(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2008-521149
(P2008-521149A)
(43)公表日　平成20年6月19日(2008.6.19)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B285
G06F 13/00	(2006.01)	G06F	13/00	610Q	

審査請求 未請求　予備審査請求 未請求　（全 73 頁）

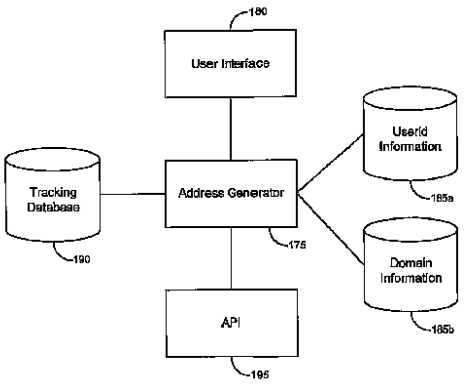
(21)出願番号　特願2007-543525 (P2007-543525)
(86)(22)出願日　平成17年11月23日 (2005.11.23)
(85)翻訳文提出日　平成19年7月20日 (2007.7.20)
(86)国際出願番号　PCT/US2005/042753
(87)国際公開番号　WO2006/058217
(87)国際公開日　平成18年6月1日 (2006.6.1)
(31)優先権主張番号　10/997,626
(32)優先日　平成16年11月23日 (2004.11.23)
(33)優先権主張国　米国 (US)

(71)出願人　506367803
マークモニター　インコーポレイテッド
アメリカ合衆国　アイダホ　８３７０４，　ボイシ，　エヌ．　アンセスター　プレイス　３９１，　エメラルド　テック　センター
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明
(74)代理人　100113413
弁理士　森下　夏樹

最終頁に続く

(54)【発明の名称】オンライン詐欺の可能性に関連するデータを解析するための方法およびシステム

(57)【要約】
本発明の様々な実施形態はデータを解析するための方法、システムおよびソフトウェアを提供する。例えば、特定の実施形態においては、ウェブサイトについてのデータのセットは、ウェブサイトが不正である（例えば、フィッシング詐欺、グレイマーケットの商品の販売などの詐欺的スキームに包含される）可能性があるかどうかを決定するために解析され得る。例示的な実施形態においては、データのセットは複数のコンポーネント（一部の場合には、これらの各々は個別のデータセットであると考慮され得る）に分割され得る。単なる例として、データのセットは複数のデータ供給源から集められたデータを備え得、および／または各コンポーネントは複数のデータ供給源から集められたデータを備え得る。別の例として、データのセットは複数のセクションを有するドキュメントを備え得、各コンポーネントは複数のセクションの１つを備え得る。



【特許請求の範囲】
【請求項１】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、該方法は、
コンピュータが、該ウェブサイトと関連するデータのセットにアクセスすることと、
該コンピュータが、該データのセットを複数のコンポーネントに分割することと、
該複数のコンポーネントの少なくとも幾つかを解析することと、
該解析されたコンポーネントの各々にスコアを割り当てることであって、該スコアは、複数のスコアが割り当てられるように、該解析されたコンポーネントの各々の解析に基づいている、ことと、
該データのセットに複合スコアを割り当てることであって、該複合スコアは、該複数のスコアに基づいている、ことと、
該複合スコアに基づいて、詐欺である可能性があるウェブサイトとして該ウェブサイトを分類することと
を包含する、方法。
【請求項２】
ウェブサイトを詐欺である可能性があるウェブサイトとして分類する方法であって、前記データのセットは、ニュースグループの掲示を含む、請求項１に記載の方法。
【請求項３】
ウェブサイトを詐欺である可能性があるウェブサイトとして分類する方法であって、前記データのセットは、ウェブページを含む、請求項１に記載の方法。
【請求項４】
ウェブサイトを詐欺である可能性があるウェブサイトとして分類する方法であって、前記データのセットは、インターネットチャットセッションからの複写を含む、請求項１に記載の方法。
【請求項５】
ウェブサイトを詐欺である可能性があるウェブサイトとして分類する方法であって、前記データのセットは、電子メールメッセージを含む、請求項１に記載の方法。
【請求項６】
ウェブサイトを詐欺である可能性があるウェブサイトとして分類する方法であって、前記複数のコンポーネントは、
前記電子メールメッセージのヘッダ部分と、
該電子メールメッセージの本体部分と、
該電子メールメッセージの本体部分内に組み込まれたユニフォームリソースロケータ（「ＵＲＬ」）であって、該ＵＲＬは、ウェブサイトを参照する、ＵＲＬと
を含む、請求項５に記載の方法。
【請求項７】
ウェブサイトを詐欺である可能性があるウェブサイトとして分類する方法であって、前記データのセットにアクセスすることは、前記電子メールメッセージを受信することを含む、請求項５に記載の方法。
【請求項８】
ウェブサイトを詐欺である可能性があるウェブサイトとして分類する方法であって、前記データのセットは、該ウェブサイトと関連するドメインについてのデータを含む、請求項１に記載の方法。
【請求項９】
ウェブサイトを詐欺である可能性があるウェブサイトとして分類する方法であって、前記データのセットにアクセスすることは、ゾーンファイルにおいてドメインレジストレーションにアクセスすることを含む、請求項８に記載の方法。
【請求項１０】
ウェブサイトを詐欺である可能性があるウェブサイトとして分類する方法であって、前

記複数のコンポーネントは、該ウェブサイトと関連するインターネットプロトコル（「ＩＰ」）アドレスを含み、該複数のコンポーネントの少なくとも幾つかを解析することは、
該ウェブサイトと関連するドメインを識別することと、
該ドメインに割り当てられたインターネットプロトコル（「ＩＰ」）ブロックを識別することと、
該ＩＰアドレスと該ドメインに割り当てられた該ＩＰブロックとを比較することと
を含む、請求項８に記載の方法。
【請求項１１】
ウェブサイトを詐欺である可能性があるウェブサイトとして分類する方法であって、前記データのセットは、該ウェブサイトをホストするサーバについてのデータのセットを含む、請求項１に記載の方法。
【請求項１２】
ウェブサイトを詐欺である可能性があるウェブサイトとして分類する方法であって、前記データのセットにアクセスすることは、該ウェブサイトに問い合わせることを含む、請求項１１に記載の方法。
【請求項１３】
ウェブサイトを詐欺である可能性があるウェブサイトとして分類する方法であって、前記データのセットは、該ウェブサイトを参照するユニフォームリソースロケータ（「ＵＲＬ」）についてのデータのセットを含む、請求項１に記載の方法。
【請求項１４】
電子メールメッセージを分類する方法であって、該方法は、
コンピュータが、該電子メールメッセージを複数のコンポーネントに分割することと、
該コンピュータが、該複数のコンポーネントの少なくとも１つを解析することと、
該複数のコンポーネントの少なくとも１つの解析に基づいて、該複数のコンポーネントの少なくとも１つにスコアを割り当てることと、
該複数のコンポーネントの少なくとも１つに割り当てられたスコアに基づいて、該電子メールメッセージを分類することと
を包含する、方法。
【請求項１５】
電子メールメッセージを分類する方法であって、該方法は、
前記コンピュータが、前記複数のコンポーネントの各々を解析することと、
該複数のコンポーネントの各々に対して、該コンピュータが、該コンポーネントにスコアを割り当て、該スコアは、該コンポーネントの解析に基づいている、ことと、
該複数のコンポーネントの各々に割り当てられたスコアに基づいて、該電子メールメッセージに複合スコアを割り当てることと
をさらに含み、
該電子メールメッセージを分類することは、該複合スコアに基づいて該電子メールメッセージを分類することを含む、請求項１４に記載の方法。
【請求項１６】
電子メールメッセージを分類する方法であって、該電子メールメッセージは、ヘッダ部分、本体部分およびウェブサイトを参照するユニフォームリソースロケータ（「ＵＲＬ」）を含み、該方法は、
該ヘッダ部分を解析することと、
該ヘッダ部分にスコアを割り当てることと
をさらに含む、請求項１４に記載の方法。
【請求項１７】
電子メールメッセージを分類する方法であって、該方法は、
該本体部分を解析することと、
該本体部分にスコアを割り当てることと
をさらに含む、請求項１６に記載の方法。

【請求項１８】
電子メールメッセージを分類する方法であって、
該本体部分を解析し、該本体部分にスコアを割り当てるステップは、該ヘッダ部分に割り当てられたスコアが特定の閾値スコアを超える場合にだけ実行される、請求項１７に記載の方法。
【請求項１９】
電子メールメッセージを分類する方法であって、該方法は、
前記ＵＲＬを解析することと、
該ＵＲＬにスコアを割り当てることと
をさらに含む、請求項１７に記載の方法。
【請求項２０】
電子メールメッセージを分類する方法であって、
該ＵＲＬを解析し、該ＵＲＬにスコアを割り当てるステップは、該本体部分に割り当てられたスコアが特定の閾値スコアを超える場合にだけ実行される、請求項１９に記載の方法。
【請求項２１】
電子メールメッセージを分類する方法であって、
前記ＵＲＬを解析することは、該ＵＲＬにより参照されたウェブサイトをホストするサーバに問い合わせることを含む、請求項１９に記載の方法。
【請求項２２】
電子メールメッセージを分類する方法であって、該方法は、
該ヘッダ部分および本体部分に組み合わせスコアを割り当てることであって、該組み合わせスコアは、該ヘッダ部分に割り当てられたスコアおよび該本体部分に割り当てられたスコアに基づいていること
をさらに含み、
該ＵＲＬを解析し、該ＵＲＬにスコアを割り当てるステップは、該本体部分に割り当てられた組み合わせスコアが特定の閾値スコアを超える場合にだけ実行される、請求項１９に記載の方法。
【請求項２３】
電子メールメッセージを分類する方法であって、該方法は、
該電子メールメッセージに複合スコアを割り当てることであって、該複合スコアは、該ヘッダ部分に割り当てられたスコア、該本体部分に割り当てられたスコアおよび該ＵＲＬに割り当てられたスコアに基づいている、ことと、
該複合スコアに基づいて該メッセージを分類することと
をさらに含む、請求項１９に記載の方法。
【請求項２４】
電子メールメッセージを分類する方法であって、該電子メールメッセージを分類することが、フィシング詐欺に係る電子メールメッセージを分類することを含む、請求項１４に記載の方法。
【請求項２５】
電子メールメッセージを分類する方法であって、該電子メールメッセージを分類することが、不適切に商標を使用するものとして該電子メールメッセージを分類することを含む、請求項１４に記載の方法。
【請求項２６】
ウェブサイトを分類する方法であって、該方法は、
コンピュータが該ウェブサイト上の複数のテストを実行することと、
該コンピュータが該複数のテストの各々に基づいてスコアを割り当てることと、
該コンピュータが該複数のテストの各々に対するスコアに基づいて該ウェブサイトに複合スコアを割り当てることと、
該コンピュータが該複合スコアに基づいて該ウェブサイトを分類することと

