(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2017-531249
(P2017-531249A)
(43)公表日　平成29年10月19日(2017.10.19)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/60	(2013.01)	G06F 21/60		5L096
G06T 7/00	(2017.01)	G06T 7/00	300F	

審査請求 有　予備審査請求 未請求　（全 32 頁）

(21)出願番号　特願2017-511681 (P2017-511681)
(86)(22)出願日　平成27年7月31日 (2015.7.31)
(85)翻訳文提出日　平成29年2月26日 (2017.2.26)
(86)国際出願番号　PCT/US2015/043056
(87)国際公開番号　WO2016/039885
(87)国際公開日　平成28年3月17日 (2016.3.17)
(31)優先権主張番号　14/483,131
(32)優先日　平成26年9月10日 (2014.9.10)
(33)優先権主張国　米国 (US)

(71)出願人　501113353
シマンテック　コーポレーション
Ｓｙｍａｎｔｅｃ　Ｃｏｒｐｏｒａｔｉｏｎ
アメリカ合衆国，カリフォルニア州　９４０４３，マウンテン　ビュー，エリス　ストリート　３５０
(74)代理人　100147485
弁理士　杉村　憲司
(74)代理人　100134119
弁理士　奥町　哲行
(72)発明者　アビアントーン・ラムジー
アメリカ合衆国　カリフォルニア州　９４１０９　サンフランシスコ　ジョーンズストリート　１５３７

最終頁に続く

(54)【発明の名称】データ配信チャネルを介して機密情報を送信する試みを検出するためのシステム及び方法

(57)【要約】
データ配信チャネルを介して機密情報を送信する試みを検出するための、開示されるコンピュータ実装方法は、（１）データ配信チャネルを通してファイルを送信する試みを識別すること、（２）画像マッチング技術を使用して、ファイルと、画像形式で格納されると共にデータ漏えい防止ポリシーによって保護された少なくとも１つの既知の機密ファイルとを比較すること、（３）画像マッチング技術の結果に基づいて、ファイルがデータ漏えい防止ポリシーに違反していると判断すること、及び（４）ファイルがデータ漏えい防止ポリシーに違反しているとの判断に応答して、セキュリティ対策を実施することを含んでもよい。他の様々な方法、システム、及びコンピュータ可読媒体も開示される。

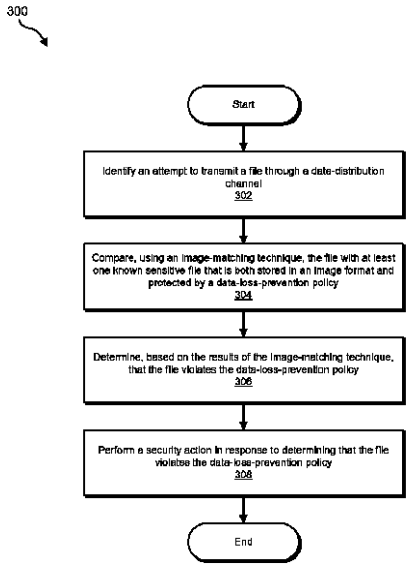


FIG. 3

【特許請求の範囲】
【請求項１】
データ配信チャネルを介して機密情報を送信する試みを検出するためのコンピュータ実装方法であって、前記方法の少なくとも一部分が、少なくとも１つのプロセッサを備えるコンピューティングデバイスによって実施され、前記方法が、
データ配信チャネルを通してファイルを送信する試みを識別することと、
画像マッチング技術を使用して、前記ファイルと、画像形式で格納されると共にデータ漏えい防止ポリシーによって保護された少なくとも１つの既知の機密ファイルとを比較することと、
前記画像マッチング技術の結果に基づいて、前記ファイルが前記データ漏えい防止ポリシーに違反していると判断することと、
前記ファイルが前記データ漏えい防止ポリシーに違反しているとの判断に応答して、セキュリティ対策を実施することと、
を含む、コンピュータ実装方法。
【請求項２】
前記セキュリティ対策が、
前記データ配信チャネルを通して前記ファイルを送信する前記試みをブロックすることと、
前記データ配信チャネルを通して前記ファイルを送信する前記試みを管理者に警告することと、
前記データ配信チャネルを通して前記ファイルを送信する前記試みが前記データ漏えい防止ポリシーに違反していることをユーザに通知することと、
前記データ配信チャネルを通して前記ファイルを送信する前記試みの記録を取ることと、
のうち少なくとも１つを含む、請求項１に記載のコンピュータ実装方法。
【請求項３】
前記画像マッチング技術を使用して、前記ファイルと前記既知の機密ファイルとを比較することが、前記ファイルを前記画像形式に変換することを含む、請求項１に記載のコンピュータ実装方法。
【請求項４】
前記既知の機密ファイルがテキストベースのフォームを含み、前記画像マッチング技術の結果に基づいて、前記ファイルが前記データ漏えい防止ポリシーに違反していると判断することが、前記ファイルが前記テキストベースのフォームの編集バージョンを含むと判断することを含む、請求項１に記載のコンピュータ実装方法。
【請求項５】
前記画像マッチング技術を使用して、前記ファイルと前記既知の機密ファイルとを比較することが、前記既知の機密ファイルと前記ファイルとの間で異なる要素のセットを表す差分画像を作成することを含む、請求項１に記載のコンピュータ実装方法。
【請求項６】
前記画像マッチング技術を使用して、前記ファイルと前記既知の機密ファイルとを比較することが、前記既知の機密ファイル内の主要点のセットと同種である前記ファイル内の主要点のセットを識別することを含む、請求項１に記載の方法。
【請求項７】
前記画像マッチング技術を使用して、前記ファイルと前記既知の機密ファイルとを比較することが、
前記ファイルの単一の視覚要素を前記既知の機密ファイルの単一の視覚要素と比較することと、
前記ファイルの主要特徴間の距離比のセットを前記既知の機密ファイルの主要特徴間の距離比のセットと比較することと、
距離メトリックを使用して、前記ファイルに属する特徴ベクトルのセットを前記既知の

機密ファイルに属する特徴ベクトルのセットと比較することと、
のうち少なくとも１つを含む、請求項１に記載の方法。
【請求項８】
前記画像マッチング技術を使用して、前記ファイルと、前記画像形式で格納されると共に前記データ漏えい防止ポリシーによって保護された前記既知の機密ファイルとを比較することが、
画像形式で格納されると共に前記データ漏えい防止ポリシーによって保護された既知の機密ファイルのギャラリーを識別することと、
粗い画像マッチング技術を使用して、前記ファイルと前記ギャラリー内の複数の既知の機密ファイルとを比較することと、
前記粗い画像マッチング技術よりも多くのコンピューティング資源を消費する、より精細な画像マッチング技術を使用して、前記ファイルと、前記粗い画像マッチング技術によって廃棄されなかった前記ギャラリー内の複数の既知の機密ファイルとを比較することと、
前記より精細な画像マッチング技術よりも多くのコンピューティング資源を消費する最終画像マッチング技術を使用して、前記ファイルと、前記より精細な画像マッチング技術によって廃棄されなかった前記ギャラリー内の複数の既知の機密ファイルとを比較することと、
を含む、請求項１に記載のコンピュータ実装方法。
【請求項９】
前記画像マッチング技術の結果に基づいて、前記ファイルが前記データ漏えい防止ポリシーに違反していると判断することが、前記ファイルが個人識別情報を含むと判断することを含む、請求項１に記載のコンピュータ実装方法。
【請求項１０】
前記コンピューティングデバイスに格納されている追加ファイルを識別することと、
前記画像マッチング技術を使用して、前記追加ファイルと、前記画像形式で格納されると共に前記データ漏えい防止ポリシーによって保護された少なくとも１つの追加の既知の機密ファイルとを比較することと、
前記画像マッチング技術に基づいて、前記追加ファイルが前記データ漏えい防止ポリシーに違反していると判断することと、
前記追加ファイルが前記データ漏えい防止ポリシーに違反しているとの判断に応答して、追加のセキュリティ対策を実施することと、
を更に含む、請求項１に記載のコンピュータ実装方法。
【請求項１１】
データ配信チャネルを介して機密情報を送信する試みを検出するためのシステムであって、前記システムが、
データ配信チャネルを通してファイルを送信する試みを識別する、メモリに格納された、識別モジュールと、
画像マッチング技術を使用して、前記ファイルと、画像形式で格納されると共にデータ漏えい防止ポリシーによって保護された少なくとも１つの既知の機密ファイルとを比較する、メモリに格納された、比較モジュールと、
前記画像マッチング技術の結果に基づいて、前記ファイルが前記データ漏えい防止ポリシーに違反していると判断する、メモリに格納された、判断モジュールと、
前記ファイルが前記データ漏えい防止ポリシーに違反しているとの判断に応答してセキュリティ対策を実施する、メモリに格納された、セキュリティモジュールと、
前記識別モジュール、前記比較モジュール、前記判断モジュール、及び前記セキュリティモジュールを実行するように構成された、少なくとも１つの物理的プロセッサと、
を備える、システム。
【請求項１２】
前記セキュリティ対策が、

前記データ配信チャネルを通して前記ファイルを送信する前記試みをブロックすることと、
前記データ配信チャネルを通して前記ファイルを送信する前記試みを管理者に警告することと、
前記データ配信チャネルを通して前記ファイルを送信する前記試みが前記データ漏えい防止ポリシーに違反していることをユーザに通知することと、
前記データ配信チャネルを通して前記ファイルを送信する前記試みの記録を取ることと、
のうち少なくとも１つを含む、請求項１１に記載のシステム。
【請求項１３】
前記比較モジュールが、前記画像マッチング技術を使用して、前記ファイルを前記画像形式に変換することによって、前記ファイルと前記既知の機密ファイルとを比較する、請求項１１に記載のシステム。
【請求項１４】
前記既知の機密ファイルがテキストベースのフォームを含み、前記判断モジュールが、前記画像マッチング技術の結果に基づいて、前記ファイルが前記テキストベースのフォームの編集バージョンを含むと判断することによって、前記ファイルが前記データ漏えい防止ポリシーに違反していると判断する、請求項１１に記載のシステム。
【請求項１５】
前記比較モジュールが、前記画像マッチング技術を使用して、前記既知の機密ファイルと前記ファイルとの間で異なる要素のセットを表す差分画像を作成することによって、前記ファイルと前記既知の機密ファイルとを比較する、請求項１１に記載のシステム。
【請求項１６】
前記比較モジュールが、前記画像マッチング技術を使用して、前記既知の機密ファイル内の主要点のセットと同種である前記ファイル内の主要点のセットを識別することによって、前記ファイルと前記既知の機密ファイルとを比較する、請求項１１に記載のシステム。
【請求項１７】
前記比較モジュールが、前記画像マッチング技術を使用して、
前記ファイルの単一の視覚要素を前記既知の機密ファイルの単一の視覚要素と比較することと、
前記ファイルの主要特徴間の距離比のセットを前記既知の機密ファイルの主要特徴間の距離比のセットと比較することと、
距離メトリックを使用して、前記ファイルに属する特徴ベクトルのセットを前記既知の機密ファイルに属する特徴ベクトルのセットと比較することと、
のうち少なくとも１つによって前記ファイルと前記既知の機密ファイルとを比較する、請求項１１に記載のシステム。
【請求項１８】
前記比較モジュールが、前記画像マッチング技術を使用して、
画像形式で格納されると共に前記データ漏えい防止ポリシーによって保護された既知の機密ファイルのギャラリーを識別することと、
粗い画像マッチング技術を使用して、前記ファイルと前記ギャラリー内の複数の既知の機密ファイルとを比較することと、
前記粗い画像マッチング技術よりも多くのコンピューティング資源を消費する、より精細な画像マッチング技術を使用して、前記ファイルと、前記粗い画像マッチング技術によって廃棄されなかった前記ギャラリー内の複数の既知の機密ファイルとを比較することと、
前記より精細な画像マッチング技術よりも多くのコンピューティング資源を消費する最終画像マッチング技術を使用して、前記ファイルと、前記より精細な画像マッチング技術によって廃棄されなかった前記ギャラリー内の複数の既知の機密ファイルとを比較するこ

