max ？
855
いいえ
はい
810
845

フロントページの続き

(74)代理人 100086243
弁理士 坂口 博
(72)発明者 インセルティス カロ、フェルナンド
スペイン イー４６１８２ バレンシア パテルナ モンテーカナダ シー・スラッシュ６１２－ナンバー９

審査官 安田 太

(56)参考文献 特開平１０－２４３１０５（ＪＰ，Ａ）
特開２００１－１４４７４５（ＪＰ，Ａ）
特開２００２－３４２１４５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 13/00