を含む、方法。
【請求項２７】
ウェブサイトを分類する方法であって、前記複数のテストの少なくとも１つが、該ウェブサイトを参照するユニフォームリソースロケータに関する、請求項２６に記載の方法。
【請求項２８】
ウェブサイトを分類する方法であって、前記複数のテストの少なくとも１つが、該ウェブサイトの内容に関する、請求項２６に記載の方法。
【請求項２９】
ウェブサイトを分類する方法であって、複数のテストを実行することが、
該ウェブサイトと関連するドメインに対するＷＨＯＩＳ情報のセットを解析することを含む、請求項２６に記載の方法。
【請求項３０】
ウェブサイトを分類する方法であって、複数のテストを実行することが、
該ウェブサイトについての情報に対する反不正使用情報のソースを検索することを含む、請求項２６に記載の方法。
【請求項３１】
ウェブサイトを分類する方法であって、複数のテストを実行することが、
該ウェブサイトをホストするサーバの地理的な位置を決定することを含む、請求項２６に記載の方法。
【請求項３２】
ウェブサイトを分類する方法であって、複数のテストを実行することが、
該ウェブサイトをホストするサーバが安全なプロトコルを実装するかどうかを評価することを含む、請求項２６に記載の方法。
【請求項３３】
ウェブサイトを分類する方法であって、複数のテストを実行することが、
該ウェブサイトをホストするサーバに関するアクティブなポートのセットを検証することを含む、請求項２６に記載の方法。
【請求項３４】
ウェブサイトを分類する方法であって、複数のテストを実行することが、
該ウェブサイトからのウェブページをダウンロードすることを含む、請求項２６に記載の方法。
【請求項３５】
ウェブサイトを分類する方法であって、複数のテストを実行することが、
ウェブページがオンライン形態を実施するかどうかを決定するために該ウェブページを解析することを含む、請求項３４に記載の方法。
【請求項３６】
ウェブサイトを分類する方法であって、複数のテストを実行することが、
ユーザからの個人情報を要求するかどうかを決定するために前記オンライン形態を解析することを含む、請求項３５に記載の方法。
【請求項３７】
ウェブサイトを分類する方法であって、複数のテストを実行することが、
スペリングまたは文法におけるエラーについて該ウェブサイトを解析することを含む、請求項３４に記載の方法。
【請求項３８】
ウェブサイトを分類する方法であって、複数のテストを実行することが、
該ウェブサイト上のユニフォームリソースロケータ（「ＵＲＬ」）を識別することと、
該識別されたＵＲＬが該ウェブサイトに外在するリソースを参照するかどうかを決定するために、該識別されたＵＲＬを解析することと
を含む、請求項３４に記載の方法。
【請求項３９】

ウェブサイトを分類する方法であって、該ウェブサイトに外在するリソースが、合法的なウェブサイトによりホストされる画像および合法的なウェブサイトによりホストされるウェブページからなるグループから選ばれたリソースを含む、請求項３８に記載の方法。

【請求項４０】

ウェブサイトを分類する方法であって、複数のテストを実行することが、

ウェブページの表現を生成することを含む、請求項３４に記載の方法。

【請求項４１】

ウェブサイトを分類する方法であって、複数のテストを実行することが、

ウェブページの記憶された表現と該ウェブページの表現とを比較することを含む、請求項４０に記載の方法。

【請求項４２】

ウェブサイトを分類する方法であって、該ウェブサイトの表現が、該ウェブページから計算されたハッシュ値を含む、請求項４０に記載の方法。

【請求項４３】

ウェブサイトを分類する方法であって、該ウェブサイトの表現が、該ウェブページから計算されたチェックサムを含む、請求項４０に記載の方法。

【請求項４４】

非合法である可能性があるドメインとしてドメインを分類する方法であって、該方法は、

コンピュータが該ドメインと関連するドメインレジストレーション記録にアクセスすることと、

該ドメインに関する複数のテストを実行することと、

複数のテストの各々のために、複数のスコアが該ドメインに割り当てられるように、該ドメインにスコアを割り当てることと、

該ドメインに対して複合スコアを割り当てることであって、該複合スコアは、該複数のスコアに基づいている、ことと、

該複合スコアに基づいて、該ドメインを非合法である可能性があるドメインとして分類することと

を含む、方法。

【請求項４５】

非合法である可能性があるドメインとしてドメインを分類する方法であって、複数のテストを実行することが、該ドメインと関連するウェブサイトをホストするサーバに関する少なくとも１つのテストを実行することを含む、請求項４４に記載の方法。

【請求項４６】

非合法である可能性があるドメインとしてドメインを分類する方法であって、複数のテストを実行することが、

該ドメインと関連するウェブサイトを識別することと、

該ウェブサイトと関連するインターネットプロトコル（「ＩＰ」）アドレスを識別することと、

該ドメインに割り当てられたＩＰブロックを識別することと、

該ＩＰアドレスと該ドメインに割り当てられたＩＰブロックとを比較することと

を包含する、請求項４４に記載の方法。

【請求項４７】

非合法である可能性があるドメインとしてドメインを分類する方法であって、

該ドメインに関する複数のテストを実行することが、該ドメインの所有者を評価することを含む、請求項４４に記載の方法。

【請求項４８】

非合法である可能性があるドメインとしてドメインを分類する方法であって、

該ドメインに関する複数のテストを実行することが、該ドメインの所有者と該ドメイン名と同じ商標の所有者とを比較することとを含む、請求項４７に記載の方法。

【請求項４９】
非合法である可能性があるドメインとしてドメインを分類する方法であって、
該ドメインに関する複数のテストを実行することが、該ドメインと関連するＷＨＯＩＳ情報のセットを評価することを含む、請求項４４に記載の方法。
【請求項５０】
非合法である可能性があるドメインとしてドメインを分類する方法であって、
該ドメインに関する複数のテストを実行することが、該ドメインと関連するドメイン名システム（「ＤＮＳ」）情報のセットを評価することを含む、請求項４４に記載の方法。
【請求項５１】
非合法である可能性があるドメインとしてドメインを分類する方法であって、
該ドメインに関する複数のテストを実行することが、該ドメインと関連するウェブサイトを解析することを含む、請求項４４に記載の方法。
【請求項５２】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、該方法は、
ウェブサイトを参照するユニフォームリソースロケータ（「ＵＲＬ」）を識別することと、
（ａ）該コンピュータが該ＵＲＬにより参照されたウェブサイトが起動中であることを検証することと、
（ｂ）該コンピュータが該ＵＲＬにより参照されたドメインについての情報を解析することと、
（ｃ）該コンピュータが該ＵＲＬのフォーマットを解析することと、
（ａ）、（ｂ）および（ｃ）の各々の結果に基づいて、詐欺である可能性があるウェブサイトとして該ＵＲＬにより参照されたウェブサイトを分類することと
を含む、方法。
【請求項５３】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、
該ＵＲＬにより参照されたドメインについての情報を解析することが、
該ドメインについてのドメイン名システム（「ＤＮＳ」）情報のセットを評価することと、
ＤＮＳ情報のセットを解析することと
を含む、請求項５２に記載の方法。
【請求項５４】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、
該ＵＲＬにより参照されたドメインについての情報を解析することが、
該ドメインについてのＷＨＯＩＳ情報のセットを評価することと、
該ＷＨＯＩＳ情報のセットを解析することと
を含む、請求項５２に記載の方法。
【請求項５５】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、前記ＵＲＬは、ディレクトリパスを含み、該ＵＲＬのフォーマットを解析することは、該ディレクトリパスを評価することを含む、請求項５２に記載の方法。
【請求項５６】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、
該ＵＲＬのフォーマットを解析することが、該ＵＲＬのコード化フォーマットを評価することを含む、請求項５２に記載の方法。
【請求項５７】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、該方法は、
該ＵＲＬにより参照されたウェブサイトをホストするサーバの地理的位置を決定するこ

とをさらに含む、請求項５２に記載の方法。
【請求項５８】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、
詐欺である可能性があるウェブサイトとして該ＵＲＬにより参照されたウェブサイトを分類することが、
（ａ）の結果に基づいて該ＵＲＬに第一のスコアを割り当てることと、
（ｂ）の結果に基づいて該ＵＲＬに第二のスコアを割り当てることと、
（ｃ）の結果に基づいて該ＵＲＬに第三のスコアを割り当てることと、
該第一のスコア、該第二のスコアおよび該第三のスコアに基づいて該ＵＲＬに複合スコアを割り当てること、
該複合スコアに基づいて該ＵＲＬにより参照されたウェブサイトを分類することと
を含む、請求項５２に記載の方法。
【請求項５９】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、該ウェブサイトは、ウェブページを含み、該方法は、
コンピュータが該ウェブサイトを参照するユニフォームリソースロケータ（「ＵＲＬ」）を解析することと、
コンピュータが該ウェブサイトをホストするサーバを解析することと、
該ウェブページを解析することと、
該ウェブサイトを参照するＵＲＬの解析、該ウェブサイトをホストするサーバの解析および該ウェブページの解析に基づいて、該ウェブサイトを詐欺である可能性があるドメインとして分類することと
を含む、方法。
【請求項６０】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、
該ウェブサイトを参照するＵＲＬを解析することが、
該ＵＲＬにより参照されたウェブサイトが起動中であることを検証することと、
該ＵＲＬにより参照されたドメインについての情報を解析することと、
該ＵＲＬのフォーマットを解析することと
を含む、請求項５９に記載の方法。
【請求項６１】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、
該ウェブサイトをホストするサーバを分析することが、
該ウェブサイトと関連するドメインに対するＷＨＯＩＳ情報のセットを解析することと、
該ウェブサイトをホストするサーバの地理的位置を決定することと、
該ウェブサイトをホストするサーバが安全なプロトコルを実装するかどうかを評価することと、
該ウェブサイトをホストするサーバ上の起動中のポートのセットを検証することと
のうちの少なくとも１つを含む、請求項５９に記載の方法。
【請求項６２】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、
該ウェブページを解析することが該ウェブページをダウンロードすることを含む、請求項５９に記載の方法。
【請求項６３】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類する方法であって、
該ウェブページを解析することが、
該ウェブページがオンライン形態を実施するかどうかを決定するために該ウェブページを解析することと、
該オンライン形態がユーザからの個人情報を要求するかどうかを決定するために、該ウ