とと、
によって、前記ファイルと、前記画像形式で格納されると共に前記データ漏えい防止ポリシーによって保護された前記既知の機密ファイルとを比較する、請求項１１に記載のシステム。
【請求項１９】
前記判断モジュールが、前記画像マッチング技術の結果に基づいて、前記ファイルが個人識別情報を含むと判断することによって、前記ファイルが前記データ漏えい防止ポリシーに違反していると判断する、請求項１１に記載のシステム。
【請求項２０】
１つ以上のコンピュータ可読命令を含む非一時的コンピュータ可読媒体であって、コンピューティングデバイスの少なくとも１つのプロセッサによって実行されると、前記コンピューティングデバイスに、
データ配信チャネルを通してファイルを送信する試みを識別させ、
画像マッチング技術を使用して、前記ファイルと、画像形式で格納されると共にデータ漏えい防止ポリシーによって保護された少なくとも１つの既知の機密ファイルとを比較させ、
前記画像マッチング技術の結果に基づいて、前記ファイルが前記データ漏えい防止ポリシーに違反していると判断させ、
前記ファイルが前記データ漏えい防止ポリシーに違反しているとの判断に応答して、セキュリティ対策を実施させる、
非一時的コンピュータ可読媒体。
【発明の詳細な説明】
【背景技術】
【０００１】
企業のネットワーク及びファイリングキャビネットは、多くの場合、秘密電子メール、企業の非公開文書、従業員記録、個人識別情報、納税申告用紙、財務情報などの形態の、機密データで満たされている。この機密データは、数十又は更には数百のサーバ、パーソナルコンピュータ、及び／又はハードコピーにわたって散在していることがある。このデータが安全に保たれていることを保証することは、企業の評判及びその成功の両方にとって非常に重要となる場合がある。企業は、機密データが適正に扱われることを保証するデータ漏えい防止（ＤＬＰ）ポリシーを有することがあるが、データを電子メールから可搬型記憶デバイスへ、ファックスへ、ファイル共有へと送信する無数の方法があることにより、ＤＬＰポリシーの実施は以前にも増して困難になっている。
【発明の概要】
【発明が解決しようとする課題】
【０００２】
従来のＤＬＰシステムは、一般的に、光学文字読み取り技術（ＯＣＲ）を使用して、発信するハードコピー文書を検査して、それらの内容がＤＬＰポリシーによって保護されているかを判断する。残念ながら、ＯＣＲ技術は、資源集約的かつ不正確である場合が多い。したがって、本開示は、データ配信チャネルを介して機密情報を送信する試みを検出するための、追加の改善されたシステム及び方法に対する必要性を特定し、それに対処する。
【課題を解決するための手段】
【０００３】
更に詳細に後述するように、本開示は、全ての文書を画像として取り扱い、次に画像処理技術を使用して、ＤＬＰポリシーによって保護された画像のギャラリーと比較するための特徴を抽出することによって、データ配信チャネルを介して機密情報を送信する試みを検出する様々なシステム及び方法について記載する。
【０００４】
一実施例では、データ配信チャネルを介して機密情報を送信する試みを検出するための

コンピュータ実装方法は、（１）データ配信チャネルを通してファイルを送信する試みを識別すること、（２）画像マッチング技術を使用して、ファイルと、画像形式で格納されると共にＤＬＰポリシーによって保護された少なくとも１つの既知の機密ファイルとを比較すること、（３）画像マッチング技術の結果に基づいて、ファイルがＤＬＰポリシーに違反していると判断すること、及び（４）ファイルがＤＬＰポリシーに違反しているとの判断に応答してセキュリティ対策を実施することを含んでもよい。

【０００５】

いくつかの実施形態では、セキュリティ対策は、（１）データ配信チャネルを通してファイルを送信する試みをブロックすること、（２）データ配信チャネルを通してファイルを送信する試みを管理者に警告すること、（３）データ配信チャネルを通してファイルを送信する試みがＤＬＰポリシーに違反していることをユーザに通知すること、及び／又は（４）データ配信チャネルを通してファイルを送信する試みの記録を取ることを含んでもよい。

【０００６】

ファイルは、様々な方法で既知の機密ファイルと比較されてもよい。一実施形態では、ファイルと既知の機密ファイルとの比較は、ファイルを画像形式に変換することを含んでもよい。いくつかの実施例では、ファイルと既知の機密ファイルとの比較は、既知の機密ファイルとファイルとの間で異なる要素のセットを表す差分画像を作成することを含んでもよい。

【０００７】

それに加えて、又は別の方法として、ファイルと既知の機密ファイルとの比較（画像ドメイン内）は、既知の機密ファイル内の主要点のセットと同種であるファイル内の主要点のセットを識別することを含んでもよい。それに加えて、ファイルと既知の機密ファイルとの比較は、（１）ファイルの単一の視覚要素を既知の機密ファイルの単一の視覚要素と比較すること、（２）ファイルの主要特徴間の距離比のセットを既知の機密ファイルの主要特徴間の距離比のセットと比較すること、及び／又は（３）距離メトリックを使用して、ファイルに属する特徴ベクトルのセットを既知の機密ファイルに属する特徴ベクトルのセットと比較することを含んでもよい。

【０００８】

いくつかの実施例では、画像比較はいくつかのステップを伴ってもよい。一実施形態では、ファイルと既知の機密との比較は、（１）画像形式で格納されると共にデータ漏えい防止ポリシーによって保護された既知の機密ファイルのギャラリーを識別すること、（２）粗い画像マッチング技術を使用して、ファイルとギャラリー内の複数の既知の機密ファイルとを比較すること、（３）粗い画像マッチング技術よりも多くのコンピューティング資源を消費する、より精細な画像マッチング技術を使用して、ファイルと、粗い画像マッチング技術によって廃棄されなかったギャラリー内の複数の既知の機密ファイルとを比較すること、及び（４）より精細な画像マッチング技術よりも多くのコンピューティング資源を消費する最終画像マッチング技術を使用して、ファイルと、より精細な画像マッチング技術によって廃棄されなかったギャラリー内の複数の既知の機密ファイルとを比較することを含んでもよい。

【０００９】

一実施形態では、画像マッチング技術の結果に基づいて、ファイルがＤＬＰポリシーに違反していると判断することは、ファイルが個人識別情報を含むと判断することを含んでもよい。例えば、既知の機密ファイルはテキストベースのフォームを含んでもよく、ファイルがＤＬＰポリシーに違反していると判断することは、ファイルが、個人識別情報を含む、テキストベースのフォームの編集バージョンを含むと判断することを含んでもよい。

【００１０】

いくつかの実施例では、コンピュータ実装方法は保存データに適用されてもよい。例えば、コンピュータ実装方法は、（１）コンピューティングデバイスに格納されている追加ファイルを識別すること、（２）画像マッチング技術を使用して、追加ファイルと、画像

形式で格納されると共にＤＬＰポリシーによって保護された少なくとも１つの追加の既知の機密ファイルとを比較すること、（３）画像マッチング技術に基づいて、追加ファイルがＤＬＰポリシーに違反していると判断すること、及び（４）追加ファイルがＤＬＰポリシーに違反しているとの判断に応答して、追加のセキュリティ対策を実施することを更に含んでもよい。

【００１１】

一実施形態では、上述の方法を実装するシステムは、（１）データ配信チャネルを通してファイルを送信する試みを識別する、メモリに格納された、識別モジュール、（２）画像マッチング技術を使用して、ファイルと、画像形式で格納されると共にＤＬＰポリシーによって保護された少なくとも１つの既知の機密ファイルとを比較する、メモリに格納された、比較モジュール、（３）画像マッチング技術の結果に基づいて、ファイルがＤＬＰポリシーに違反していると判断する、メモリに格納された、判断モジュール、（４）ファイルがＤＬＰポリシーに違反しているとの判断に応答してセキュリティ対策を実施する、メモリに格納された、セキュリティモジュール、並びに（５）識別モジュール、比較モジュール、判断モジュール、及びセキュリティモジュールを実行するように構成された、少なくとも１つの物理的プロセッサを含んでもよい。

【００１２】

いくつかの実施例では、上述の方法は、非一時的コンピュータ可読媒体上のコンピュータ可読命令としてコード化されてもよい。例えば、コンピュータ可読媒体は、コンピューティングデバイスの少なくとも１つのプロセッサによって実行されると、（１）データ配信チャネルを通してファイルを送信する試みを識別すること、（２）画像マッチング技術を使用して、ファイルと、画像形式で格納されると共にＤＬＰポリシーによって保護された少なくとも１つの既知の機密ファイルとを比較すること、（３）画像マッチング技術の結果に基づいて、ファイルがＤＬＰポリシーに違反していると判断すること、及び（４）ファイルがＤＬＰポリシーに違反しているとの判断に応答して、セキュリティ対策を実施することを、コンピューティングデバイスに行わせる、１つ以上のコンピュータ実行可能命令を含んでもよい。

【００１３】

上述の実施形態のいずれかによる特徴が、本明細書に記載する一般原理にしたがって、互いに組み合わせて使用されてもよい。これら及び他の実施形態、特徴、及び利点は、以下の発明を実施するための形態を、添付の図面及び特許請求の範囲と併せ読むことによって、更に十分に理解されるだろう。

【図面の簡単な説明】

【００１４】

添付図面は、いくつかの例示的な実施形態を図示するものであり、本明細書の一部である。以下の説明と併せて、これらの図面は本開示の様々な原理を実証し説明する。

【図１】データ配信チャネルを介して機密情報を送信する試みを検出するための例示的なシステムを示すブロック図である。

【図２】データ配信チャネルを介して機密情報を送信する試みを検出するための追加の例示的なシステムを示すブロック図である。

【図３】データ配信チャネルを介して機密情報を送信する試みを検出するための例示的な方法を示すフローチャートである。

【図４】データ配信チャネルを介して機密情報を送信する試みを検出するための例示的なシステムを示すブロック図である。

【図５】データ配信チャネルを介して機密情報を送信する試みを検出するための例示的な方法を示すフローチャートである。

【図６】データ配信チャネルを介して機密情報を送信する試みを検出するための例示的なコンピューティングシステムの例示的な出力を示すブロック図である。

【図７】本明細書に記載及び／又は図示される実施形態のうち１つ以上を実装することができる例示的なコンピューティングシステムを示すブロック図である。

【図８】本明細書に記載及び／又は図示される実施形態のうち１つ以上を実装することができる例示的なコンピューティングネットワークを示すブロック図である。

【００１５】

図面を通して、同一の参照符号及び記述は、必ずしも同一ではないが類似している要素を示す。本明細書に記載される例示的な実施形態は、様々な修正物及び代替的な形態が可能であるが、特定の実施形態が例として図面に示されており、本明細書に詳細に記載される。しかしながら、本明細書に記載される例示的な実施形態は、開示される特定の形態に限定されることを意図しない。むしろ、本開示は、添付の特許請求の範囲内にある全ての修正物、等価物、及び代替物を網羅する。

【発明を実施するための形態】

【００１６】

本開示は、一般に、データ配信チャネルを介して機密情報を送信する試みを検出するためのシステム及び方法に向けられている。より詳細に後述されるように、全ての文書を画像として取り扱うことによって、本明細書に記載されるシステムは、ＯＣＲに固有の問題を回避しながら、文書を効率的に比較することができる。文書が機密文書のバージョンであることが見出された場合、本明細書に記載されるシステムは、ＤＬＰポリシー違反を識別するため、及び／又はかかる違反をより容易に調査可能にするために、文書のバージョン間における変更の検出、位置決め、及び／又は強調表示を行ってもよい。

【００１７】

以下に、図１、図２、及び図４を参照して、データ配信チャネルを介して機密情報を送信する試みを検出するための、例示的なシステムを詳細に説明する。対応するコンピュータ実装方法の詳細な説明もまた、図３、図５、及び図６に関連して提供される。それに加えて、本明細書に記載される実施形態のうち１つ以上を実装することができる、例示的なコンピューティングシステム及びネットワークアーキテクチャの詳細な説明が、それぞれ図７及び図８に関連して提供される。

【００１８】

図１は、データ配信チャネルを介して機密情報を送信する試みを検出するための、例示的なシステム１００のブロック図である。この図に図示されるように、例示的なシステム１００は、１つ以上のタスクを実施するための１つ以上のモジュール１０２を含んでもよい。例えば、より詳細に後述するように、例示的なシステム１００は、データ配信チャネルを通してファイルを送信する試みを識別してもよい、識別モジュール１０４を含んでもよい。例示的なシステム１００は、それに加えて、画像マッチング技術を使用して、ファイルと、画像形式で格納されると共にデータ漏えい防止ポリシーによって保護されてもよい少なくとも１つの既知の機密ファイル１２２とを比較してもよい、比較モジュール１０６を含んでもよい。例示的なシステム１００はまた、画像マッチング技術の結果に基づいて、ファイルがデータ漏えい防止ポリシーに違反していると判断してもよい、判断モジュール１０８を含んでもよい。例示的なシステム１００は、それに加えて、ファイルがデータ漏えい防止ポリシーに違反しているとの判断に応答してセキュリティ対策を実施してもよい、セキュリティモジュール１１０を含んでもよい。別々の要素として図示されるが、図１のモジュール１０２のうち１つ以上が、単一のモジュール又はアプリケーションの部分を表してもよい。

【００１９】

特定の実施形態では、図１のモジュール１０２のうち１つ以上は、コンピューティングデバイスによって実行されると、１つ以上のタスクをコンピューティングデバイスに実施させてもよい、１つ以上のソフトウェアアプリケーション又はプログラムを表してもよい。例えば、より詳細に後述するように、モジュール１０２のうち１つ以上は、図２に図示されるデバイス（例えば、コンピューティングデバイス２０２及び／又はサーバ２０６）、図７のコンピューティングシステム７１０、並びに／あるいは図８の例示的なネットワークアーキテクチャ８００の部分など、１つ以上のコンピューティングデバイスに格納され、その上で動くように構成された、ソフトウェアモジュールを表してもよい。図１のモ