ェブページに組み込まれたオンライン形態を解析することと、
スペリングまたは文法のエラーについて該ウェブページを解析することと、
前記識別されたＵＲＬが該ウェブサイトに外在するリソースを参照するかどうかを決定するために、該ウェブページに組み込まれたユニフォームリソースロケータ（「ＵＲＬ」）を解析することと、
該ウェブページの表現とウェブページの記憶された表現とを比較することと
のうちの少なくとも１つをさらに含む、請求項６２に記載の方法。
【請求項６４】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類するコンピュータシステムであって、該コンピュータシステムは、プロセッサと、以下：
該ウェブサイトと関連するデータのセットにアクセスすることと、
該データのセットを複数のコンポーネントに分割することと、
該複数のコンポーネントの少なくとも幾つかを解析することと、
該解析されたコンポーネントの各々にスコアを割り当てることであって、該スコアは、複数のスコアが割り当てられるように、該解析されたコンポーネントの各々の解析に基づいている、ことと、
該データのセットに複合スコアを割り当てることであって、該複合スコアが該複数のスコアに基づいている、ことと、
該複合スコアに基づいて、該ウェブサイトを詐欺である可能性があるウェブサイトとして分類することと
を該プロセッサによって実行可能な命令とを含む、コンピュータシステム。
【請求項６５】
電子メールメッセージを分類するためのコンピュータシステムであって、該コンピュータシステムは、プロセッサと、以下：
該電子メールメッセージを複数のコンポーネントに分割することと、
該複数のコンポーネントの少なくとも１つを解析することと、
該複数のコンポーネントの少なくとも１つの解析に基づいて、スコアを該複数のコンポーネントの少なくとも１つに割り当てることと、
該複数のコンポーネントの少なくとも１つに割り当てられたスコアに基づいて該電子メールメッセージを分類することと
を該プロセッサによって実行可能な命令とを含む、コンピュータシステム。
【請求項６６】
ウェブサイトを分類するためのコンピュータシステムであって、該コンピュータシステムは、プロセッサと、以下：
該ウェブサイトに関する複数のテストを実行することと、
該複数のテストの各々にスコアを割り当てることと、
複数のテストの各々に対するスコアに基づいて、該ウェブサイトに複合スコアを割り当てることと、
該複合スコアに基づいて該ウェブサイトを分類することと
を該プロセッサによって実行可能な命令とを含む、コンピュータシステム。
【請求項６７】
非合法である可能性があるドメインとしてドメインを分類するコンピュータシステムであって、該コンピュータシステムは、プロセッサと、以下：
ドメインレジストレーションにアクセスすることと、
該ドメインに関する複数のテストを実行することと、
該複数のテストのために、該ドメインに複数のスコアが割り当てられるように、該ドメインにスコアを割り当てることと、
該ドメインに複合スコアを割り当てることであって、該複合スコアが複数のスコアに基づいている、ことと、
該複合スコアに基づいて、該ドメインを非合法である可能性があるドメインとして分類

することと
を該プロセッサによって実行可能な命令とを含む、コンピュータシステム。
【請求項６８】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類するコンピュータシステムであって、該コンピュータシステムは、プロセッサと、以下：
ウェブサイトを参照するユニフォームリソースロケータ（「ＵＲＬ」）を識別することと、
（ａ）該ＵＲＬにより参照されたウェブサイトが起動中であることを検証することと、
（ｂ）該ＵＲＬにより参照されたドメインについての情報を解析することと、
（ｃ）該ＵＲＬのフォーマットを解析することと、
（ａ）、（ｂ）および（ｃ）の各々の結果に基づいて、詐欺である可能性があるウェブサイトとして該ＵＲＬにより参照されたウェブサイトを分類することと
を該プロセッサによって実行可能な命令とを含む、コンピュータシステム。
【請求項６９】
詐欺である可能性があるウェブサイトとしてウェブサイトを分類するコンピュータシステムであって、該ウェブサイトは、ウェブページを含み、該コンピュータシステムは、プロセッサと、以下：
該ウェブサイトを参照するユニフォームリソースロケータ（「ＵＲＬ」）を解析することと、
該ウェブサイトをホストするサーバを解析することと、
該ウェブページを解析することと、
該ウェブサイトを参照するＵＲＬの解析、該ウェブサイトをホストするサーバの解析および該ウェブページの解析に基づいて、該ウェブサイトを詐欺である可能性があるウェブサイトとして分類することと
を該プロセッサによって実行可能な命令とを含む、コンピュータシステム。
【請求項７０】
コンピュータ可読媒体上に組み込まれたソフトウェアプログラムであって、該ソフトウェアプログラムが、以下：
ウェブサイトと関連するデータのセットにアクセスすることと、
該データのセットを複数のコンポーネントに分割することと、
該複数のコンポーネントの少なくとも幾つかを解析することと、
該解析されたコンポーネントの各々にスコアを割り当てることであって、該スコアは、複数のスコアが割り当てられるように、該解析されたコンポーネントの各々の解析に基づいている、ことと、
該データのセットに複合スコアを割り当て、該複合スコアが該複数のスコアに基づく、ことと、
該複合スコアに基づいて、該ウェブサイトを詐欺である可能性があるウェブサイトとして分類することと
を１つ以上のコンピュータによって実行可能な命令とを含む、ソフトウェアプログラム。
【請求項７１】
コンピュータ可読媒体上に組み込まれたソフトウェアプログラムであって、該ソフトウェアプログラムが、以下：
電子メールメッセージを複数のコンポーネントに分割することと、
該複数のコンポーネントの少なくとも１つを解析することと、
該複数のコンポーネントの少なくとも１つの解析に基づいて、該複数のコンポーネントの少なくとも１つにスコアを割り当てることと、
該複数のコンポーネントの少なくとも１つに割り当てられたスコアに基づいて、該電子メールメッセージを分類することと
を１つ以上のコンピュータによって実行可能な命令とを含む、ソフトウェアプログラム

。
【請求項７２】
コンピュータ可読媒体上に組み込まれたソフトウェアプログラムであって、該ソフトウェアプログラムが、以下：
該ウェブサイトに関する複数のテストを実行することと、
複数のテストの各々にスコアを割り当てることと、
該複数のテストの各々に対するスコアに基づいて該ウェブサイトに複合スコアを割り当てることと、
該複合スコアに基づいて該ウェブサイトを分類することと
を１つ以上のコンピュータによって実行可能な命令とを含む、ソフトウェアプログラム
。
【請求項７３】
コンピュータ可読媒体上に組み込まれたソフトウェアプログラムであって、該ソフトウェアプログラムが、以下：
ドメインレジストレーションにアクセスすることと、
該ドメインレジストレーションと関連するドメインに関する複数のテストを実行することと、
複数のテストの各々のために、複数のスコアが該ドメインに割り当てられるように、該ドメインにスコアを割り当てることと、
該ドメインに対して複合スコアを割り当てることであって、該複合スコアは、該複数のスコアに基づいている、ことと、
該複合スコアに基づいて、該ドメインを非合法である可能性があるドメインとして分類することと
を１つ以上のコンピュータによって実行可能な命令とを含む、ソフトウェアプログラム
。
【請求項７４】
コンピュータ可読媒体上に組み込まれたソフトウェアプログラムであって、該ソフトウェアプログラムが、以下：
ウェブサイトを参照するユニフォームリソースロケータ（「ＵＲＬ」）を識別することと、
（ａ）該ＵＲＬにより参照されたウェブサイトが起動中であることを検証することと、
（ｂ）該ＵＲＬにより参照されたドメインについての情報を解析することと、
（ｃ）該ＵＲＬのフォーマットを解析することと、
（ａ）、（ｂ）および（ｃ）の各々の結果に基づいて、詐欺である可能性があるウェブサイトとして該ＵＲＬにより参照されたウェブサイトを分類することと
を１つ以上のコンピュータによって実行可能な命令とを含む、ソフトウェアプログラム
。
【請求項７５】
コンピュータ可読媒体上組み込まれたソフトウェアプログラムであって、該ソフトウェアプログラムが、以下：
ウェブサイトを参照するユニフォームリソースロケータ（「ＵＲＬ」）を解析することであって、該ウェブサイトは、ウェブページを含む、ことと、
該ウェブサイトをホストするサーバを解析することと、
該ウェブページを解析することと、
該ウェブサイトを参照するＵＲＬの解析、該ウェブサイトをホストするサーバの解析および該ウェブページの解析に基づいて、該ウェブサイトを詐欺である可能性があるウェブサイトとして分類すること
を１つ以上のコンピュータによって実行可能な命令とを含む、ソフトウェアプログラム
。
【請求項７６】

ウェブサイトと関連するデータのセットにアクセスするための手段と、
該データのセットを複数のコンポーネントに分割するための手段と、
該複数のコンポーネントのうちの少なくとも幾つかを解析するための手段と、
該解析されたコンポーネントの各々にスコアを割り当てる手段であって、複数のスコアが割り当てられるように、該スコアが該解析されたコンポーネントの各々の解析に基づいている、手段と、
該データのセットに複合スコアを割り当てる手段であって、該複合スコアが該複数のスコアに基づいている、手段と、
該複合スコアに基づいて、該ウェブサイトを詐欺である可能性があるウェブサイトとして分類するための手段と
を含む、システム。

【請求項７７】
電子メールメッセージを複数のコンポーネントに分割するための手段と、
該複数のコンポーネントの少なくとも１つを解析するための手段と、
該複数のコンポーネントの少なくとも１つの解析に基づいて、該複数のコンポーネントの少なくとも１つにスコアを割り当てるための手段と、
該複数のコンポーネントの少なくとも１つに割り当てられたスコアに基づいて、該電子メールメッセージを分類するための手段と
を含む、システム。

【請求項７８】
該ウェブサイトに関する複数のテストを実行するための手段と、
該複数のテストの各々にスコアを割り当てるための手段と、
該複数のテストの各々に対するスコアに基づいて該ウェブサイトに複合スコアを割り当てるための手段と、
該複合スコアに基づいて該ウェブサイトを分類するための手段と
を含む、システム。

【請求項７９】
ドメインレジストレーションにアクセスするための手段と、
該ドメインレジストレーションと関連するドメインに関する複数のテストを実行するための手段と、
該複数のテストの各々のために、複数のスコアが該ドメインに割り当てられるように、該ドメインにスコアを割り当てるための手段と、
該ドメインに対して複合スコアを割り当てる手段であって、該複合スコアが該複数のスコアに基づいている、手段と、
該複合スコアに基づいて、該ドメインを非合法である可能性があるドメインとして分類するための手段と
を含む、システム。

【請求項８０】
ウェブサイトを参照するユニフォームリソースロケータ（「ＵＲＬ」）を識別するための手段と、
（ａ）該ＵＲＬにより参照されたウェブサイトが起動中であることを検証するための手段と、
（ｂ）該ＵＲＬにより参照されたドメインについての情報を解析するための手段、
（ｃ）該ＵＲＬのフォーマットを解析するための手段と、
（ａ）、（ｂ）および（ｃ）の各々の結果に基づいて、詐欺である可能性があるウェブサイトとして該ＵＲＬにより参照されたウェブサイトを分類するための手段と
を含む、システム。

【請求項８１】
ウェブサイトを参照するユニフォームリソースロケータ（「ＵＲＬ」）を解析するための手段であって、該ウェブサイトは、ウェブページを含む、手段と、

該ウェブサイトをホストするサーバを解析するための手段と、
該ウェブページを解析するための手段と、
該ウェブサイトを参照するＵＲＬの解析、該ウェブサイトをホストするサーバの解析および該ウェブページの解析に基づいて、該ウェブサイトを詐欺である可能性があるウェブサイトとして分類するための手段と
を含む、システム。

【発明の詳細な説明】

【技術分野】

【０００１】

（著作権通知）

本特許書面の開示の一部は、著作権保護の対象となる材料（ｍａｔｅｒｉａｌ）を含む。著作権者は、特許商標庁の特許公開または記録に現れる特許書面または特許開示の、任意の人物によるファクシミリ複製に対して異議を有さないが、その他の場合には、全ての著作権のいかなる権利をも留保する。

【０００２】

（関連出願の引用）

本出願は、Ｓｈｒａｉｍ他によって、２００４年５月２日に出願され、「Ｏｎｌｉｎｅ Ｆｒａｕｄ Ｓｏｌｕｔｉｏｎ」と題された米国特許出願第１０／７０９，３９８号の一部係属出願であり、かつ該出願の利益を主張し、該出願の開示はその全体が本明細書において全ての目的のために参考として援用される。本出願はまた、以下の仮出願、すなわち、Ｓｈｒａｉｍ他によって、２００４年１０月４日に出願され、「Ｏｎｌｉｎｅ Ｆｒａｕｄ Ｓｏｌｕｔｉｏｎ」と題された米国特許仮出願第６０／６１５，９７３号と、Ｓｈｕｌｌによって、２００４年９月１７日に出願され、「Ｍｅｔｈｏｄｓ ａｎｄ Ｓｙｓｔｅｍｓ ｆｏｒ Ｐｒｅｖｅｎｔｉｎｇ Ｏｎｌｉｎｅ Ｆｒａｕｄ」と題された米国特許仮出願第６０／６１０，７１４号と、Ｓｈｕｌｌによって、２００４年９月１７日に出願され、「Ｃｕｓｔｏｍｅｒ－Ｂａｓｅｄ Ｄｅｔｅｃｔｉｏｎ ｏｆ Ｏｎｌｉｎｅ Ｆｒａｕｄ」と題された米国特許仮出願第６０／６１０，７１５号との利益を主張し、これらの仮出願の開示はその全体が本明細書において全ての目的のために参考として援用される。

【０００３】

本出願はまた、共有に係る同時係属中の以下の出願でも関連し、これらの出願の各々は、本出願と同日に出願され、本明細書において、全ての目的のために参考として援用される。これらの出願とは、すなわち、Ｓｈｒａｉｍ他により出願され「Ｏｎｌｉｎｅ Ｆｒａｕｄ Ｓｏｌｕｔｉｏｎ」（代理人整理番号第０４０２４６－０００１２０ＵＳ号）と題された米国特許出願第－－／－－－－－－号と、Ｓｈｕｌｌ他により出願され「Ｅｎｈａｎｃｅｄ Ｒｅｓｐｏｎｓｅｓ ｔｏ Ｏｎｌｉｎｅ Ｆｒａｕｄ」（代理人整理番号第０４０２４６－０００５１０ＵＳ号）と題された米国特許出願第－－／－－－－－－号と、Ｓｈｕｌｌ他により出願され「Ｃｕｓｔｏｍｅｒ－Ｂａｓｅｄ Ｄｅｔｅｃｔｉｏｎ ｏｆ Ｏｎｌｉｎｅ Ｆｒａｕｄ」（代理人整理番号第０４０２４６－０００６１０ＵＳ号）と題された米国特許出願第－－／－－－－－－号と、Ｓｈｕｌｌ他により出願され「Ｅａｒｌｙ Ｄｅｔｅｃｔｉｏｎ ｏｆ Ｏｎｌｉｎｅ Ｆｒａｕｄ」（代理人整理番号第０４０２４６－０００７００ＵＳ号）と題された米国特許出願第－－／－－－－－－号と、Ｓｈｕｌｌ他により出願され「Ｅｎｈａｎｃｅｄ Ｒｅｓｐｏｎｓｅｓ ｔｏ Ｏｎｌｉｎｅ Ｆｒａｕｄ」（代理人整理番号第０４０２４６－０００８００ＵＳ号）と題された米国特許出願第－－／－－－－－－号と、Ｓｈｕｌｌ他により出願され「Ｇｅｎｅｒａｔｉｎｇ Ｐｈｉｓｈ Ｍｅｓｓａｇｅｓ」（代理人整理番号第０４０２４６－００１２００ＵＳ号）と題された米国特許出願第－－／－－－－－－号と、Ｓｈｕｌｌ他により出願され「Ａｄｖａｎｃｅｄ Ｒｅｓｐｏｎｓｅｓ ｔｏ Ｏｎｌｉｎｅ Ｆｒａｕｄ」（代理人整理番号第０４０２４６－００１３００ＵＳ号）と題された米国特許出願第－－／－－－－－－号、である。

【０００４】
（技術分野）
本発明は、コンピュータシステムに関し、より詳細には、オンライン詐欺を検出する、防止する、オンライン詐欺に応答する、および／または、あるいはオンライン詐欺に対処するための、システム、方法およびソフトウェアに関する。
【背景技術】
【０００５】
電子メール（「ｅｍａｉｌ」）は、現代の通信の重要商品になっている。しかしながら、不幸にも、通常のベースで電子メールを使用する任意の人物は、様々な広告主からほぼ全ての電子メールアドレスに送信される大量の「スパム」（望まれない（ｕｎｓｏｌｉｃｉｔｅｄ）電子メール）に日常接している。伝統的な紙の「ジャンクメール（ｊｕｎｋｍａｉｌ）」にどこか類似しているが、スパムは、実質的にコストがかからないという点と、スパム提供者（「スパムメール送信者」）が、莫大な数のスパムを簡単かつ素早く生成し得、かつ伝送し得るという点で独特である。さらに、インターネット規格のシンプルメール転送プロトコル（「ＳＭＴＰ」）における制限は、スパムメール送信者に比較的匿名で、結果として、相応して低い責任能力でスパムを送信可能にする。結果として、スパムは大多数の受信者を苛立たせ、また、伝送されたスパムの量に対して、スパムメール送信者にとっては、わずかな成功の売り上げ機会を生み出すにすぎないものの、スパム「産業」は急激に発展している。安価にかつ素早く大量のスパムを送信するためのスパムの能力を与えられ、スパムメール送信者は、スパム広告の比較的に低い応答率からでさえ、かなりの利益を上げ得る。
【０００６】
それらの特性として、スパムメール送信者はスパムを送信するための新しい受信者（犠牲者）を継続的に検索する。スパム「産業」は、それゆえ、「ハーベスタ（ｈａｒｖｅｓｔｅｒ）」という派生的な産業を生み出した。「ハーベスタ」は有効な電子メールアドレスのリストを生成するためにインターネットおよび他の供給源を捜し回り、次いでスパムメール送信者に売る。（明らかに、これらの活動は協力して行われるので、多くのスパムメール送信者は、彼ら自身のため、または仲間のスパムメール送信者のためにハーベスタとして活動する）。ハーベスタは電子メールアドレスリストを取得するための種々の手法を使用し、しばしば、継続的に新しい電子メールアドレスを求めてインターネットをうろつく自動検索プログラム（一般的には「ロボット（ｒｏｂｏｔ）」または「ウェブクローラ（ｗｅｂｃｒａｗｌｅｒ）」と呼ばれる）を開発する。例えば、ハーベスタは、その上でユーザがフィードバックなどのために通常電子メールアドレスを提供する、インターネット（および他の）ニュースグループ、チャットルーム、およびディレクトリサービス（例えば、ホワイトページ）サイト、ならびにメッセージボード、メーリングリストおよびウェブページから電子メールアドレスを取得する。
【０００７】
マーケティング手法としてのスパムの成功は、「フィッシング」操作を行うためにスパムを使用するという結果を生じ始める。フィッシング操作は、消費者に、彼／彼女が他の場合にはとらない行動をとらせる、任意のタイプの社会工学のアタック（典型的にブランド名の不正使用に頼る）として定義され得る。フィッシング詐欺は、わいろ（ｂｒｉｂｅｒｙ）、お世辞（ｆｌａｔｔｅｒｙ）、欺き（ｄｅｃｅｉｔ）、甘言を弄すこと（ｃａｊｏｌｉｎｇ）によって、および他の方法を介して操作し得る。フィッシング操作は、しばしば消費者への大量コンタクト（例えば、「スパム」電子メールメッセージ、テキストメッセージ、ＶｏＩＰコール、インスタントメッセージなどによって、ならびに他のデバイスを介して）を含み、一般的にはコンタクトされた消費者を応答サイトへ向けさせ、応答サイトはしばしばウェブサイトであり、しかしまたは電話番号などであり得る。
【０００８】
フィッシング詐欺の１つのかなり一般的な例は、非常に低い値段で周知のソフトウェアアプリケーションまたはパッケージ（これらは、実際には著作権侵害されたか、またはそ

うでなければ不正に取得されたものである）を広告し、およびソフトウェアが購入され得るウェブサイトへ応答者を向けるスパム電子メールメッセージである。そのサイトを訪問すると、広告された値段がひどく非現実的であり、おそらく以前の違法行為を指示する（例えば、ブラックマーケットまたはグレイマーケットの商品）ことを、消費者は知る（または知るべきである）。しかしながら、一部の消費者は、無知から、または故意の盲目からのいずれかで、ソフトウェアが正当であるという、フィッシュメール送信者の保証を受容し、結果として不正なソフトウェアを購入し、フィッシング詐欺を完了する。

【０００９】

別の一般的なフィッシング操作は「スプーフィング」詐欺として周知である。この実行は、電子メールメッセージの「Ｆｒｏｍ：」または「Ｒｅｐｌｙ－ｔｏ：」ヘッダに偽の電子メールアドレスを挿入することを含み、このことにより、相対的に信頼できる供給源から電子メールが発生されたと信じるように受信者を誤解させる。スプーフされた電子メールメッセージは、しばしば周知のインターネットサービスプロバイダ（「ＩＳＰ」）（例えば、Ａｍｅｒｉｃａ Ｏｎｌｉｎｅ™およびＴｈｅ Ｍｉｃｒｏｓｏｆｔ Ｎｅｔｗｏｒｋ™）、または容易に識別可能な電子メールアドレスを有する他の注目を集める実体（ｅｎｔｉｔｙ；例えば、ＩＢＭ™、Ｍｉｃｒｏｓｏｆｔ™、Ｇｅｎｅｒａｌ Ｍｏｔｏｒｓ™およびＥ－Ｂａｙ™、ならびにさまざまな金融機関、オンライン小売業および同様のもの）からであることを装う。このスプーフィングは、スプーフィングが顧客の混乱を引き起こし、非常に洗練されたオンラインの存在の価値を破壊し、スプーフされたブランドの一般的な不信を生成し、評判の良い実体のオンライン通信およびオンライン取引の価値を大きく弱めるというだけではなく、多くの理由においてこれらの実体に受容不能である。