ジュール１０２のうち１つ以上は、１つ以上のタスクを実施するように構成された１つ以上の専用コンピュータの全て又は一部も表してもよい。

【００２０】

図１に図示されるように、例示的なシステム１００はまた、データベース１２０などの１つ以上のデータベースを含んでもよい。一実施例では、データベース１２０は、機密ファイル１２２を格納するように構成されてもよい。データベース１２０は、単一のデータベース若しくはコンピューティングデバイスの部分、又は複数のデータベース若しくはコンピューティングデバイスの部分を表してもよい。例えば、データベース１２０は、図２のサーバ２０６の一部分、図７のコンピューティングシステム７１０、及び／又は図８の例示的なネットワークアーキテクチャ８００の部分を表してもよい。別の方法として、図１のデータベース１２０は、図２のサーバ２０６、図７のコンピューティングシステム７１０、及び／又は図８の例示的なネットワークアーキテクチャ８００の部分など、コンピューティングデバイスによってアクセスすることができる、１つ以上の物理的に別個のデバイスを表してもよい。

【００２１】

図１の例示的なシステム１００は様々な方法で実装されてもよい。例えば、例示的なシステム１００の全て又は一部は、図２における例示的なシステム２００の部分を表してもよい。図２に示されるように、システム２００は、ネットワーク２０４を介してサーバ２０６と通信するコンピューティングデバイス２０２を含んでもよい。一実施例では、コンピューティングデバイス２０２は、モジュール１０２のうち１つ以上を用いてプログラムされてもよく、かつ／又はデータベース１２０内のデータの全て若しくは一部を格納してもよい。それに加えて、又は別の方法として、サーバ２０６は、モジュール１０２のうち１つ以上を用いてプログラムされてもよく、かつ／又はデータベース１２０内のデータの全て若しくは一部を格納してもよい。

【００２２】

一実施形態では、図１のモジュール１０２のうち１つ以上により、コンピューティングデバイス２０２及び／又はサーバ２０６の少なくとも１つによって実行されると、データ配信チャネルを介して機密ファイルを送信する試みを、コンピューティングデバイス２０２及び／又はサーバ２０６が検出することが可能になってもよい。例えば、より詳細に後述するように、識別モジュール１０４は、データ配信チャネル２０９を通してファイル２０８を送信する試みを識別してもよい。比較モジュール１０６は、次に、画像マッチング技術を使用して、ファイル２０８と、画像形式で格納されると共にＤＬＰポリシー２１２によって保護された少なくとも１つの既知の機密ファイル１２２とを比較してもよい。判断モジュール１０８は、次に、一致結果２１４に基づいて、ファイル２０８がＤＬＰポリシー２１２に違反していると判断してもよい。最後に、セキュリティモジュール１１０は、ファイル２０８がＤＬＰポリシー２１２に違反しているとの判断に応答して、セキュリティ対策２１６を実行してもよい。

【００２３】

コンピューティングデバイス２０２は、一般に、コンピュータ実行可能命令を読み取ることができる任意のタイプ又は形態のコンピューティングデバイスを表す。コンピューティングデバイス２０２の例としては、非限定的に、ラップトップ、タブレット、デスクトップ、サーバ、携帯電話、携帯情報端末（ＰＤＡ）、マルチメディアプレーヤー、埋め込みシステム、ウェアラブルデバイス（例えば、スマートウォッチ、スマートグラスなど）、ゲームコンソール、それらの１つ以上の組み合わせ、図７の例示的なコンピューティングシステム７１０、あるいは他の任意の好適なコンピューティングデバイスが挙げられる。

【００２４】

サーバ２０６は、一般に、画像のギャラリーを格納することができる任意のタイプ又は形態のコンピューティングデバイスを表す。サーバ２０６の例としては、非限定的に、様々なデータベースサービスを提供するように、かつ／又は特定のソフトウェアアプリケー

ションを実行するように構成された、アプリケーションサーバ及びデータベースサーバが挙げられる。

【００２５】

ネットワーク２０４は、一般に、通信若しくはデータ転送を容易にすることができる、任意の媒体又はアーキテクチャを表す。ネットワーク２０４の例としては、非限定的に、イントラネット、広域ネットワーク（Wide Area Network）（ＷＡＮ）、ローカルエリアネットワーク（Local Area Network）（ＬＡＮ）、パーソナルエリアネットワーク（Personal Area Network）（ＰＡＮ）、インターネット、電力線通信（ＰＬＣ）、セルラーネットワーク（例えば、Global System for Mobile Communications（ＧＳＭ（登録商標））ネットワーク）、図８の例示的なネットワークアーキテクチャ８００などが挙げられる。ネットワーク２０４は、無線若しくは有線接続を使用して通信又はデータ転送を容易にしてもよい。一実施形態では、ネットワーク２０４は、コンピューティングデバイス２０２とサーバ２０６との間の通信を容易にしてもよい。

【００２６】

図３は、データ配信チャネルを介して機密情報を送信する試みを検出するための、例示的なコンピュータ実装方法３００のフローチャートである。図３に示されるステップは、任意の好適なコンピュータ実行可能コード及び／又はコンピューティングシステムによって実施されてもよい。いくつかの実施形態では、図３に示されるステップは、図１のシステム１００、図２のシステム２００、図７のコンピューティングシステム７１０、及び／又は図８の例示的なネットワークアーキテクチャ８００の部分の構成要素のうち１つ以上によって実施されてもよい。

【００２７】

図３に図示されるように、ステップ３０２で、本明細書に記載されるシステムのうち１つ以上が、データ配信チャネルを通してファイルを送信する試みを識別してもよい。例えば、識別モジュール１０４は、図２のサーバ２０６の一部として、データ配信チャネル２０９を通してファイル２０８を送信する試みを識別してもよい。

【００２８】

「データ配信チャネル」という用語は、本明細書で使用するとき、一般に、あるエンティティから別のエンティティにデジタル情報を分散させることができる、任意のタイプ若しくは形態の通信経路、コンピューティングシステム、及び／又は実行可能コードを指す。データ配信チャネルの例としては、非限定的に、コンピューティングデバイス、移動通信デバイス、電子メールアカウント、テキストメッセージ通信サービス、ソーシャルネットワーキングプラットフォーム、インターネット及びイーサネット（登録商標、以下同じ）ネットワーク、サーバ、取外し可能な記憶デバイス、データ転送ケーブル、並びに／あるいは他の任意の好適な通信チャネルが挙げられる。

【００２９】

識別モジュール１０４は、様々な方法及び／又はコンテキストで、ファイルを送信する試みを識別してもよい。例えば、識別モジュール１０４は、エンドポイントデバイスにインストールされてもよく、ユニバーサルシリアルバス（ＵＳＢ）ポート、ネットワーク接続、ファイル転送プロトコルクライアント、及び／又は電子メールクライアントなど、エンドポイントデバイスのデータ配信チャネルを監視してもよい。別の実施例では、識別モジュール１０４は、ネットワークゲートウェイにインストールされてもよく、ネットワークトラフィックを監視してもよい。例えば、識別モジュール１０４は、ファックス機器を監視して、発信するファックスを介して機密情報を送信する試みを識別してもよい。いくつかの実施形態では、識別モジュール１０４は、安全な環境外の宛先にファイルを送信する試みのみを識別してもよい。他の実施形態では、識別モジュール１０４は、データ配信チャネルを介してファイルを送信するあらゆる試みを識別してもよい。

【００３０】

いくつかの実施形態では、識別モジュール１０４は、ファイルを送信する試みを識別すると（また、ステップ３０４の実施に先立って）、更なる解析が保証されるか否かを判断

するために、予備的解析を実施してもよい。一実施形態では、この予備的解析は、ファイルの色ヒストグラムを解析することを伴ってもよい。例えば、識別モジュール１０４は、ファイルの色ヒストグラムを解析することによって、ファイルが明るい色の画像（例えば、休暇中の写真）であり、したがって機密情報を含む白黒フォームに一致する可能性は低いと判断してもよい。この実施例では、識別モジュール１０４は、ファイルを送信する試みを可能にしてもよく、かつ／又は更なる解析のために比較モジュール１０６にファイルを伝えるのを控えてもよい。この初期解析を実施することによって、識別モジュール１０４は、一部の画像がＤＬＰポリシーに属していないことがあることを迅速に判断してもよく、それにより、別の方法では画像をより徹底的に解析するのに必要であろう、追加資源を節約してもよい。

【００３１】

ステップ３０４で、本明細書に記載されるシステムのうち１つ以上は、画像マッチング技術を使用して、ファイルと、画像形式で格納されると共にＤＬＰポリシーによって保護された少なくとも１つの既知の機密ファイルとを比較してもよい。例えば、比較モジュール１０６は、図２のサーバ２０６の一部として、画像マッチング技術を使用して、ファイル２０８と、画像形式で格納されると共にＤＬＰポリシー２１２によって保護された少なくとも１つの既知の機密ファイル１２２とを比較してもよい。

【００３２】

「画像マッチング技術」という用語は、本明細書で使用するとき、一般に、ある画像が別の画像に類似しているか否かを判断するのに使用される、任意の方法又は方法の組み合わせを指す。画像マッチング技術は、大域的及び局所的の両方の画像処理並びに／又はコンピュータビジョン技術を含んでもよい。大域的技術は画像全体を解析し、一方局所的技術は画像中の関心点のセットに焦点を当てる。いくつかの実施例では、局所的画像マッチング技術は、スケール不変性特徴変換（scale-invariant feature transform）（ＳＩＦＴ）技術、高速堅牢特徴（speeded-up robust features）（ＳＵＲＦ）技術、並びに／あるいは有向ＦＡＳＴ及び回転ＢＲＩＥＦ（oriented fast and rotated brief）（ＯＲＢ）技術など、自動又は手動で決定される主要点の周りの記述子と呼ばれる特徴ベクトルを画像から抽出する技術を含んでもよい。これらの記述子は、一般的に、スケール、照明、回転、及び視点の変化に関してある程度の不変性を提供する。大域的画像マッチング技術の例としては、ヒストグラムマッチング、相関フィルタ、主成分分析（ＰＣＡ）、線形判別分析（ＬＤＡ）などが挙げられるがそれらに限定されない。

【００３３】

「画像形式」という用語は、本明細書で使用するとき、一般に、画素の二次元アレイとして描画されてもよい、任意のデータ記憶形式を指す。いくつかの実施形態では、画像形式は、各画素を記述するデータ、及び／又は画像の幾何学的記述を含むデータを含んでもよい。いくつかの実施例では、画像形式で格納されたファイルは、形態及び／又は他のオブジェクトの絵であってもよい。画像形式の例としては、非限定的に、ラスタ画像形式、ビットマップ画像形式、グラフィックス交換形式、ポータブルネットワークグラフィックス、ベクトル画像形式、複合画像形式、及び／又は立体画像形式が挙げられる。

【００３４】

「機密ファイル」という用語は、本明細書で使用するとき、一般に、ＤＬＰポリシーによって保護されてもよい任意のファイルを指す。それに加えて、「データ漏えい防止ポリシー」又は「ＤＬＰポリシー」は、本明細書で使用するとき、一般に、潜在的なデータ漏えいを検出及び／又は防止するように設計された、任意のポリシー及び／又はシステムを指す。ＤＬＰシステムは、使用中、活動中、及び／又は保存中であってもよいデータに作用してもよい。ＤＬＰシステムは、データの格納及び／又は送信に関するポリシー、ＤＬＰポリシーを実施するように構成されたソフトウェア、ＤＬＰポリシーの物理的実施、並びに／あるいはデータの送信を防止してもよいハードウェア修正物を含んでもよい。ＤＬＰポリシーの例としては、非限定的に、「企業の非公開データは移動可能な記憶媒体にコピーできない」、「個人識別情報は電子メール送信できない」、及び／又は「納税申告用

紙はファックス送信できない」を挙げることができる。同様に、ＤＬＰ実施の例としては、非限定的に、可搬型記憶媒体への書込み要求を防止すること、発信する電子メールをフィルタ処理して機密データを検出すること、デバイスが安全でないネットワーク上にある状態で機密データにアクセスするのを防止すること、及び／又は機密データを含むファックスをブロックすることを挙げることができる。

【００３５】

比較モジュール１０６は、様々な手段及び／又はコンテキストでファイルを比較してもよい。例えば、比較モジュール１０６は、様々な方法を使用してファイルが機密情報を含むか否かを判断してもよい、ＤＬＰポリシー実施アプリケーションの一部であってもよい。他の実施形態では、比較モジュール１０６は、汎用画像比較アプリケーションの一部であってもよい。

【００３６】

いくつかの実施例では、比較モジュール１０６は、ファイルを画像形式に変換することによって、ファイルを既知の機密ファイルと比較してもよい。例えば、ファイルは画像形式でないことがあり、したがって、画像形式で格納されている機密ファイルと比較される前に変換が必要なことがある。具体的には、ファイルは、ファックス、ポータブルドキュメントフォーマットファイル、テキストファイル、及び／又は．ＤＯＣファイルの形態であることがある。そのため、比較モジュール１０６は、続行する前に所与の解像度にすることによって、非画像ファイルを画像形式に変換してもよい。例えば、比較モジュール１０６は、ファイル２０８を、画像形式で格納された既知の機密ファイルのギャラリーと比較する試みの前に、（例えば、様々な変換技術の１つ以上を使用して）テキストファイルからビットマップファイルに変換してもよい。