【００１０】

さらに、多くの場合には、スパムメール送信者および／またはスプーフメール送信者は彼らの「産業」の中で情報を広める手段（メッセージボード、チャットルーム、ニュースグループおよび同様のもののような種々のオンラインフォーラムを含む）を発展させる。このような位置において、スパムメール送信者はしばしばさらに効果的なスパム送信／スプーフィング、新しいスプーフサイトなど、ならびに収集されたアドレスのリストの取引および／または広告するための戦略を議論する。これらのリソースを用いることによって、スパムメール送信者および／またはスプーフメール送信者は、最も効果的なスパム送信／スプーフィング手法に焦点を当て得、他のスプーフされたウェブサイトおよび同様なものから学び得および／またはコピーし得る。このようなリソースはまた、効果的なスパム送信／スプーフィング手法を素早く選び取ることを新しいスパムメール送信者またはスプーフ送信者に可能にする。

【００１１】

可能性としては、大変不安になるが、スパム（特にスプーフされたスパム）は、フィッシングアタックのような詐欺的な活動（アイデンティティの窃盗、認証されないクレジットカードの取引および／またはアカウントからの預金引き出しなどを含む）を促進するためにますます使用され得る。この手法は、信頼できる会社を装うことを含み、しばしばアカウント情報をアップデートするため、オンライン取引などを確認するため、などと称する要求に応答して、疑いを知らない消費者に秘密の個人情報を提供させる。単なる例として、スプーフメール送信者は、受信者の銀行からであると称する、および受信者が詐欺的なウェブサイトに対し電子メールを返信、またはログオンすることによって個人情報を提供することによって受信者のアイデンティティを「確認」する（皮肉な）要求をするスプーフ電子メールを送信し得る。同様に、通常のスプーフのメッセージは、受信者が周知の電子商取引サイトにログオンし、そのサイトによって記憶されるクレジットカード情報を「アップデートする」ことを要求する。

【００１２】

スパムメッセージ（特にフィッシングスキームの一部であるスパムメッセージ）はしばしば、フィッシュメール送信者のウェブサイトにリンクするユニフォームリソースロケー

タ（「ＵＲＬ」）を含む。例えば、ウェブサイトは、不正な商品を販売するための応答ポイントであり得る。他の場合には、ＵＲＬはスプーフされた送信者のウェブサイトに関連するように考えられるように構成され得るが、実際には受信者をスプーフされたウェブサイト（すなわち、電子メールのスプーフされた供給源のウェブサイトを真似する、または該ウェブサイトに似るように設計されるウェブサイト）へとあて先変更し得る。スプーフされたウェブサイトを訪問することで、受信者は情報（受信者の住所、電話番号、社会保障番号、銀行のアカウント番号、クレジットカード番号、母の旧姓など）を要求するフォームを示され得る。信頼できる会社と通信していると信じている受信者は、この情報の一部または全てを提供し得、次いで情報は任意の不正な種々の目的のために使用するためにスパムメールを送信する人物の自由になる。（一部の場合には、フィッシュ送信者によって収集される個人情報などを提供する命令を有する正当なウェブサイト上に示される不正なおよび／またはスプーフされたポップアップウィンドウを有する、正当なウェブサイトを示すように、リンクが構成され得る）。

【００１３】

かくして、フィッシング詐欺および他の不正なオンライン活動が繁栄している。このような活動は、明らかに違法であり、不道徳である。フィッシュメールを送信する人物の相対的な匿名性、ならびにインターネットの国際性は、これらの活動の効果的な法的告発を妨げる。単なる例として、詐欺的なウェブサイトに関連するサーバは、告発／犯人の引き渡し（ｅｘｔｒａｄｉｔｉｏｎ）がかなり起こりにくい国に配置され得る。さらに、詐欺的なウェブサイトはしばしばかなり一時的なものであり、フィッシュメールを送信する人物が新しいサーバまたはＩＳＰに移動するまでに、所与のサーバまたはＩＳＰに短い時間（可能性としてはおよそ数日、または数時間のみでさえ）存在する。詐欺的なウェブサイトをホストする多くのサーバが、フィッシュメールを送信する人物またはその仲間によって既に危険にされた（または「ハックされた」）合法的なウェブサイトであり、サーバの所有者／操作者は、サーバが不正な目的のためにひそかに使用されていることを知らないままであるという事実が、実施の問題を複雑にする。

【００１４】

従って、これらの不正使用を扱うための効果的な解決策が必要である。

【発明の開示】

【課題を解決するための手段】

【００１５】

本発明の様々な実施形態は、データを解析するための方法、システムおよびソフトウェアを提供する。例えば、特定の実施形態においては、ウェブサイトについてのデータのセットが、ウェブサイトが不正である（例えば、フィッシング詐欺、グレイマーケットの商品の販売などのような詐欺的なスキームに包含される）可能性があるかを決定するために解析され得る。例示的な実施形態においては、データのセットは複数のコンポーネントに分割され得る（これらの各々は、一部の場合には、個別のデータセットと考えられ得る）。単なる例として、データのセットは複数のデータ供給源から集められたデータを備え得、および／または各コンポーネントは複数のデータ供給源の１つから集められたデータを備え得る。別の例として、データのセットは複数のセクションを有するドキュメントを備え得、各コンポーネントは複数のセクションの１つを備え得る。当業者は、特定のコンポーネントの解析はあるテストおよび／または評価を備え得ること、また別のコンポーネントの解析は異なるテストおよび／または評価を備え得ることを認識する。他の場合には、各コンポーネントの解析は類似のテストおよび／または評価を備え得る。種々のテストおよび／または評価は一般には、インプリメンテーション特有であり得る。

【００１６】

実施形態の一セットは方法を提供し、方法の一部または全部はコンピュータによって行われ得る。単なる例として、一部の実施形態は、データを解析するための方法を提供する。例示的な実施形態は、詐欺の可能性のあるウェブサイトとして、ウェブサイトを分類する方法を提供する。方法はウェブサイトに関連するデータのセットにアクセスするコンピ

ュータを備え得る。データのセットの例は、ウェブサイトに関連する電子メールメッセージ（例えば、ウェブサイトを参照するＵＲＬを備える電子メールメッセージ、ウェブサイトについて議論する電子メールメッセージなど）、ウェブサイトに関連するドメインについてのデータのセット、ウェブサイトをホストするサーバについてのデータのセット、および／またはウェブサイト、ニュースグループの更新、ウェブページ、インターネットチャットセッションの表現形式などを参照するＵＲＬについてのデータのセット、を含むがこれらに限定はされない。データのセットのタイプに依存して、データのセットへのアクセスは種々の手順（例えば、電子メールメッセージを受信すること、サーバに問い合わせをすること、ドメインレジストレーションゾーンファイルにアクセスすることなど）を含み得る。

【００１７】

例示的な方法はデータのセットを複数のコンポーネントに分割すること、および／または複数のコンポーネントの少なくとも一部を解析することをさらに含み得る。特定の実施形態においては、可能性としては解析されたコンポーネントの各々の解析に基づいて、スコアが複数のコンポーネントの各々に割り当てられ得る。それゆえに、複数のスコアが割り当てられ得る。次いで、ある実施形態においては、複合のスコア（これは複数のスコアうちの１つ、一部、または全てに基づき得る）が、データのセットに割り当てられ得る。ウェブサイトは、次いで、分類され得る。一部の場合には、ウェブサイトの分類は複数のスコアのうちの１つ（または１つ以上）に基づき得る。他の場合には、分類は複合のスコアに基づき得、複合のスコアは上記されるように割り当てられ得る。

【００１８】

他の実施形態は電子メールメッセージを解析する方法を提供する。例示的な実施形態は電子メールメッセージを複数のコンポーネントに分割するコンピュータを備える。コンピュータは複数のコンポーネントの少なくとも１つを解析し得、（可能性としては複数のコンポーネントの少なくとも１つの解析に基づいて）、複数のコンポーネントの少なくとも１つにスコアを割り当て得る。可能性としてはスコアに基づいて、電子メールメッセージは分類され得る。

【００１９】

一部の実施形態に従って、コンピュータは複数のコンポーネントの各々を解析し得る。複数のコンポーネントの各々に対して、コンピュータはコンポーネントにスコアを割り当て得る。複数のコンポーネントに各々に割り当てられるスコアに基づいて、複合のスコアが電子メールメッセージに割り当てられ得る。このような場合には、電子メールメッセージを分類することは、複合のスコアに基づいて電子メールメッセージを分類することを含み得る。例示的な方法は電子メールメッセージを、フィッシング詐欺（および／または他のオンライン詐欺）に包含されている、商標を不適切に使用している、などとして分類するために使用され得る。

【００２０】

特定の実施形態においては、電子メールメッセージはヘッダ部分、本体部分および／またはＵＲＬ（これらの各々は、一部の場合には電子メールメッセージのコンポーネントと考慮され得る）を備え得る。それゆえ、ヘッダ部分は解析され得、および／またはスコアが割り当てられ得る。本体部分は解析され得、および／またはスコアが割り当てられ得る。ならびに／もしくはＵＲＬは解析され得、および／またはスコアが割り当てられ得る。一部の場合には、スコアリングは、例えば、本体部分はヘッダ部分がある閾値を超える場合に限り解析され、同様にＵＲＬはヘッダ部分および／または本体部分のそれぞれのスコア（および／またはヘッダ部分に対するスコアおよび本体部分に対するスコアに基づく結合スコア）がある閾値スコアを超える場合に限り解析され得るという点において、本質的に段階的であり得る。複合のスコアは電子メールメッセージに（例えば、ヘッダ部分、本体部分、および／またはＵＲＬに対するスコアに基づいて）割り当てられ得、および／または電子メールメッセージは複合のスコアに基づいて分類され得る。

【００２１】

さらなる実施形態はウェブサイトを分類する方法を提供し得る。単なる例として、このような一方法は、ウェブサイト上で複数のテストを行うこと、テストの各々に基づいてスコアを割り当てること、複数のテストの各々に基づいて複合のスコアを割り当てること、および／またはウェブサイトを分類すること（可能性としては、複合のスコアに基づいて）を含み得る。テストは種々の要因に関連し得る。単なる例として、１つ以上のテストはウェブサイト、ウェブサイトのコンテンツ、ウェブサイトのウェブページなどを参照するＵＲＬと関連し得る。

【００２２】

ＵＲＬを解析（上記したように、ウェブサイトを参照するＵＲＬ上でテストを行うために使用され得る）する例示的な方法は、ウェブサイトを参照するユニフォームリソースロケータ（「ＵＲＬ」）を識別することを備え得る。方法は、ＵＲＬによって参照されるウェブサイトが稼動中であることを検証すること、ＵＲＬによって参照されるドメインについての情報を解析すること、および／またはＵＲＬのフォーマットを解析することをさらに含み得る。これらの検証および解析の１つ以上の結果に基づいて、ＵＲＬによって参照されるウェブサイトは詐欺の可能性のあるウェブサイトとして分類され得る。ＵＲＬによって参照されるドメインについての情報の解析は、このようなウェブサイト（本明細書に記載される任意の解析を含むがこれに限定はされない）をホストするＵＲＬおよび／またはサーバに関連するウェブサイトを解析することを含み得る。ＵＲＬのフォーマットを解析することは、ＵＲＬのディレクトリパスを評価すること、ＵＲＬのコード化フォーマットすることを評価することなどを含み得る。方法はＵＲＬによって参照されるウェブサイトをホストするサーバの地理的な位置を決定することをさらに含み得る。