【００３７】

いくつかの実施形態では、比較モジュール１０６は、画像マッチング技術を使用して、既知の機密ファイル内の主要点のセットと同種であるファイル内の主要点のセットを識別してもよい。例えば、比較モジュール１０６は、画像マッチング技術を使用して、ファイル２０８を、採用した画像マッチング技術に関連する距離メトリックを用いて機密ファイル１２２と比較してもよい。１つを超える機密ファイル１２２がデータベースに存在する場合、比較モジュール１０６は、ファイル２０８とデータベース内のファイルそれぞれとの間の類似性を測定して、１つ以上のファイルが一致を生成するかを判断してもよい。

【００３８】

例えば、回転、スケーリング、照明、及び視点の変化に耐性がある（例えば自動的に若しくは管理者によって識別される、全ての主要点に対する）画像記述子を生成する、上述したような局所的画像マッチング技術を使用して、比較モジュール１０６は、ファイル２０８に属する記述子と機密ファイル１２２に属する記述子との間の距離を測定してもよい。記述子が浮動値のベクトルからなる場合、Ｌ２又はＬ１の距離メトリックが使用されてもよい。記述子がブール値のベクトルからなる場合、Ｌ０又はハミング距離が、類似性を測定するのに使用されてもよい。他の任意の好適な距離メトリックもまた使用されてもよい。

【００３９】

それに加えて、比較モジュール１０６は、マッチング記述子のセットの空間的分布に基づいて、ファイル２０８を既知の機密ファイルのギャラリー中の最もマッチングがよい機密ファイルに対してマッピングする、幾何学的変換を評価してもよい。このマッピングは、誤整列を補正するホモグラフィ及び／又は投影変換を含んでもよい。

【００４０】

他の実施形態では、比較モジュール１０６は、画像マッチング技術を使用して、（１）ファイルの単一の視覚要素を既知の機密ファイルの単一の視覚要素と比較すること、（２）ファイルの主要特徴間の距離比のセットを既知の機密ファイルの主要特徴間の距離比のセットと比較すること、及び／又は（３）適切な距離メトリックを使用して、ファイルに属する特徴ベクトルのセットを既知の機密ファイルに属する特徴ベクトルのセットと比較

することの少なくとも１つによって、ファイルを既知の機密ファイルと比較してもよい。

【００４１】

例えば、比較モジュール１０６は、機密ファイル１２２の重要な視覚要素を識別し、その重要な視覚要素の存在に関してファイル２０８を検査してもよい。視覚要素の例としては、非限定的に、単色の領域、直線、又は幾何学形状（例えば、円、正方形、三角形、若しくは他の任意の適切な形状）が挙げられる。それに加えて、比較モジュール１０６は、機密ファイル１２２の特定の領域内の線を位置決めし、ファイル２０８内で類似の長さを有すると共に類似の位置にある線を位置決めしてもよい。この比較に基づいて、比較モジュール１０６は、そのファイル２０８が機密ファイル１２２と一致すると判断してもよい。

【００４２】

比較モジュール１０６は、それに加えて、又は別の方法として、ファイル２０８内に含まれる主要点のセットを識別し、それらの間の距離の比を計算してもよい。機密ファイル１２２がファイル２０８内のものに類似した距離比を有する主要点を含む場合、比較モジュール１０６は、ファイル２０８が機密ファイル１２２に類似していると判断してもよい。

【００４３】

いくつかの実施形態では、比較モジュール１０６は、画像マッチング技術を使用して、（１）画像形式で格納されると共にデータ漏えい防止ポリシーによって保護された、既知の機密ファイルのギャラリーを識別すること、（２）粗い画像マッチング技術を使用して、ファイルとギャラリー内の複数の既知の機密ファイルとを比較すること、（３）粗い画像マッチング技術よりも多くのコンピューティング資源を消費する、より精細な画像マッチング技術を使用して、ファイルと、粗い画像マッチング技術によって廃棄されなかったギャラリー内の複数の既知の機密ファイルとを比較すること、及び（４）より精細な画像マッチング技術よりも多くのコンピューティング資源を消費する最終画像マッチング技術を使用して、ファイルと、より精細な画像マッチング技術によって廃棄されなかったギャラリー内の複数の既知の機密ファイルとを比較することによって、ファイルと、画像形式で格納されると共にデータ漏えい防止ポリシーによって保護された既知の機密ファイルとを比較してもよい。上述のカスケードアーキテクチャは、特に機密ファイルのデータベースが大きい場合に、機密ファイル１２２の識別を大幅に高速化するように設計されてもよい。カスケードアーキテクチャは、最も粗いものから最も精細なものまで複雑性及びマッチング力の増加によってソートされた一連のサブマッチャーからなってもよく、２つの主な利点を提供する。第一に、カスケードアーキテクチャによって、比較モジュール１０６が、資源を消費しすぎることなく簡単な不一致を漸次的に排除し、より精細な一致及びより多くの資源を消費する更なる解析を要する、より困難な潜在的一致に集中することによって、探索空間を絞り込むことを可能にしてもよい。第二に、カスケードアーキテクチャによって、比較モジュール１０６が、資源を消費しすぎることなく、クエリファイル２０８に対する一致が機密ファイルのギャラリーに存在しないと早い段階で判断することによって、早期に終了することを可能にしてもよい。

【００４４】

図４に図示されるように、カスケードアーキテクチャ４１４は、ファイル２０８を、いくつかの実施例では機密ファイル１１２を含む、様々な機密ファイルを格納してもよいギャラリー４０２内のいずれか又は全てのファイルと比較してもよい。カスケードアーキテクチャ４１４は、粗いマッチャー４０４、より精細なマッチャー４０６、及び／又は最も精細なマッチャー４０８を含んでもよい。いくつかの実施形態では、カスケードアーキテクチャは、より精細なマッチャー４０６と最も精細なマッチャー４０８との間に、任意の数の追加のマッチャーを含んでもよい。一実施例では、粗いマッチャー４０４は、ファイル２０８をギャラリー４０２内のファイルと比較してもよい。粗いマッチャー４０４にしたがって、ファイル２０８に類似したファイルがギャラリー４０２内にない場合、本明細書に記載されるシステムは、その時点でカスケードアーキテクチャを終了させてもよい。

次に、より精細なマッチャー４０６が、ファイル２０８を、粗いマッチャー４０４によって除外されなかったギャラリー４０２内の残りのファイルと比較してもよい。より精細なマッチャー４０６にしたがって、ファイル２０８に類似したファイルがギャラリー４０２内にない場合、本明細書に記載されるシステムは、カスケードアーキテクチャを終了させてもよい。このプロセスは、より精細なマッチャー４０８が、ギャラリー４０２内のファイルからファイル２０８に対する最上位の一致４１０を作成するか、又はギャラリー４０２内にはファイル２０８に対する一致がないと判断するまで、任意の数の照合を繰り返してもよい。

【００４５】

図３に戻ると、ステップ３０６で、本明細書に記載されるシステムのうち１つ以上は、画像マッチング技術の結果に基づいて、ファイルがＤＬＰポリシーに違反していると判断してもよい。例えば、判断モジュール１０８は、図２のサーバ２０６の一部として、一致結果２１４に基づいて、ファイル２０８がＤＬＰポリシー２１２に違反していると判断してもよい。

【００４６】

判断モジュール１０８は、様々な手段及び／又はコンテキストで、ファイルがＤＬＰポリシーに違反していると判断してもよい。例えば、判断モジュール１０８は、ファイル２０８とＤＬＰポリシー２１２によって保護されていてもよい機密ファイル１２２との間の類似性を実証する、比較モジュール１０６からの情報を受信してもよい。一実施例として、ＤＬＰポリシー２１２は、従業員の緊急連絡先フォームを第三者に電子メール送信すべきでないことを提示してもよい。この実施例では、機密ファイル１２２は空白の緊急連絡先フォームを構成してもよく、ファイル２０８は、緊急連絡先フォームに記入したバージョンを構成してもよい。そのため、判断モジュール１０８は、ファイル２０８を送信する試みがＤＬＰポリシー２１２の違反を構成すると判断してもよい。

【００４７】

一実施形態では、既知の機密ファイルはテキストベースのフォームを含んでもよく、画像マッチング技術の結果に基づいて、ファイルがＤＬＰポリシーに違反していると判断することは、ファイルがテキストベースのフォームの編集バージョンを含むと判断することを含んでもよい。例えば、ファイル２０８はテキストベースのフォームを含んでもよく、比較モジュール１０６は、ファイル２０８が、一致すると思われる機密ファイル１２２に十分に類似した主要点を含み、更に、機密ファイル１２２内に含まれない他の画像要素を含むと判断してもよい。かかる比較に基づいて、比較モジュール１０６は、ファイル２０８が機密ファイル１２２の編集バージョンを構成すると判断してもよく、判断モジュール１０８は、機密ファイル１２２が社会保障番号などの個人識別情報を要求するフィールドを含むことから、ファイル２０８を送信する試みがＤＬＰポリシー２１２の違反を構成すると判断してもよい。

【００４８】

いくつかの実施例では、フォームは、デジタル化され、画像ギャラリーに追加されて、既知の機密ファイルのサンプル又はコーパスを作成してもよい。例えば、図５に図示されるように、モジュール１０２は、文書５０８のデジタル化バージョンを受信し、フォーム画像ギャラリー５０６へのアクセスを有してもよい。フォーム画像ギャラリー５０６は、ＤＬＰポリシーによって保護されていることが知られているファイルのデジタル表現を含んでもよく、ファイルは、ＰＤＦフォーム５０２又は印刷フォーム５０４などの項目によって具体化されてもよい。印刷フォーム５０４の例としては、非限定的に、税務書類、給与書類、特許開示フォーム、研究ノート、又は他の任意の好適な情報の物理的表現を挙げることができる。モジュール１０２は、文書５０８を検査して、フォーム画像ギャラリー５０６からのフォームの要素が文書５０８中に存在するかを判断してもよい。モジュール１０２が、フォームからの要素が文書５０８中に存在することを見出した場合、モジュール１０２は次に、記入されているであろう任意の領域に関して文書５０８を検査し、変更を含む文書５０８の領域を強調表示してもよい。

【００４９】
文書と機密ファイルとの間の差を強調表示する例示的な一実施形態では、比較モジュール１０６は、画像マッチング技術を使用して、既知の機密ファイルとファイルとの間で異なる要素のセットを表す差分画像を作成することによって、ファイルと既知の機密ファイルとを比較してもよい。この差分画像は、機密ファイル１２２の各画素の値をファイル２０８の対応する画素から差し引くことによって作成されてもよい。比較モジュール１０６は、この差分画像操作が、識別モジュール１０４によって生成される画像変換によって生じる可能性がある軽微な整列誤差に対して堅牢になるような形で、単純な画素対画素の減算を超える特定の画像処理技術を用いてこの差分画像を生成してもよい。画像処理技術の例としては、拡張、侵食などの形態学的操作が挙げられるが、それに限定されない。

【００５０】
同様に、比較モジュール１０６は更に、ファイル２０８と機密ファイル１２２との間の差の強調表示を強調し向上させるために、差分画像に対する形態学的操作を用いてもよい。差分画像は、それにより、画像解析の更なるステップにおいて比較モジュール１０６又は判断モジュール１０８によって使用され、又はセキュリティ対策２１６の一部としてセキュリティモジュール１１０に送達されてもよい。

【００５１】
「形態学的に拡張させる」という用語は、本明細書で使用するとき、所与の画素の値が所与の半径内の他の画素に適用される、画像操作技術を指す。所与の画素の値を適用する例としては、非限定的に、所与の画素の値を周囲の画素に追加すること、並びに／あるいは画素及び周囲の画素の値を平均化することが挙げられる。他のタイプの形態学的操作はまた、本明細書に記載されるモジュールのいずれかによって用いられてもよい。

【００５２】
いくつかの実施例では、判断モジュール１０８は、少なくとも部分的には、強調表示された差分画像に基づいて、ファイルがＤＬＰポリシーに違反していると判断してもよい。図６は、強調表示動作の例示的な出力である。この実施例では、既知の機密ファイル６０２は、従業員情報のフィールドを有するフォームであってもよい。ファイル６０４は、ジェーン・スミス（Jane Smith）という氏名の従業員に関する個人情報を含む、既知の機密ファイル６０２の記入済みコピーを含んでもよい。氏名、日付、電話番号、携帯電話番号、社会保障番号、及び緊急連絡先氏名のフィールドに、ジェーン・スミスに関連する情報が記入されている。点線のボックスで区切られた領域は、既知の機密ファイル６０２をファイル６０４から差し引いた後に強調表示されていてもよい領域を指す。この実施例では、ファイル６０２は、社会保障番号を含むファイルはデータ配信チャネルを介して送信されなくてもよいことを提示するＤＬＰポリシーに違反していることがある。

【００５３】
いくつかの実施例では、判断モジュール１０８は、ファイルがＤＬＰポリシーに違反する何らかのタイプの注釈が、ＯＣＲ解析可能なテキストを含まない場合であっても、その注釈を含むと判断してもよい。例えば、判断モジュール１０８は、画像ファイル間の差が、ファイルが１つ以上の署名、透かし、スタンプ、強調表示、欄外のメモ、及び／又は他の注釈を含むことを示すと判断してもよい。この実施例では、従来のＯＣＲ技術が注釈を解釈することができなかったとしても、本明細書に記載されるシステムによって使用される画像マッチング技術は、依然として、判読不能なテキストを含むか又はテキストを全く含まない潜在的なＤＬＰポリシー違反を識別してもよく、結果としてＤＬＰ実施に対する有効な内容非依存型の方策がもたらされる。

【００５４】
一実施形態では、判断モジュール１０８は、画像マッチング技術の結果に基づいて、ファイルが個人識別情報を含むと判断することによって、ファイルがＤＬＰポリシーに違反していると判断してもよい。判断モジュール１０８は、差分画像、及び／又は比較モジュール１０６によって生成される強調表示された差のセットを利用することによって、ＤＬＰポリシー違反が起こっていることを確定してもよい。例えば、判断モジュール１０８は

、差の領域に基づいて、機密情報がフォームに入力されていると判断してもよい。それに加えて、又は別の方法として、判断モジュール１０８は、写真中の主要点と既知の機密ファイル中の主要点とのマッチングに基づいて試作デバイスなどの機密情報の表現を写真が含むと判断してもよい。

【００５５】

図３に戻ると、ステップ３０８で、本明細書に記載されるシステムのうち１つ以上は、ファイルがＤＬＰポリシーに違反しているとの判断に応答して、セキュリティ対策を実施してもよい。例えば、セキュリティモジュール１１０は、図２のサーバ２０６の一部として、ファイル２０８がＤＬＰポリシー２１２に違反しているとの判断に応答して、セキュリティ対策２１６を実施してもよい。

【００５６】

セキュリティモジュール１１０は、様々な方法でセキュリティ対策を実施してもよい。例えば、セキュリティモジュール１１０は、（１）データ配信チャネルを通してファイルを送信する試みをブロックすること、（２）データ配信チャネルを通してファイルを送信する試みを管理者に警告すること、（３）データ配信チャネルを通してファイルを送信する試みがＤＬＰポリシーに違反していることをユーザに通知すること、及び／又は（４）データ配信チャネルを通してファイルを送信する試みの記録を取ることによって、セキュリティ対策を実施してもよい。例えば、セキュリティモジュール１１０は、添付ファイルとして機密ファイルを含む電子メールをブロックし、かつ／又は電子メールを管理者に転送してもよい。

【００５７】

一実施例では、本明細書に記載されるシステムは、ＤＬＰポリシーの対象である保存ファイルを識別してもよい。例えば、管理者は、コンピューティングデバイスをスキャンして、コンピューティングデバイスに格納されたいずれかのファイルがＤＬＰポリシーの対象であるかを判断してもよい。この実施例では、また図２を参照すると、（１）識別モジュール１０４は、コンピューティングデバイス２０２に格納されている追加ファイルを識別してもよく、（２）比較モジュール１０６は、画像マッチング技術を使用して、追加ファイルを、画像形式で格納されていると共にＤＬＰポリシーによって保護された少なくとも１つの追加の既知の機密ファイルと比較してもよく、（３）判断モジュール１０８は、画像マッチング技術に基づいて、追加ファイルがＤＬＰポリシーに違反していると判断してもよく、（４）セキュリティモジュール１１０は、追加ファイルがＤＬＰポリシーに違反しているという判断に応答して、セキュリティ対策を実施してもよい。

【００５８】

上記の方法３００と関連して説明したように、本明細書に記載されるシステムは、データ配信チャネルを介して送信されるファイルを（例えば、ユーザ若しくは管理者によって提供される）参照文書のギャラリーと比較して、送信されたファイルがＤＬＰポリシーによって保護されているか否かを判断してもよい。本明細書に記載されるシステムは、参照文書及び送信される文書を画像ファイルとして取り扱ってもよく、それらが同じ文書のバージョンを表すか否かを判断するために、画像に対してコンピュータビジョン技術を実施してもよい。送信された文書がギャラリーの画像と一致した場合、本明細書に記載されるシステムは更なる解析を実施して、例えば、テキストベースのフォームの記入済みフィールドを強調表示することによって、差を強調表示してもよい。比較すべき全ての文書を画像として取り扱うことによって、本明細書に記載されるシステムは、ＯＣＲと関連付けられるオーバーヘッド及び／又は困難による負担を負うことなく、文書がＤＬＰポリシーの対象であるか否かに関する判断を効率的に行ってもよい。

【００５９】

図７は、本明細書に記載及び／又は図示される実施形態のうち１つ以上を実装することができる、例示的なコンピューティングシステム７１０のブロック図である。例えば、コンピューティングシステム７１０の全て又は一部分は、単独で又は他の要素と組み合わせて、（図３に図示されるステップのうち１つ以上などの）本明細書に記載されるステップ

のうち１つ以上を実施してもよく、かつ／又はそれを実施するための手段であってもよい。コンピューティングシステム７１０の全て又は一部分はまた、本明細書に記載及び／若しくは図示される他の任意のステップ、方法、又はプロセスを実施してもよく、かつ／あるいはそれを実施するための手段であってもよい。

【００６０】

コンピューティングシステム７１０は、コンピュータ可読命令を実行することができる、任意のシングル若しくはマルチプロセッサのコンピューティングデバイス又はシステムを幅広く表す。コンピューティングシステム７１０の例としては、非限定的に、ワークステーション、ラップトップ、クライアント側端末、サーバ、分散型コンピューティングシステム、ハンドヘルドデバイス、又は他の任意のコンピューティングシステム若しくはデバイスが挙げられる。その最も基本的な構成では、コンピューティングシステム７１０は、少なくとも１つのプロセッサ７１４及びシステムメモリ７１６を含んでもよい。

【００６１】

プロセッサ７１４は、一般に、データの処理又は命令の解釈及び実行が可能な、任意のタイプ若しくは形態の物理的処理装置（例えば、ハードウェア実装型中央処理装置）を表す。特定の実施形態では、プロセッサ７１４は、ソフトウェアアプリケーション又はモジュールから命令を受信してもよい。これらの命令によって、プロセッサ７１４に、本明細書に記載及び／又は図示される例示的な実施形態のうち１つ以上の機能を実施させてもよい。

【００６２】

システムメモリ７１６は、一般に、データ及び／又は他のコンピュータ可読命令を格納することができる、任意のタイプ若しくは形態の揮発性又は不揮発性記憶デバイス又は媒体を表す。システムメモリ７１６の例としては、非限定的に、ランダムアクセスメモリ（ＲＡＭ）、読み取り専用メモリ（ＲＯＭ）、フラッシュメモリ、又は他の任意の好適なメモリデバイスが挙げられる。必須ではないが、特定の実施形態では、コンピューティングシステム７１０は、揮発性メモリユニット（例えば、システムメモリ７１６など）、及び不揮発性記憶デバイス（例えば、詳細に後述されるような、一次記憶デバイス７３２など）の両方を含んでもよい。一実施例では、図１のモジュール１０２のうち１つ以上がシステムメモリ７１６にロードされてもよい。

【００６３】

特定の実施形態では、例示的なコンピューティングシステム７１０はまた、プロセッサ７１４及びシステムメモリ７１６に加えて、１つ以上の構成要素又は要素を含んでもよい。例えば、図７に図示されるように、コンピューティングシステム７１０は、メモリコントローラ７１８、入力／出力（Ｉ／Ｏ）コントローラ７２０、及び通信インターフェース７２２を含んでもよく、それらはそれぞれ通信基盤７１２を介して相互接続されてもよい。通信基盤７１２は一般に、コンピューティングデバイスの１つ以上の構成要素間の通信を容易にすることができる、任意のタイプ若しくは形態の基盤を表す。通信基盤７１２の例としては、非限定的に、通信バス（産業標準アーキテクチャ（ＩＳＡ）、周辺装置相互接続（ＰＣＩ）、ＰＣＩエクスプレス（ＰＣＩｅ）、又は類似のバスなど）、及びネットワークが挙げられる。

【００６４】

メモリコントローラ７１８は、一般に、メモリ若しくはデータを扱うか、又はコンピューティングシステム７１０の１つ以上の構成要素間の通信を制御することができる、任意のタイプ又は形態のデバイスを表す。例えば、特定の実施形態では、メモリコントローラ７１８は、通信基盤７１２を介して、プロセッサ７１４、システムメモリ７１６、及びＩ／Ｏコントローラ７２０の間の通信を制御してもよい。

【００６５】

Ｉ／Ｏコントローラ７２０は、一般に、コンピューティングデバイスの入出力機能を調整及び／又は制御することができる、任意のタイプ又は形態のモジュールを表す。例えば、特定の実施形態では、Ｉ／Ｏコントローラ７２０は、プロセッサ７１４、システムメモ

リ７１６、通信インターフェース７２２、ディスプレイアダプタ７２６、入力インターフェース７３０、及び記憶インターフェース７３４などの、コンピューティングシステム７１０の１つ以上の要素間におけるデータの転送を制御するか又は容易にしてもよい。

【００６６】

通信インターフェース７２２は、例示的なコンピューティングシステム７１０と１つ以上の追加のデバイスとの間の通信を容易にすることができる、任意のタイプ若しくは形態の通信デバイス又はアダプタを広く表す。例えば、特定の実施形態では、通信インターフェース７２２は、コンピューティングシステム７１０と、追加のコンピューティングシステムを含む私設又は公衆ネットワークとの間の通信を容易にしてもよい。通信インターフェース７２２の例としては、非限定的に、有線ネットワークインターフェース（ネットワークインターフェースカードなど）、無線ネットワークインターフェース（無線ネットワークインターフェースカードなど）、モデム、及び他の任意の好適なインターフェースが挙げられる。少なくとも１つの実施形態では、通信インターフェース７２２は、インターネットなどのネットワークへの直接リンクを介して、リモートサーバへの直接接続を提供してもよい。通信インターフェース７２２はまた、例えば、ローカルエリアネットワーク（イーサネットネットワークなど）、パーソナルエリアネットワーク、電話若しくはケーブルネットワーク、セルラー電話接続、衛星データ接続、又は他の任意の好適な接続を通した、かかる接続を間接的に提供してもよい。

【００６７】

特定の実施形態では、通信インターフェース７２２はまた、外部バス又は通信チャネルを介して、コンピューティングシステム７１０と１つ以上の追加のネットワーク又は記憶デバイスとの間の通信を容易にするように構成された、ホストアダプタを表してもよい。ホストアダプタの例としては、非限定的に、小型コンピュータシステムインターフェース（ＳＣＳＩ）ホストアダプタ、ＵＳＢホストアダプタ、米国電気電子学会（ＩＥＥＥ）１３９４ホストアダプタ、アドバンストテクノロジーアタッチメント（ＡＴＡ）、パラレルＡＴＡ（ＰＡＴＡ）、シリアルＡＴＡ（ＳＡＴＡ）、及び外部ＳＡＴＡ（ｅＳＡＴＡ）ホストアダプタ、ファイバーチャネルインターフェースアダプタ、イーサネットアダプタなどが挙げられる。通信インターフェース７２２はまた、コンピューティングシステム７１０が分散型又はリモートコンピューティングに関与することを可能にしてもよい。例えば、通信インターフェース７２２は、実行のためにリモートデバイスから命令を受信するか又はリモートデバイスに命令を送信してもよい。

【００６８】

図７に図示されるように、コンピューティングシステム７１０はまた、ディスプレイアダプタ７２６を介して通信基盤７１２に連結される少なくとも１つのディスプレイデバイス７２４を含んでもよい。ディスプレイデバイス７２４は、一般に、ディスプレイアダプタ７２６によって転送される情報を視覚的に表示することができる、任意のタイプ若しくは形態のデバイスを表す。同様に、ディスプレイアダプタ７２６は、一般に、ディスプレイデバイス７２４に表示するために、通信基盤７１２から（又は当該技術分野において知られているように、フレームバッファから）、グラフィックス、テキスト、及び他のデータを転送するように構成された、任意のタイプ又は形態のデバイスを表す。

【００６９】

図７に図示されるように、例示的なコンピューティングシステム７１０はまた、入力インターフェース７３０を介して通信基盤７１２に連結される少なくとも１つの入力デバイス７２８を含んでもよい。入力デバイス７２８は、一般に、コンピュータ又は人間のいずれかが生成した入力を、例示的なコンピューティングシステム７１０に提供することができる、任意のタイプ若しくは形態の入力デバイスを表す。入力デバイス７２８の例としては、非限定的に、キーボード、ポインティングデバイス、音声認識デバイス、又は他の任意の入力デバイスが挙げられる。

【００７０】

図７に図示されるように、例示的なコンピューティングシステム７１０はまた、記憶イ

ンターフェース７３４を介して通信基盤７１２に連結される、一次記憶デバイス７３２及びバックアップ記憶デバイス７３３を含んでもよい。記憶デバイス７３２及び７３３は、一般に、データ及び／又は他のコンピュータ可読命令を格納することができる、任意のタイプ若しくは形態の記憶デバイス又は媒体を表す。例えば、記憶デバイス７３２及び７３３は、磁気ディスクドライブ（例えば、いわゆるハードドライブ）、ソリッドステートドライブ、フロッピーディスクドライブ、磁気テープドライブ、光ディスクドライブ、フラッシュドライブなどであってもよい。記憶インターフェース７３４は、一般に、記憶デバイス７３２及び７３３とコンピューティングシステム７１０の他の構成要素との間でデータを転送する、任意のタイプ若しくは形態のインターフェース又はデバイスを表す。一実施例では、図１のデータベース１２０は、一次ストレージデバイス７３２に格納されてもよい。