【００２３】

一部の場合には、スコアリングシステムはインプリメントされ得る。単なる例として、第一のスコアはウェブサイトが稼動中であることを検証することの結果に基づいて割り当てられ得、第二のスコアはＵＲＬによって参照されるドメインの解析に基づいて割り当てられ得、および／またはＵＲＬのフォーマットの解析に基づいて第三のスコアを割り当てる。複合のスコアはこれらのスコアの１つ以上に基づいて割り当てられ得、ならびに／もしくはＵＲＬによって参照されるウェブサイトは任意のこれらのスコアに基づいて、および／または複合のスコアに基づいて分類され得る。

【００２４】

ウェブサイトを詐欺の可能性のあるウェブサイトとして分類する別の方法は、ウェブサイトを参照するユニフォームリソースロケータ（「ＵＲＬ」）を解析することを含み得る。この解析は上記した任意のまたは全ての手順を含み得るが、これらに限定はされない。方法はウェブサイトをホストするサーバを解析することをさらに含み得る。ウェブサイトがウェブページを備える場合には、方法はウェブページを解析することをさらに含み得る。ウェブサイトを参照するＵＲＬの解析、ウェブサイトをホストするサーバの解析、および／またはウェブページの解析に基づいて、ウェブサイトは詐欺の可能性のあるウェブサイトとして分類され得る。

【００２５】

ウェブページを解析することは、以下の手順の１つ以上を含み得る。その手順は、すなわち、ウェブページをダウンロードすることと、ウェブページがオンラインフォームをインプリメントするかを決定するためにウェブページを解析することと、（例えば、オンラインフォームがユーザから個人情報を要求するかを決定するために）ウェブページに組み込まれたオンラインフォームを解析することと、スペルまたは文法におけるエラーのためにウェブページを解析することと、識別されたＵＲＬがウェブサイトの外部のリソースを参照するかを決定するためにウェブページに組み込まれたユニフォームリソースロケータ（「ＵＲＬ」）を解析することと、ウェブページの表現を記憶されたウェブページの表現と比較することと、である。

【００２６】

さらに、実施形態の別のセットは、ドメインを解析するための方法を提供する。例示的

な方法は、ドメインを詐欺の可能性のあるドメインと分類するために使用され得、該方法はドメインに関連するドメインレジストレーション記録（例えば、ゾーンファイルにおける記録）にアクセスすることを含む。方法は、ドメインに関連するサーバによってホストされるドメインおよび／またはウェブサイトに関する複数のテスト（上記したテストを含むがこれらに限定はされない）を行うことをさらに含み得る。複数のテストの各々に対して、スコアは可能性としては複数のテストの各々に対するスコアに基づいて、ドメインに割り当てられ得、および／または複合のスコアはドメインに割り当てられ得る。可能性としては複合のスコアに基づいて、ドメインは、不正である可能性のあるドメインとして分類され得る。

【００２７】

種々のテストが行われ得る。単なる例として、テストにおいて、ドメインに関連するウェブサイトは識別され得、ウェブサイトに関連するＩＰアドレスは識別され得、ドメインに関連するＩＰブロックは識別され得、および／またはＩＰブロックはＩＰアドレスと比較され得る。別のテストはドメインの所有者を評価すること、および／またはドメインの所有者とドメインの名前に類似する商標の所有者とを比較することとを備え得る。他の例においては、ＷＨＯＩＳおよび／またはＤＮＳ情報のセットが評価され得る。一部の場合には、１つ以上のテスト（上記したテストを含むがこれらに限定はされない）はドメインに関連するウェブサイトをホストするサーバ上で行われ得る。

【００２８】

実施形態の他のセットは、システムおよび／またはソフトウェアプログラム（本発明の方法を行うように構成されるシステムおよび／または本発明の方法を行うためのコンピュータによって実行可能な命令を備えるソフトウェアプログラムを含むがこれらに限定はされない）を提供する。単なる例として、例示的なシステムは、プロセッサと、上記した方法の１つ以上を行なうためのプロセッサによって実行可能な命令とを備える。別の例としてソフトウェアプログラム（コンピュータ読み取り可能な媒体上に具体化される）は、上記した方法の１つ以上を行うために１つ以上のコンピュータによって実行可能な命令を備え得る。

【発明を実施するための最良の形態】

【００２９】

本発明の性質および利点のさらなる理解は図面を参照することによって実現され得、図面は明細書の残りの部分に記載される。図面においては、同様の参照番号が類似の構成要素を示すためにいくつかの図面を通じて使用される。一部の例においては、小文字からなるサブラベルが、複数の類似の構成要素の１つを示すために参照番号に関連付けられる。実在するサブラベルを特定化することなく参照番号が参照された場合には、このような複数の類似構成要素全てを参照することを意図する。

【００３０】

（特定の実施形態の詳細な記載）

様々な実施形態に従った、システム、方法およびソフトウェアが、オンラインの詐欺、特に「フィッシング」操作に対抗するために提供される。「スプーフィング」詐欺として公知の例示的なフィッシング操作は、「スプーフされた」電子メールのメッセージを使用して、実際はサーバが消費者の個人情報へのアクセスを得るために、信頼されている加入者を装う別のパーティにより操作されているときに、疑いを知らない消費者に、違法な（ｉｌｌｉｃｉｔ）ウェブサイトへのアクセスをさせ、信頼される加入者（例えば、銀行、オンラインの小売業者など）によって操作されていると信じられるサーバに対して個人情報を提供させる。本明細書で使用される、用語「個人情報」は、個人を識別するために使用され得る、および／または通常はその人物により比較的信頼されている実体（ｅｎｔｉｔｙ）にのみ明らかにされる任意の情報を含むことが理解されるべきである。単なる例として、個人情報は金融機関の口座番号、クレジットカード番号、有効期限および／またはセキュリティコード（当該分野では時折「カード照合番号」、「カード照合値」、「カード照合コード」または「ＣＶＶ」という）、および／または他の金融の情報；ユーザＩＤ

、パスワード、母親の旧姓、および／または他のセキュリティ情報；フルネーム、住所、電話番号、社会保障番号、運転免許証番号、および／または他の識別情報を含み得るが、これらに限定はされない。

【００３１】

（１．概観）

本発明の特定の実施形態は、このようなスプーフされた電子メールメッセージを引き込み、メッセージが詐欺活動（および／またはスプーフされたメッセージを含む）を含む確率を見積もるためにメッセージを解析し、任意の識別された詐欺活動に対する応答を提供する、システム、方法および／またはソフトウェアを特徴として提示する。図１Ａは、これらの実施形態の一部に従ったオンラインの詐欺に対抗するために使用され得る例示的なシステム１００の機能的要素を図示しており、ある実施形態がどのように操作し得るかの一般的な概観を提供する。（様々な実施形態は、以下の追加の詳細において記載される）。図１Ａにより描かれる機能のアーキテクチャおよび各々の機能的構成要素に関して記載される手順は例示の目的のみのために提供され、本発明の実施形態は、特定の、機能的なまたは構造的なアーキテクチャに必ずしも限定されないことが注意されるべきである。本明細書に記載される様々な手順は任意の適切なフレームワークにおいて行われ得る。

【００３２】

多くの場合において、図１Ａのシステム１００は、詐欺防止サービス、セキュリティサービスなど（本明細書において「詐欺防止プロバイダ」という）によって、１人以上の顧客に対して操作され得る。しばしば、顧客は、模倣されている、偽造されている、および／またはスプーフされている危険がある製品、ブランドおよび／またはウェブサイトを有する実体である（例えば、オンライン小売人、金融機関、会社など）。しかしながら、他の場合には、詐欺防止プロバイダは、顧客ならびに／もしくは顧客に加盟している実体および／または顧客に組み込まれる実体（例えば、消費者のセキュリティ部門、情報サービス部門など）の使用人であり得る。

【００３３】

本発明の一部の実施形態に従って、システム１００は、種々のデータ供給源１０５を含み（および／またはアクセスし）得る。データ供給源１０５は、図解を簡略化するためにシステム１００の一部として描かれるが、当業者は、本明細書の開示に基づいて、データ供給源１０５はしばしば第三者によって独立に維持され、システム１００によってアクセスされ得ることを認識する。一部の場合には、あるデータ供給源１０５が、（例えば、システム１００によるより簡単なアクセスのために）ローカルに（適切に）転写および／またはコピーされ得る。

【００３４】

データ供給源１０５は、任意の供給源（１つ以上のチャットルーム１０５ａ、ニュースグループフィード１０５ｂ、ドメインレジストレーションファイル１０５ｃ、および／または電子メールフィード１０５ｄを含むがこれらに限定はされない）を備え得、任意の供給源からオンライン詐欺の可能性についてのデータが取得され得る。システム１００は、オンラインの詐欺の実例を検出するために、および／または本明細書で議論される詐欺防止の方法論の効率および／または効果を強化するために、任意のデータ供給源１０５から取得された情報を使用し得る。一部の場合には、システム１００（および／またはシステム１００の構成要素）は、関連情報を見出すために、可能性としてはスケジュールされたベースで（例えば、１０分ごとに１回、１日につき１回、１週間につき１回など）様々なデータ供給源を「クロール（ｃｒａｗｌ）」する（例えば、様々なデータ供給源を自動的にアクセスすることおよび／またはそこから情報を自動的にダウンロードすること）ように構成され得る。

【００３５】

単なる例として、新しいスパミング／スプーフィングスキームを議論するために、ならびに収集される電子メールアドレスのリストを売買するために共通に使用されるいくつかのニュースグループがある。このようなスキームを追跡する反不正使用（ａｎｔｉ－ａｂ

ｕｓｅ）ニュースグループもまた存在する。システム１００は、新しいスプーフ詐欺、新しい収集されたアドレスのリスト、収集されたアドレスの新しい供給源などについての情報を見出すために、任意の適用可能なニュースグループ１０５ｂにクロールするように構成され得る。一部の場合には、システム１００は、このようなクロールにおいて特定のキーワード（例えば、「フィッシュ」、「スプーフ」など）を検索するように構成され得る。他の場合には、ニュースグループはＵＲＬをスキャンされ得、ＵＲＬはダウンロードされ得（またはコピーされ得）およびさらなる解析に供され得る（例えば、以下に詳細にて記載するように）。加えて、上記したように、モニタされ得る１つ以上の反不正使用グループがあり得る。このような反不正使用ニュースグループは、しばしば、発見された新しい詐欺を列挙し、および／またはこのような詐欺にＵＲＬを提供する。結果として、このような反不正使用グループはモニタされ得／クロールされ得る（例えば、上記した方法において、関連する情報を見出すために、次いで情報がさらなる解析に供され得る）。任意の他のデータ供給源（例えば、ウェブページおよび／またはウェブサイト全体、電子メールメッセージなどを含む）は、同様の方法でクロールおよび／または検索され得る。