【００７１】

特定の実施形態では、記憶デバイス７３２及び７３３は、コンピュータソフトウェア、データ、又は他のコンピュータ可読情報を格納するように構成された取外し可能な記憶ユニットから読み取り、かつ／又はそれに書込むように構成されてもよい。好適な取外し可能な記憶ユニットの例としては、非限定的に、フロッピーディスク、磁気テープ、光ディスク、フラッシュメモリデバイスなどが挙げられる。記憶デバイス７３２及び７３３はまた、コンピュータソフトウェア、データ、又は他のコンピュータ可読命令をコンピューティングシステム７１０にロードすることを可能にする、他の類似の構造又はデバイスを含んでもよい。例えば、記憶デバイス７３２及び７３３は、ソフトウェア、データ、又は他のコンピュータ可読情報を読み取り、かつ書込むように構成されてもよい。記憶デバイス７３２及び７３３はまた、コンピューティングシステム７１０の一部であってもよく、又は他のインターフェースシステムを通してアクセスされる別個のデバイスであってもよい。

【００７２】

他の多くのデバイス又はサブシステムが、コンピューティングシステム７１０に接続されてもよい。反対に、図７に図示される構成要素及びデバイスは、本明細書に記載及び／又は図示される実施形態を実践するために、必ずしも全てが存在しなくてもよい。上記で言及したデバイス及びサブシステムはまた、図７に示されるものとは異なる方法で相互接続されてもよい。コンピューティングシステム７１０はまた、任意の数のソフトウェア、ファームウェア、及び／又はハードウェアの構成を用いてもよい。例えば、本明細書に開示される例示的な実施形態のうち１つ以上は、コンピュータ可読媒体上で、コンピュータプログラム（コンピュータソフトウェア、ソフトウェアアプリケーション、コンピュータ可読命令、又はコンピュータ制御論理とも称される）としてコード化されてもよい。「コンピュータ可読媒体」という用語は、本明細書で使用するとき、一般に、コンピュータ可読命令を格納若しくは保有することができる、任意の形態のデバイス、キャリア、又は媒体を指す。コンピュータ可読媒体の例としては、非限定的に、搬送波などの伝送型媒体、並びに磁気記憶媒体（例えば、ハードディスクドライブ、テープドライブ、及びフロッピーディスク）、光学記憶媒体（例えば、コンパクトディスク（ＣＤ）、デジタルビデオディスク（ＤＶＤ）、及びブルーレイ（ＢＬＵ－ＲＡＹ）ディスク）、電子記憶媒体（例えば、ソリッドステートドライブ及びフラッシュメディア）、並びに他の分散システムなどの持続性タイプの媒体が挙げられる。

【００７３】

コンピュータプログラムを含むコンピュータ可読媒体は、コンピューティングシステム７１０にロードされてもよい。次に、コンピュータ可読媒体に格納されたコンピュータプログラムの全て又は一部分は、システムメモリ７１６に、並びに／又は記憶デバイス７３２及び７３３の様々な部分に格納されてもよい。プロセッサ７１４によって実行されると、コンピューティングシステム７１０にロードされたコンピュータプログラムは、プロセッサ７１４に、本明細書に記載及び／又は図示される例示的な実施形態のうち１つ以上の機能を実施させてもよく、かつ／又はそれらを実施する手段であってもよい。それに加え

て、又は別の方法として、本明細書に記載及び／又は図示される例示的な実施形態のうち１つ以上は、ファームウェア及び／又はハードウェアに実装されてもよい。例えば、コンピューティングシステム７１０は、本明細書に開示される例示的な実施形態のうち１つ以上を実装するように適合された、特定用途向け集積回路（ＡＳＩＣ）として構成されてもよい。

【００７４】

図８は、クライアントシステム８１０、８２０、及び８３０、並びにサーバ８４０及び８４５がネットワーク８５０に連結されていてもよい、例示的なネットワークアーキテクチャ８００のブロック図である。詳細に上述したように、ネットワークアーキテクチャ８００の全て又は一部分は、単独で又は他の要素と組み合わせて、（図３に図示されるステップのうち１つ以上などの）本明細書に開示されるステップのうち１つ以上を実施してもよく、かつ／又はそれを実施するための手段であってもよい。ネットワークアーキテクチャ８００の全て又は一部分はまた、本開示に記載される他のステップ及び特徴を実施するために使用されてもよく、かつ／又はそれを実施するための手段であってもよい。

【００７５】

クライアントシステム８１０、８２０、及び８３０は、一般に、図７の例示的なコンピューティングシステム７１０などの、任意のタイプ若しくは形態のコンピューティングデバイス又はシステムを表す。同様に、サーバ８４０及び８４５は、一般に、様々なデータベースサービスを提供し、かつ／又は特定のソフトウェアアプリケーションを実行するように構成された、アプリケーションサーバ又はデータベースサーバなどの、コンピューティングデバイス又はシステムを表す。ネットワーク８５０は、一般に、例えばイントラネット、ＷＡＮ、ＬＡＮ、ＰＡＮ、又はインターネットを含む、任意の電気通信又はコンピュータネットワークを表す。一実施例では、クライアントシステム８１０、８２０、及び／若しくは８３０、並びに／又はサーバ８４０及び／若しくは８４５は、図１からのシステム１００の全て又は一部分を含んでもよい。

【００７６】

図８に図示されるように、１つ以上の記憶デバイス８６０（１）～（Ｎ）はサーバ８４０に直接取り付けられてもよい。同様に、１つ以上の記憶デバイス８７０（１）～（Ｎ）はサーバ８４５に直接取り付けられてもよい。記憶デバイス８６０（１）～（Ｎ）及び記憶デバイス８７０（１）～（Ｎ）は、一般に、データ及び／又は他のコンピュータ可読命令を格納することができる、任意のタイプ若しくは形態の記憶デバイス又は媒体を表す。特定の実施形態では、記憶デバイス８６０（１）～（Ｎ）及び記憶デバイス８７０（１）～（Ｎ）は、ネットワークファイルシステム（ＮＦＳ）、サーバメッセージブロック（ＳＭＢ）、又は共通インターネットファイルシステム（ＣＩＦＳ）などの様々なプロトコルを使用して、サーバ８４０及び８４５と通信するように構成されたネットワーク接続記憶（ＮＡＳ）デバイスを表してもよい。

【００７７】

サーバ８４０及び８４５はまた、ストレージエリアネットワーク（ＳＡＮ）ファブリック８８０に接続されてもよい。ＳＡＮファブリック８８０は、一般に、複数の記憶デバイス間の通信を容易にすることができる、任意のタイプ若しくは形態のコンピュータネットワーク又はアーキテクチャを表す。ＳＡＮファブリック８８０は、サーバ８４０及び８４５と、複数の記憶デバイス８９０（１）～（Ｎ）及び／又はインテリジェント記憶アレイ８９５との間の通信を容易にしてもよい。ＳＡＮファブリック８８０はまた、記憶デバイス８９０（１）～（Ｎ）及びインテリジェント記憶アレイ８９５が、クライアントシステム８１０、８２０、及び８３０にローカルで取り付けられたデバイスとして現れるような形で、ネットワーク８５０並びにサーバ８４０及び８４５を介して、クライアントシステム８１０、８２０、及び８３０と、デバイス８９０（１）～（Ｎ）及び／又はアレイ８９５との間の通信を容易にしてもよい。記憶デバイス８６０（１）～（Ｎ）及び記憶デバイス８７０（１）～（Ｎ）と同様に、記憶デバイス８９０（１）～（Ｎ）及びインテリジェント記憶アレイ８９５は、一般に、データ及び／又は他のコンピュータ可読命令を格納す

ることができる、任意のタイプ又は形態の記憶デバイス又は媒体を表す。

【００７８】

特定の実施形態では、図７の例示的なコンピューティングシステム７１０を参照して、図７の通信インターフェース７２２などの通信インターフェースは、各クライアントシステム８１０、８２０、及び８３０とネットワーク８５０との間を接続するように使用されてもよい。クライアントシステム８１０、８２０、及び８３０は、例えば、ウェブブラウザ又は他のクライアントソフトウェアを使用して、サーバ８４０又は８４５上の情報にアクセスすることが可能であってもよい。かかるソフトウェアによって、クライアントシステム８１０、８２０、及び８３０が、サーバ８４０、サーバ８４５、記憶デバイス８６０（１）～（Ｎ）、記憶デバイス８７０（１）～（Ｎ）、記憶デバイス８９０（１）～（Ｎ）、又はインテリジェント記憶アレイ８９５によってホストされるデータにアクセスすることを可能にしてもよい。図８は、データを送受信するのに（インターネットなどの）ネットワークを使用することを示しているが、本明細書に記載及び／又は図示される実施形態は、インターネット、又は任意の特定のネットワークベースの環境に限定されない。

【００７９】

少なくとも１つの実施形態では、本明細書に開示される例示的な実施形態のうち１つ以上の全て又は一部分は、コンピュータプログラムとしてコード化され、サーバ８４０、サーバ８４５、記憶デバイス８６０（１）～（Ｎ）、記憶デバイス８７０（１）～（Ｎ）、記憶デバイス８９０（１）～（Ｎ）、インテリジェント記憶アレイ８９５、又はこれらの任意の組み合わせ上にロードされ、これらによって実行されてもよい。本明細書に開示される例示的な実施形態のうち１つ以上の全て又は一部分は、また、コンピュータプログラムとしてコード化され、サーバ８４０に記憶され、サーバ８４５によって実行され、ネットワーク８５０上でクライアントシステム８１０、８２０、及び８３０に配信されてもよい。

【００８０】

詳細に上述したように、コンピューティングシステム７１０、及び／又はネットワークアーキテクチャ８００の１つ以上の構成要素は、単独で又は他の要素と組み合わせて、データ配信チャネルを介して機密情報を送信する試みを検出するための、例示的な方法の１つ以上のステップを実施してもよく、並びに／あるいはそれを実施するための手段であってもよい。

【００８１】

前述の開示は、特定のブロック図、フローチャート、及び実施例を使用して様々な実施形態について記載しているが、本明細書に記載及び／又は図示される各ブロック図の構成要素、フローチャートのステップ、動作、及び／又は構成要素は、個別にかつ／又は集合的に、広範なハードウェア、ソフトウェア、又はファームウェア（若しくはそれらの任意の組み合わせ）の構成を使用して実装されてもよい。それに加えて、他の多くのアーキテクチャが同じ機能性を達成するように実装可能であるので、他の構成要素内に含まれる構成要素のいずれの開示も、本質的に例示と見なされるべきである。

【００８２】

いくつかの実施例では、図１の例示的なシステム１００の全て又は一部分は、クラウドコンピューティング環境又はネットワークベースの環境の一部を表してもよい。クラウドコンピューティング環境は、インターネットを介して、様々なサービス及びアプリケーションを提供してもよい。これらのクラウドベースのサービス（例えば、サービスとしてのソフトウェア、サービスとしてのプラットフォーム、サービスとしての基盤など）は、ウェブブラウザ又は他のリモートインターフェースを通してアクセス可能であってもよい。本明細書に記載される様々な機能は、リモートデスクトップ環境又は他の任意のクラウドベースのコンピューティング環境を通して提供されてもよい。

【００８３】

様々な実施形態では、図１の例示的なシステム１００の全て又は一部分は、クラウドベースのコンピューティング環境内でのマルチテナンシーを容易にすることができる。換言

すれば、本明細書に記載されるソフトウェアモジュールは、本明細書に記載される機能の１つ以上に対するマルチテナンシーを容易にするように、コンピューティングシステム（例えば、サーバ）を構成してもよい。例えば、本明細書に記載されるソフトウェアモジュールの１つ以上は、２つ以上のクライアント（例えば、顧客）がサーバ上で作動しているアプリケーションを共有できるように、サーバをプログラムしてもよい。このようにプログラムされたサーバは、複数の顧客（即ち、テナント）の間で、アプリケーション、オペレーティングシステム、処理システム、及び／又は記憶システムを共有してもよい。本明細書に記載されるモジュールのうち１つ以上はまた、ある顧客が別の顧客のデータ及び／又は構成情報にアクセスすることができないように、顧客ごとにマルチテナントアプリケーションのデータ及び／又は構成情報を分割してもよい。

【００８４】

様々な実施形態によれば、図１の例示的なシステム１００の全て又は一部分は、仮想環境内で実装されてもよい。例えば、本明細書に記載されるモジュール及び／又はデータは、仮想機械内で常駐及び／又は実行してもよい。本明細書で使用するとき、「仮想機械」という用語は、一般に、仮想機械マネージャ（例えば、ハイパーバイザ）によってコンピューティングハードウェアから抽出される、任意のオペレーティングシステム環境を指す。それに加えて、又は別の方法として、本明細書に記載されるモジュール及び／又はデータは、仮想化層内で常駐及び／又は実行してもよい。本明細書で使用するとき、「仮想化層」という用語は、一般に、オペレーティングシステム環境にオーバーレイする、並びに／あるいはそこから抽出される、任意のデータ層及び／又はアプリケーション層を指す。仮想化層は、基礎となる基本オペレーティングシステムの一部であるかのように仮想化層を提示する、ソフトウェア仮想化ソリューション（例えば、ファイルシステムフィルタ）によって管理されてもよい。例えば、ソフトウェア仮想化ソリューションは、最初に基本ファイルシステム及び／又はレジストリ内の場所に方向付けられる呼出しを、仮想化層内の場所にリダイレクトしてもよい。

【００８５】

いくつかの実施例では、図１の例示的なシステム１００の全て又は一部分は、モバイルコンピューティング環境の一部を表してもよい。モバイルコンピューティング環境は、携帯電話、タブレットコンピュータ、電子ブックリーダー、携帯情報端末、ウェアラブルコンピューティングデバイス（例えば、ヘッドマウントディスプレイを備えたコンピューティングデバイス、スマートウォッチなど）などを含む、広範なモバイルコンピューティングデバイスによって実装されてもよい。いくつかの実施例では、モバイルコンピューティング環境は、例えば、バッテリ電力への依存、任意の所与の時間における１つのみのフォアグラウンドアプリケーションの提示、リモート管理特性、タッチスクリーン特性、位置及び移動データ（例えば、全世界測位システム、ジャイロスコープ、加速度計などによって提供される）、システムレベルの構成に対する修正を制限する、及び／又は第三者のソフトウェアが他のアプリケーションの挙動を検査する能力を限定する、アプリケーションのインストールを制限するように（例えば、認可されたアプリケーションストアからのみ生じるように）制御するなどの制限されたプラットフォームを含む、１つ以上の個別の特性を有してもよい。本明細書に記載される様々な機能は、モバイルコンピューティング環境に提供されてもよく、かつ／又は他のモバイルコンピューティング環境と相互作用してもよい。

【００８６】

加えて、図１の例示的なシステム１００の全て又は一部分は、情報管理のための１つ以上のシステムの部分を表してもよく、それと相互作用してもよく、それによって作成されるデータを消費してもよく、並びに／あるいはそれによって消費されるデータを作成してもよい。本明細書で使用するとき、「情報管理」という用語は、データの保護、組織化、及び／又は格納を指してもよい。情報管理のためのシステムの例としては、非限定的に、記憶システム、バックアップシステム、アーカイブシステム、複製システム、高可用性システム、データ検索システム、仮想化システムなどを挙げることができる。

【００８７】
いくつかの実施形態では、図１の例示的なシステム１００の全て又は一部分は、情報セキュリティのための１つ以上のシステムの部分を表してもよく、それによって保護されるデータを作成してもよく、かつ／又はそれと通信してもよい。本明細書で使用するとき、「情報セキュリティ」という用語は、保護されたデータへのアクセスの制御を指してもよい。情報セキュリティのためのシステムの例としては、非限定的に、管理されたセキュリティサービスを提供するシステム、データ漏えい防止システム、本人認証システム、アクセス制御システム、暗号化システム、ポリシー遵守システム、侵入検出及び防止システム、電子証拠開示システムなどが挙げられ得る。

【００８８】
いくつかの実施例によれば、図１の例示的なシステム１００の全て又は一部分は、エンドポイントセキュリティのための１つ以上のシステムの部分を表してもよく、それと通信してもよく、かつ／又はそれから保護を受けてもよい。本明細書で使用するとき、「エンドポイントセキュリティ」という用語は、権限がない及び／又は違法な使用、アクセス、並びに／あるいは制御からの、エンドポイントシステムの保護を指してもよい。エンドポイント保護のためのシステムの例としては、非限定的に、アンチマルウェアシステム、ユーザ認証システム、暗号化システム、プライバシーシステム、スパムフィルタリングサービスなどを挙げることができる。

【００８９】
本明細書に記載及び／又は図示されるプロセスパラメータ及び一連のステップは、単なる例として与えられるものであり、所望に応じて変更することができる。例えば、本明細書に図示及び／又は記載されるステップは特定の順序で示されるか又は考察されることがあるが、これらのステップは必ずしも図示又は考察される順序で実施されなくてもよい。本明細書に記載及び／又は図示される様々な例示的方法は、また、本明細書に記載若しくは図示されるステップの１つ以上を省略するか、又は開示されるものに加えて追加のステップを含んでもよい。

【００９０】
様々な実施形態を、完全に機能しているコンピューティングシステムのコンテキストで明細書に記載及び／又は図示してきたが、これらの例示的な実施形態の１つ以上は、実際に配信を実施するのに使用されるコンピュータ可読媒体の特定のタイプにかかわらず、様々な形態のプログラム製品として配信されてもよい。本明細書で開示される実施形態はまた、特定のタスクを実行するソフトウェアモジュールを使用して実装されてもよい。これらのソフトウェアモジュールは、コンピュータ可読記憶媒体に、又はコンピューティングシステムに格納することができる、スクリプト、バッチ、又は他の実行可能ファイルを含んでもよい。いくつかの実施形態では、これらのソフトウェアモジュールは、本明細書で開示される例示的な実施形態のうち１つ以上を実行するように、コンピューティングシステムを構成してもよい。

【００９１】
それに加えて、本明細書に記載されるモジュールのうち１つ以上は、データ、物理的デバイス、及び／又は物理的デバイスの表現を、１つの形態から別の形態へと変換してもよい。例えば、本明細書に列挙されるモジュールの１つ以上は、変換されるファイルを受信し、ファイルデータを変換し、変換の結果を画像マッチング技術に出力し、変換の結果を使用して、２つの画像が同じ文書を表しているか否かを判断し、変換の結果をデータベースに格納してもよい。それに加えて、又は別の方法として、本明細書に列挙されるモジュールの１つ以上は、コンピューティングデバイス上で実行すること、コンピューティングデバイスにデータを格納すること、及び／又は別の方法でコンピューティングデバイスと相互作用することによって、プロセッサ、揮発性メモリ、不揮発性メモリ、及び／又は物理コンピューティングデバイスの他の任意の一部を、ある形態から別の形態へと変換してもよい。

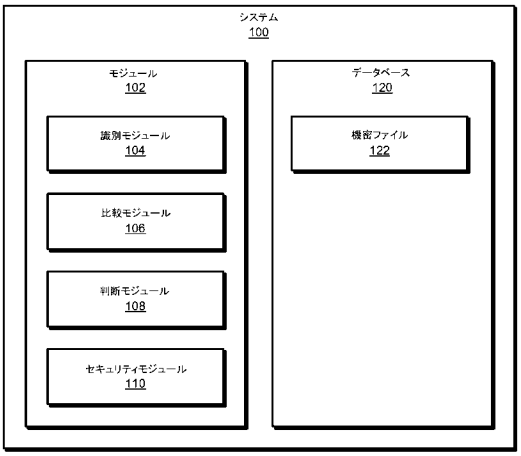
【００９２】

前述の記載は、本明細書に開示される例示的な実施形態の様々な態様を、他の当業者が最良に利用することができるように提供してきた。この例示的な記載は、網羅的であることを意図するものではなく、又は開示される任意の正確な形態に限定することを意図するものではない。本開示の趣旨及び範囲から逸脱することなく、多くの修正例及び変形例が可能である。本明細書で開示される実施形態は、あらゆる点で例示的であり、限定的ではないものと見なされるべきである。本開示の範囲を決定する際に、添付の特許請求の範囲及びそれらの等価物を参照するべきである。

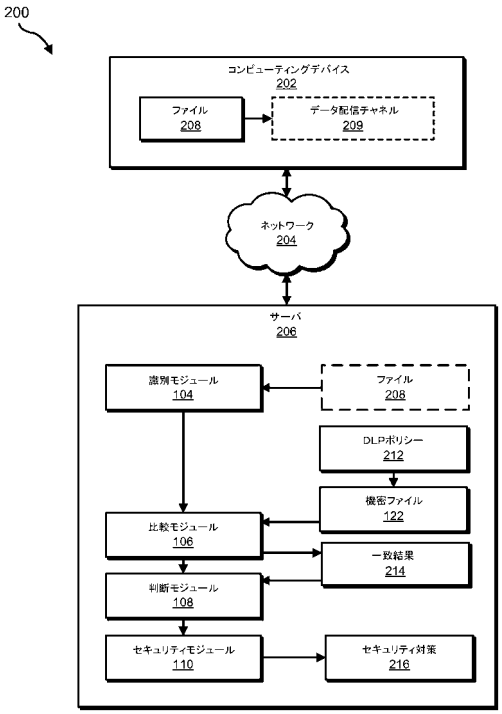
【００９３】

別途記載のない限り、「～に接続される」及び「～に連結される」という用語（並びにそれらの派生語）は、本明細書及び特許請求の範囲で使用するとき、直接的接続及び間接的接続（すなわち、他の要素又は構成要素を介する）の両方を許容するものとして解釈されるべきである。それに加えて、「１つの（a）」又は「１つの（an）」という用語は、本明細書及び特許請求の範囲で使用するとき、「～のうち少なくとも１つ」を意味するものとして解釈されるべきである。最後に、簡潔にするため、「含む」及び「有する」という用語（並びにそれらの派生語）は、本明細書及び特許請求の範囲で使用するとき、「備える」という単語と互換性があり、同じ意味を有する。

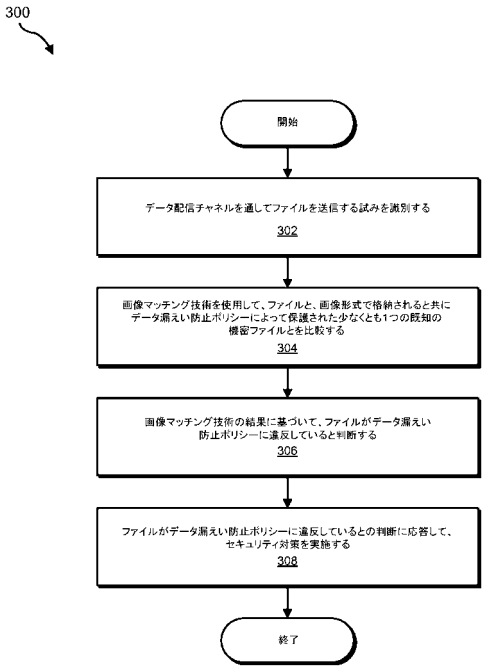
【図１】



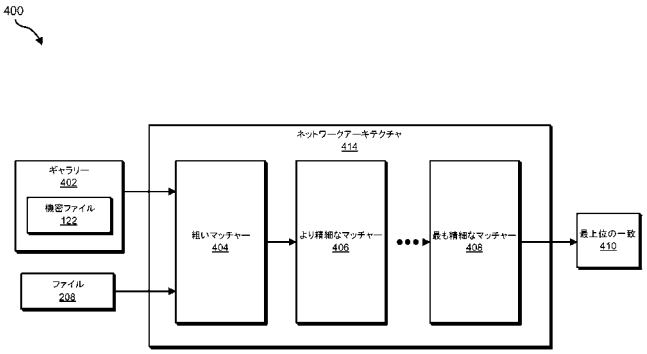
【図２】



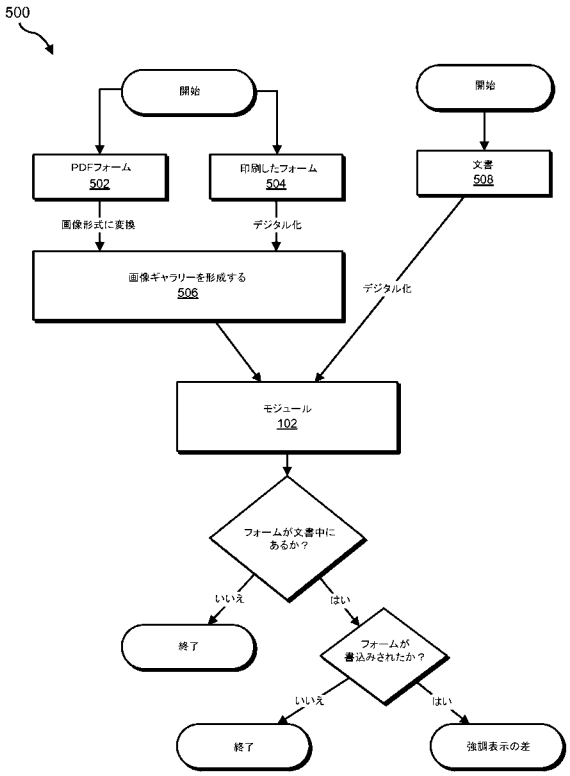
【図３】


300
開始
データ配信チャネルを通してファイルを送信する試みを識別する
302
画像マッチング技術を使用して、ファイルと、画像形式で格納されると共にデータ漏えい防止ポリシーによって保護された少なくとも1つの既知の機密ファイルとを比較する
304
画像マッチング技術の結果に基づいて、ファイルがデータ漏えい防止ポリシーに違反していると判断する
306
ファイルがデータ漏えい防止ポリシーに違反しているとの判断に応答して、セキュリティ対策を実施する
308
終了