【００３６】

別の例として、オンラインのチャットルーム（インターネットリレーチャット（ＩＲＣ）チャネル、様々なＩＳＰ（例えば、Ｙａｈｏｏ™、Ａｍｅｒｉｃａ Ｏｎｌｉｎｅ™、など）により維持され／ホストされるチャットルームおよび／または同様のものを含むがこれらに限定はされない）（例えば、１０５ａ）は、関連情報についてモニタされ得る（および／またはこのようなチャットルームからのログはクロールされ得る）。一部の場合において、自動化処理（「ボット（ｂｏｔ）」として当該分野において公知）は、この目的のために使用され得る。しかしながら、他の場合には、付き添い人がこのようなチャットルームを個人的にモニタし得る。当業者は、しばしばこのようなチャットルームが、アクセス特権を維持するために参加を要求することを理解する。それゆえ、一部の場合には、ボットまたは付き添い人のいずれかが、貢献者として見られるためにこのようなチャットルームに対して入力を通知し得る。

【００３７】

ドメインレジストレーションゾーンファイル１０５ｃ（ならびに／もしくは任意の他のドメインの供給源および／またはインターネットレジストリ（例えば、ＡＲＩＮ）のようなネットワーク情報）はまた、データ供給源として使用され得る。当業者が認識するように、ゾーンファイルは、新しいドメインレジストレーションを反映するために定期的に（例えば、時間ごとにまたは日ごとに）アップデートされる。これらのファイルは、新しいドメインレジストレーションを探すために定期的にクロール／スキャンされ得る。特定の実施形態においては、ゾーンファイル１０５ｃは、顧客の名前および／またはドメインに類似したレジストレーションをスキャンされ得る。単なる例として、システム１００は、異なるトップレベルドメイン（「ＴＬＤ」）またはグローバルトップレベルドメイン（「ｇＴＬＤ」）および／または類似の綴りを有するドメインを用いて類似するドメインレジストレーションを検索するように構成され得る。従って、顧客が＜ａｃｍｅｐｒｏｄｕｃｔｓ．ｃｏｍ＞ドメインを使用する場合には、＜ａｃｍｅｐｒｏｄｕｃｔｓ．ｂｉｚ＞、＜ａｃｍｅｐｒｏｄｕｃｔｓ．ｃｏ．ｕｋ＞および／または＜ａｃｍｅｐｒｏｄｕｃｔ．ｃｏｍ＞のレジストレーションは、スプーフサイトの可能性のあるホストとして重要であり得、このようなドメインに対するドメインレジストレーションは、レジストレーションが対応するドメインのさらなる解析のためにダウンロードされ得および／または記され得る。一部の実施形態において、疑わしいドメインが見出される場合には、そのドメインはモニタリングリスト上に置かれ得る。モニタリングリスト上のドメインは、ドメインが「生きて」いるかどうか（例えば、ドメインに関連するアクセス可能なウェブページがあるかどうか）を決定するために、以下のさらなる詳細において記載されるように、定期的にモニタされ得る。

【００３８】

１つ以上の電子メールフィード１０５ｄは、システム１００に追加のデータ供給源を提

供し得る。電子メールフィードは、上記したようにスパムメッセージを含む電子メールメッセージの任意の供給源であり得る。（実際、１つの入力電子メールメッセージは、一部の実施形態に従って電子メールフィードと考えられ得る）。一部の場合において、例えば、以下により詳細に記載するように、おとり（ｂａｉｔ）電子メールアドレスは、本発明の実施形態により「シードされ」、またはプラントされ得、および／またはこれらのプラントされたアドレスは電子メールの供給源を提供し得る（例えば、電子メールフィード）。それゆえ、システム１００は、アドレスプランタ１７０を含み得、アドレスプランタ１７０は、図１Ｂとの関連において詳細に示される。

【００３９】

アドレスプランタ１７０は、電子メールアドレスジェネレータ１７５を含み得る。アドレスジェネレータ１７５は、ユーザインターフェース１８０および／または１つ以上のデータベース１８５と通信し得る（これらの各々が関係のデータベースおよび／または任意の他の適切な記憶メカニズムを含み得る）。１つのこのようなデータ記憶装置は、ユーザＩＤ情報１８５ａのデータベースを含み得る。ユーザＩＤ情報１８５ａは、本発明の実施形態に従うユーザＩＤを生成するために使用され得る名前、番号および／または他の識別子のリストを含み得る。一部の場合には、ユーザＩＤ情報１８５ａは（例えば、ファーストネーム、ラストネーム、番号または他のキャラクタのような変更子などに）分類され得る。別のデータ記憶装置は、ドメイン情報１８０を含み得る。ドメイン情報１８０のデータベースは、アドレスに利用可能なドメインのリストを含み得る。多くの場合には、これらのドメインは、アドレスプランタ１７０の操作者によって所有／管理されるドメインである。しかしながら、他の場合には、ドメインは他者（例えば、商用のＩＳＰおよび／または消費者のＩＳＰなど）によって管理され得る。

【００４０】

アドレスジェネレータ１７５は、アドレスジェネレーションエンジンを備え、アドレスジェネレーションエンジンは、インターネット上の適切な位置（または他の場所に）にプラントされ得る電子メールアドレスを生成する（個別ベースで、および／またはバッチベースで）ように構成され得る。単なる例として、アドレスジェネレータ１７５は、ユーザＩＤデータ記憶装置１８５ａから１つ以上のユーザＩＤ情報の要素を選択するように（および／または複数のこのような要素を組み合わせるように）構成され得、これらの要素をドメインデータ記憶装置１８５ｂから選択されたドメインに付加するように構成され得、これにより電子メールアドレスを作成する。これらの構成要素を組み合わせるための手順は、任意に決定できる。単なる例として、一部の実施形態においては、アドレスジェネレータ１７５は、比較的多くのアドレスがこれらのドメインにおいて生成されるように、あるドメインネームに優先順位を決めるように構成され得る。他の実施形態において、処理は１つ以上のアドレスコンポーネントのランダムな選択を含み得る。

【００４１】

アドレスプランタ１７０の一部の実施形態は、追跡データベース１９０を含み、追跡データベース１９０は、プラント操作（特定のアドレスがプラントされる位置（例えば、ウェブサイトなど）、プラントの日付／時間、ならびにプラントについての任意の他の関連する詳細を含むがこれらに限定はされない）を追跡するために使用され得る。単なる例として、所与のアドレスを有するメーリングリストに加入することによりアドレスがプラントされる場合には、メーリングリストは（可能性としては、ウェブサイト、リストの管理人の電子メールアドレスなども同様に）、追跡データベースに記録され得る。一部の場合において、この情報の追跡は自動化され得る（例えば、アドレスプランタ１７０のユーザインターフェース１８０が、ウェブブラウザおよび／または電子メールクライアントを含む場合には、ならびにそのウェブブラウザ／電子メールクライアントがアドレスをプラントするために使用される場合には、プラントの情報についての情報は、アドレスプランタ１７０により自動的に登録され得る）。あるいは、ユーザがアドレスを手動でプラントし得（例えば、ユーザ独自のウェブブラウザ、電子メールクライアントなどを使用して）、結果として追跡データベースに、専用の入力ウィンドウ、ウェブブラウザなどを介して、

関連情報を付加し得る。

【００４２】

実施形態の１つのセットにおいて、アドレスプランタ１７０は、電子メールアドレスを生成するため、特定された位置において電子メールアドレスをプラントするため（アドレスジェネレータ１７０によって生成されるかどうか）、および／またはプラント操作についての情報を追跡するために使用され得る。特定の実施形態においては、アドレスプランタ１７０はまた、１つ以上のアプリケーションプログラミングインターフェース（「ＡＰＩ」）１９５を含み得、ＡＰＩ１９５は、図１のシステム１００の他の構成要素（または任意の他の適切なシステム）が、アドレスプランタとプログラムされているように相互作用することを可能にする。単なる例として、一部の実施形態において、ＡＰＩ１９５は、プラント操作を行うために、アドレスプランタ１７０がウェブブラウザ、電子メールクライアント、などとインターフェースすることを可能にする。（他の実施形態においては、上記したように、このような機能性はアドレスプランタ１７０自体に含まれ得る）。

【００４３】

ある実施形態におけるＡＰＩ１９５の特定の使用は、他のシステム構成要素（特にイベントマネージャ１３５を含む）が、アドレスプラント操作（および／またはそれらの結果）についての情報を取得および／またはアップデートすることを可能にする。（一部の場合において、アドレスプランタ１７０へのプログラムに基づいたアクセスは必要とされ得ない。システム１００の必要な構成要素は、必要な場合には、単にＳＱＬなどを通じてデータ記憶装置１８５の１つ以上にアクセスし得る）。単なる例として、電子メールメッセージがシステム１００により解析される場合には（例えば、以下に詳細に記載されるように）、システム１００は、アドレスプランタ１７０および／またはデータ記憶装置１８５の１つ以上を問い合わせ（ｉｎｔｅｒｒｏｇａｔｅ）し得ることにより、電子メールアドレスがアドレスプランタ１７０によりプラントされたアドレスにアドレスされたかどうかを決定する。そうである場合には、アドレスプランタ１７０（または、イベントマネージャ１３５のようなシステム１００の一部の他の構成要素）は、プラントする位置を、フィッシュメッセージを誘発しそうな位置として記し得、それにより、追加のアドレスが所望どおりにこのような位置にプラントされ得る。このようにして、システム１００は、プラント操作の効率を強化するようにフィードバックループをインプリメントし得る（このフィードバック処理は任意の所望のタイプの「望まれない」メッセージ（フィッシュメッセージ、一般的なスパムメッセージ、商標の悪用を証明するメッセージなどを含むがこれらに限定はされない）に対してインプリメントされ得ることに注意する）。

【００４４】

他の電子メールフィードは、本明細書の他の箇所に記載され、それらはスパムメール送信者／フィッシュメール送信者から直接受信されたメッセージと、ユーザ、ＩＳＰおよび／または任意の他の供給源（可能性としては、電子メールがスパムおよび／またはフィッシュであるという疑いに基づいて）から転送された電子メールと、メーリングリスト（反不正使用メーリングリストを含むがこれらに限定はされない）から転送された電子メールなどを含む（が、それに限定はされない）。電子メールメッセージ（これは、スパムメッセージであり得る）がシステム１００により受信される場合には、そのメッセージは、解析され得、フィッシング／スプーフィングスキームの一部であるかどうかを決定する。任意のこれらのデータフィードから受信された情報の解析は、以下にさらに詳細に記載され、解析は、しばしば、ウェブサイト（しばしば、データ供給源１０５から受信／ダウンロードされたＵＲＬまたは他の情報により参照される）がフィッシングおよび／またはスプーフィングの詐欺に従事する可能性があるかどうかの評価を含む。