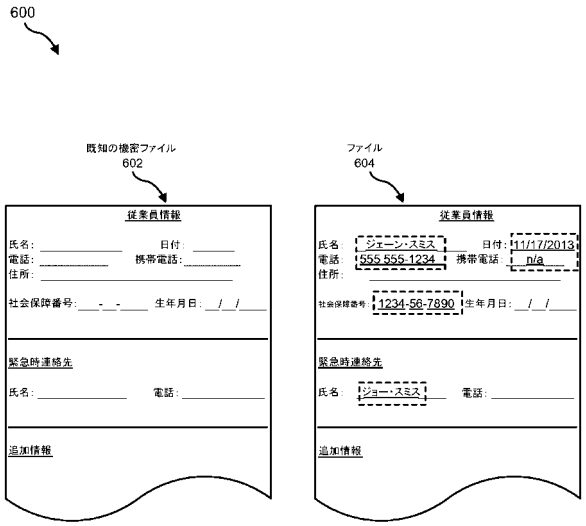
【図４】


400
ネットワークアーキテクチャ
414
ギャラリー
402
機密ファイル
122
ファイル
208
粗いマッチャー
404
より精細なマッチャー
406
最も精細なマッチャー
408
最上位の一致
410

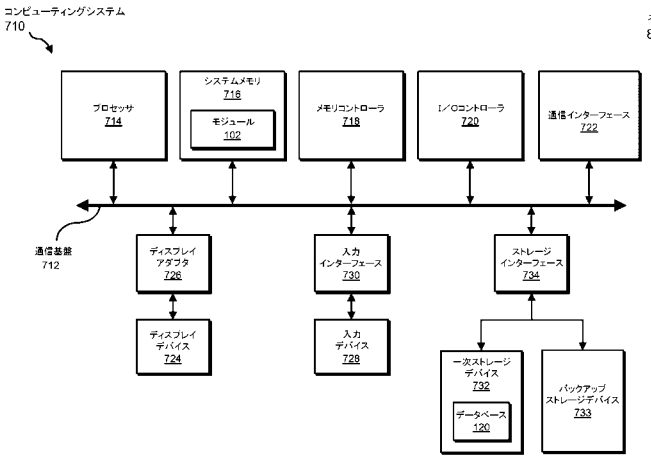
【図５】


500
開始
PDFフォーム
502
印刷したフォーム
504
画像形式に変換
デジタル化
画像ギャラリーを形成する
506
開始
文書
508
デジタル化
モジュール
102
フォームが文書中にあるか？
いいえ
はい
終了
フォームが書込みされたか？
いいえ
はい
終了
強調表示の差

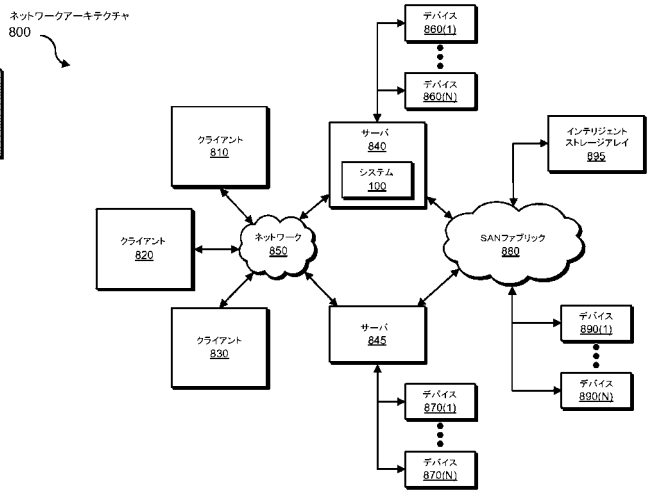
【図６】


600
既知の機密ファイル
602
従業員情報
氏名：
日付：
電話：
携帯電話：
住所：
社会保障番号：
生年月日：
緊急時連絡先
氏名：
電話：
追加情報
ファイル
604
従業員情報
氏名
ジェーン・スミス
日付：11/17/2013
電話
555 555-1234
携帯電話：n/a
住所：
社会保障番号：1234-56-7890
生年月日：
緊急時連絡先
氏名：
ジョー・スミス
電話：
追加情報

【図７】



【図８】



【手続補正書】
【提出日】平成29年2月26日(2017.2.26)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
データ配信チャネルを介して機密情報を送信する試みを検出するためのコンピュータ実装方法であって、前記方法の少なくとも一部分が、少なくとも１つのプロセッサを備えるコンピューティングデバイスによって実施され、前記方法が、
データ配信チャネルを通してファイルを送信する試みを識別することと、
画像マッチング技術を使用して、前記ファイルと、画像形式で格納されると共にデータ漏えい防止ポリシーによって保護された少なくとも１つの既知の機密ファイルとを比較することと、
前記画像マッチング技術の結果に基づいて、前記ファイルが、個人識別情報を含むことによって前記データ漏えい防止ポリシーに違反していると判断することと、
前記ファイルが前記データ漏えい防止ポリシーに違反しているとの判断に応答して、セキュリティ対策を実施することと、
を含む、コンピュータ実装方法。
【請求項２】
前記セキュリティ対策が、
前記データ配信チャネルを通して前記ファイルを送信する前記試みをブロックすることと、

前記データ配信チャネルを通して前記ファイルを送信する前記試みを管理者に警告することと、
前記データ配信チャネルを通して前記ファイルを送信する前記試みが前記データ漏えい防止ポリシーに違反していることをユーザに通知することと、
前記データ配信チャネルを通して前記ファイルを送信する前記試みの記録を取ることと、
のうち少なくとも１つを含む、請求項１に記載のコンピュータ実装方法。
【請求項３】
前記画像マッチング技術を使用して、前記ファイルと前記既知の機密ファイルとを比較することが、前記ファイルを前記画像形式に変換することを含む、請求項１に記載のコンピュータ実装方法。
【請求項４】
前記既知の機密ファイルがテキストベースのフォームを含み、前記画像マッチング技術の結果に基づいて、前記ファイルが前記データ漏えい防止ポリシーに違反していると判断することが、前記ファイルが前記テキストベースのフォームの編集バージョンを含むと判断することを含む、請求項１に記載のコンピュータ実装方法。
【請求項５】
前記画像マッチング技術を使用して、前記ファイルと前記既知の機密ファイルとを比較することが、前記既知の機密ファイルと前記ファイルとの間で異なる要素のセットを表す差分画像を作成することを含む、請求項１に記載のコンピュータ実装方法。
【請求項６】
前記画像マッチング技術を使用して、前記ファイルと前記既知の機密ファイルとを比較することが、前記既知の機密ファイル内の主要点のセットと同種である前記ファイル内の主要点のセットを識別することを含む、請求項１に記載の方法。
【請求項７】
前記画像マッチング技術を使用して、前記ファイルと前記既知の機密ファイルとを比較することが、
前記ファイルの単一の視覚要素を前記既知の機密ファイルの単一の視覚要素と比較することと、
前記ファイルの主要特徴間の距離比のセットを前記既知の機密ファイルの主要特徴間の距離比のセットと比較することと、
距離メトリックを使用して、前記ファイルに属する特徴ベクトルのセットを前記既知の機密ファイルに属する特徴ベクトルのセットと比較することと、
のうち少なくとも１つを含む、請求項１に記載の方法。
【請求項８】
前記画像マッチング技術を使用して、前記ファイルと、前記画像形式で格納されると共に前記データ漏えい防止ポリシーによって保護された前記既知の機密ファイルとを比較することが、
画像形式で格納されると共に前記データ漏えい防止ポリシーによって保護された既知の機密ファイルのギャラリーを識別することと、
粗い画像マッチング技術を使用して、前記ファイルと前記ギャラリー内の複数の既知の機密ファイルとを比較することと、
前記粗い画像マッチング技術よりも多くのコンピューティング資源を消費する、より精細な画像マッチング技術を使用して、前記ファイルと、前記粗い画像マッチング技術によって廃棄されなかった前記ギャラリー内の複数の既知の機密ファイルとを比較することと、
前記より精細な画像マッチング技術よりも多くのコンピューティング資源を消費する最終画像マッチング技術を使用して、前記ファイルと、前記より精細な画像マッチング技術によって廃棄されなかった前記ギャラリー内の複数の既知の機密ファイルとを比較することと、

を含む、請求項１に記載のコンピュータ実装方法。
【請求項９】
前記データ配信チャネルが取外し可能な記憶媒体を含む、請求項１に記載のコンピュータ実装方法。
【請求項１０】
前記コンピューティングデバイスに格納されている追加ファイルを識別することと、
前記画像マッチング技術を使用して、前記追加ファイルと、前記画像形式で格納されると共に前記データ漏えい防止ポリシーによって保護された少なくとも１つの追加の既知の機密ファイルとを比較することと、
前記画像マッチング技術に基づいて、前記追加ファイルが前記データ漏えい防止ポリシーに違反していると判断することと、
前記追加ファイルが前記データ漏えい防止ポリシーに違反しているとの判断に応答して、追加のセキュリティ対策を実施することと、
を更に含む、請求項１に記載のコンピュータ実装方法。
【請求項１１】
データ配信チャネルを介して機密情報を送信する試みを検出するためのシステムであって、前記システムが、
データ配信チャネルを通してファイルを送信する試みを識別する、メモリに格納された、識別モジュールと、
画像マッチング技術を使用して、前記ファイルと、画像形式で格納されると共にデータ漏えい防止ポリシーによって保護された少なくとも１つの既知の機密ファイルとを比較する、メモリに格納された、比較モジュールと、
前記画像マッチング技術の結果に基づいて、前記ファイルが、個人識別情報を含むことによって前記データ漏えい防止ポリシーに違反していると判断する、メモリに格納された、判断モジュールと、
前記ファイルが前記データ漏えい防止ポリシーに違反しているとの判断に応答してセキュリティ対策を実施する、メモリに格納された、セキュリティモジュールと、
前記識別モジュール、前記比較モジュール、前記判断モジュール、及び前記セキュリティモジュールを実行するように構成された、少なくとも１つの物理的プロセッサと、
を備える、システム。
【請求項１２】
前記既知の機密ファイルがテキストベースのフォームを含み、前記判断モジュールが、前記画像マッチング技術の結果に基づいて、前記ファイルが前記テキストベースのフォームの編集バージョンを含むと判断することによって、前記ファイルが前記データ漏えい防止ポリシーに違反していると判断する、請求項１１に記載のシステム。
【請求項１３】
前記比較モジュールが、前記画像マッチング技術を使用して、前記既知の機密ファイルと前記ファイルとの間で異なる要素のセットを表す差分画像を作成することによって、前記ファイルと前記既知の機密ファイルとを比較する、請求項１１に記載のシステム。
【請求項１４】
前記比較モジュールが、前記画像マッチング技術を使用して、
画像形式で格納されると共に前記データ漏えい防止ポリシーによって保護された既知の機密ファイルのギャラリーを識別することと、
粗い画像マッチング技術を使用して、前記ファイルと前記ギャラリー内の複数の既知の機密ファイルとを比較することと、
前記粗い画像マッチング技術よりも多くのコンピューティング資源を消費する、より精細な画像マッチング技術を使用して、前記ファイルと、前記粗い画像マッチング技術によって廃棄されなかった前記ギャラリー内の複数の既知の機密ファイルとを比較することと、
前記より精細な画像マッチング技術よりも多くのコンピューティング資源を消費する最

終画像マッチング技術を使用して、前記ファイルと、前記より精細な画像マッチング技術によって廃棄されなかった前記ギャラリー内の複数の既知の機密ファイルとを比較することと、

によって、前記ファイルと、前記画像形式で格納されると共に前記データ漏えい防止ポリシーによって保護された前記既知の機密ファイルとを比較する、請求項１１に記載のシステム。

【請求項１５】

１つ以上のコンピュータ可読命令を含む非一時的コンピュータ可読媒体であって、コンピューティングデバイスの少なくとも１つのプロセッサによって実行されると、前記コンピューティングデバイスに、

データ配信チャネルを通してファイルを送信する試みを識別させ、

画像マッチング技術を使用して、前記ファイルと、画像形式で格納されると共にデータ漏えい防止ポリシーによって保護された少なくとも１つの既知の機密ファイルとを比較させ、

前記画像マッチング技術の結果に基づいて、前記ファイルが、個人識別情報を含むことによって前記データ漏えい防止ポリシーに違反していると判断させ、

前記ファイルが前記データ漏えい防止ポリシーに違反しているとの判断に応答して、セキュリティ対策を実施させる、

非一時的コンピュータ可読媒体。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/043056

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/62 H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2012/183174 A1 (BASAVAPATNA PRASANNA GANAPATHI [IN] ET AL) 19 July 2012 (2012-07-19) paragraph [0020] - paragraph [0026] paragraph [0040] -----	1-20
A	Kyn: "Computer vision - Wikipedia, the free encyclopedia", , 1 September 2014 (2014-09-01), XP055219484, Retrieved from the Internet: URL:https://en.wikipedia.org/w/index.php?title=Computer_vision&oldid=623719213 [retrieved on 2015-10-08] the whole document -----	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 October 2015	30/10/2015

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Koblitz, Birger

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/043056

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012183174 A1	19-07-2012	US 8199965 B1	12-06-2012
		US 2012183174 A1	19-07-2012

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

（特許庁注：以下のものは登録商標）
１．Ｂｌｕ－ｒａｙ

(72)発明者 リンゼー・マイケル
アメリカ合衆国 カリフォルニア州 ９４１１５ サンフランシスコ ブキャナンストリート ２４００ アパートメント ３０２

Ｆターム(参考) 5L096 AA06 HA08 JA11