【００４５】

システムに入来する任意の電子メールメッセージは、本発明の様々な方法に従って解析され得る。当業者が認識するように、大量のインターネット上の望まれない電子メールのトラフィックがあり、これらのメッセージの多くがオンラインの詐欺のコンテキストにおいて重要であり得る。単なる例として、一部の電子メールメッセージは、本明細書でさら

に詳細に記載されるフィッシング詐欺の一部として伝送され得る。他のメッセージは、消費者にブラックマーケットおよび／またはグレイマーケットの商品（例えば、海賊版ソフトウェア、偽造のデザイナー商品（時計、ハンドバッグなどを含むがこれらに限定はされない））を勧め得る。さらに他のメッセージは正当な商品のための広告であり得るが、非合法の方法を含み得、そうでなければ（例えば、契約によって）禁止されている実行（例えば、不適当な商標の使用および／または商品の違法な故意の値下げなど）を含み得る。本発明の様々な実施形態は、以下に記載されるように、これらの実行の１つ以上を検索し、識別し、および／またはこれらの実行の１つ以上に応答するように構成され得る。（ある実施形態が、同様の振る舞いをする電子メールフィード以外のゾーンファイル、ウェブサイト、チャットルームなどを含む、データ供給源にアクセス、モニタ、クロールなどを行うように構成され得ることにも同様に注意する）。単なる例として、システム１００は、用語ＲＯＬＥＸ™に対して１つ以上のデータ供給源をスキャンするように、および／またはＲＯＬＥＸ™の時計の任意の不適当な広告を識別するように構成され得る。

【００４６】

当業者は、普通の電子メールアドレスは、多くの望まれない電子メールメッセージを受信することを認識し、システム１００は、以下に記載されるように、このようなメッセージを受信および／または解析するように構成され得る。入来するメッセージは、多くの方法により受信され得る。単なる例として、一部のメッセージは、メッセージを促すために行動がとられないので、「ランダムに」受信され得る。あるいは、１人以上のユーザが、このようなメッセージをシステムに転送し得る。単なる例として、ＩＳＰは、ＩＳＰのユーザに、全ての望まれないメッセージを特定のアドレスに転送するように命令し得、特定のアドレスは、以下に記載されるようにシステム１００によりモニタされ得、またはユーザの入力メッセージのコピーをこのようなアドレスに自動的に転送し得る。特定の実施形態においては、ＩＳＰは、ＩＳＰのユーザに伝送された疑わしいメッセージ（および／または例えば、このようなメッセージに含まれる任意のＵＲＬを含むこのような疑わしいメッセージの一部）をシステム１００（および／またはシステム１００の任意の適切な構成要素）に定期的なベースで転送し得る。一部の場合には、ＩＳＰは、この処理を円滑にするように設計されたフィルタリングシステムを有し得、および／またはシステム１００のある特徴はＩＳＰのシステム内でインプリメント（および／または複製）され得る。

【００４７】

上記したように、システム１００はまた、例えば、スパムメール送信者／フィッシュメール送信者による収集のために、特定のデータ供給源内におとりの電子メールアドレス（および／または他のおとりの情報）をプラントまたはシードし得る。通常は、これらのおとりの電子メールアドレスは、電子メールアドレスのハーベスタに対する魅力的なターゲットを提供するように設計され、おとりの電子メールアドレスは通常は（常にではないが）フィッシュメール送信者を引き込む目的で特別に生成され、それゆえに通常の電子メール通信には使用されない。

【００４８】

それゆえ、図１Ａに戻ると、システム１００は「ハニーポット」１１０をさらに含み得る。ハニーポット１１０は、データ供給源１０５の各々から情報を受信するために使用され得、および／または必要であればさらなる解析のためにその情報を相関付けるために使用され得る。ハニーポット１１０は、本発明の様々な実施形態に従って、このような情報を種々の方法で受信し得、どのようにハニーポット１１０が情報を受信するかは任意に決定できる。

【００４９】

単なる例として、上記したようにハニーポット１００は、必ずしも必要でないが、データ供給源を実際にクロールすること／モニタすることを行うために使用され得る。（一部の場合には、１つ以上の他のコンピュータ／プログラムは実際にクロールすること／モニタすることの操作を行うために使用され得、および／またはこのような操作を介して取得された任意の関連情報をハニーポット１１０に伝送し得る。例えば、処理はゾーンファイ

ルをモニタするように構成され得、任意の新しい、無効のおよび／またはそうでない場合には変更されたドメインレジストレーションの解析のためにハニーポット１１０に伝送するように構成され得る。あるいは、ゾーンファイルはハニーポット１１０に対する入力として送られ、および／またはハニーポット１１０は、任意の変更されたドメインレジストレーションを検索するために使用され得る）。ハニーポット１１０はまた、電子メールメッセージ（これは別の受信者から転送され得る）を受信するように構成され得、および／または１つ以上のおとりの電子メールを入来する電子メールについてモニタリングするように構成され得る。特定の実施形態においては、システム１００は、ハニーポット１１０が１つ以上の電子メールアドレス（これはおとりのアドレスであり得る）に対するメールサーバであるように構成され得、ゆえにこのようなアドレスにアドレスされた全てのメールはハニーポット１１０に直接送信される。ハニーポット１１０は、それゆえ、電子メールメッセージを受信するように機能する（例えば、ＳＭＴＰサーバなど）、および／またはおとりの電子メールアドレスにアドレスされた電子メールメッセージを引き出すように機能する（例えば、ＰＯＰ３および／またはＩＭＡＰクライアントなど）デバイスおよび／またはソフトウェアを含み得る。このようなデバイスおよびソフトウェアは当該分野において周知であり、本明細書で詳細に議論する必要はない。様々な実施形態に従って、ハニーポット１１０は、任意の（または全ての）種々の周知のメッセージフォーマット（ＳＭＴＰ、ＭＩＭＥ、ＨＴＭＬ、ＲＴＦ、ＳＭＳおよび／または同様のものを含む）を受信するように構成され得る。ハニーポット１１０はまた、１つ以上のデータベース（および／または他のデータ構造）を備え得、これは電子メールメッセージおよび他のデータ（例えば、ゾーンファイルなど）ならびにクロールする／モニタリングする操作から取得された情報を維持／分類するために使用され得る。

【００５０】

一部の局面において、ハニーポット１１０は、受信されたデータ（受信された電子メールメッセージを含むがこれに限定はされない）の一部の予備的な分類および／またはフィルタ掛けを行うように構成され得る。特定の実施形態において、例えば、ハニーポット１１０は、受信されたデータの「ブラックリストに列挙される」単語または言いまわしを検索するように構成され得る。（「ブラックリスト」の概念は以下にさらに詳細に記載される）。ハニーポット１１０は、優先順位を決められた処理のために、および／またはこれらのまたは他の判定基準に基づいてデータ／メッセージにフィルタを掛けるために、このようなブラックリストに列挙される用語を含むデータ／メッセージを分離する。

【００５１】

ハニーポット１１０はまた、顧客ポリシー１１５に従って操作するように構成され得る。例示的な顧客ポリシーは、ハニーポットに、特定のタイプおよび／またはフォーマットの電子メールを見張るように命令し得る（例えば、特定のキーワードを検索するために、顧客ごとをベースとしてカスタマイズすることを可能にさせることを含む）。加えて、ハニーポット１１０は、拡張モニタリングオプション１２０を活用し得る（他の状況をモニタすること（例えば、危険性のために顧客のウェブサイトをモニタすることなど）を含む）。ハニーポット１１０は、メッセージを受信すると、選択的に電子メールメッセージをデータファイルに変換し得る。

【００５２】

一部の実施形態においては、ハニーポット１１０は、１つ以上の相関エンジン１２５と通信し、相関エンジン１２５は、電子メールメッセージ（および／または他の情報／データ（例えば、クロールする／モニタリングする操作から受信された情報））のさらに詳細な解析を行い得る。（しかしながら、本明細書の機能の様々な構成要素（例えば、ハニーポット１１０、相関エンジン１２５など）への割り当ては任意であることに注意されるべきであり、一部の実施形態に従って、特定の構成要素は、他の構成要素に割り当てられた機能性を統合し得る）。

【００５３】

定期的なベースで、および／または入来するメッセージ／情報がハニーポット１１０に

より受信される／引き出される場合に、ハニーポット１１０は、受信された／引き出された電子メールメッセージ（および／または対応するデータファイル）を、解析のために利用可能な相関エンジン１２５に伝送する。あるいは、各相関エンジン１２５は、ハニーポット１１０からメッセージ／データファイルを定期的に引き出すように構成され得る（例えば、スケジュールされたＦＴＰ処理などを用いること）。例えば、特定のインプリメンテーションにおいては、ハニーポット１１０は、上記したように、電子メールメッセージおよび／または他のデータ（これは分類／フィルタされたり、されなかったりする）を記憶し得、各相関エンジンは、定期的なおよび／またはアドホックなベースでデータおよび／またはメッセージを引き出し得る。例えば、相関エンジン１２５が、利用可能な処理能力を有する場合には（例えば、相関エンジン１２５がそのキューにおいて任意のデータ／メッセージの処理を終えている）、相関エンジン１２５は、処理のためにハニーポット１１０から次の１００個のメッセージ、データファイルなどをダウンロードし得る。特定の実施形態に従って、様々な相関エンジン（例えば、１２５ａ、１２５ｂ、１２５ｃ、１２５ｄ）は、あるタイプのデータ（例えば、ドメインレジストレーション、電子メールなど）を処理するように特別に構成され得る。他の実施形態においては、全ての相関エンジン１２５は任意の利用可能なデータを処理するように構成され得、および／または複数の相関エンジン（例えば、１２５ａ、１２５ｂ、１２５ｃ、１２５ｄ）は、並列処理の強化された効率を利用するようにインプリメントされ得る。

【００５４】

相関エンジン１２５は、データ（単なる例として電子メールメッセージを含む）を解析し得、ハニーポット１１０により受信された任意のメッセージがフィッシュメッセージであるか、および／または個人情報を収集するための詐欺的な試行を証明しそうであるかを決定する。この解析のための手順は以下に詳細に記載される。

【００５５】

相関エンジン１２５は、イベントマネージャ１３５と通信し得、イベントマネージャ１３５はまた、モニタリングセンタ１３０と通信し得る。（あるいは、相関エンジン１２５はまた、モニタリングセンタ１３０と直接通信し得る）。特定の実施形態においては、イベントマネージャ１３５は、コンピュータおよび／またはソフトウェアアプリケーションであり得、これらはモニタリングセンタ１３０内の技術者によりアクセス可能であり得る。相関エンジン１２５が、特定の入力電子メールメッセージが詐欺的な活動の候補でありそうであること、またはクロールする／モニタリングする操作を介して取得される情報が詐欺的な活動を指示し得ることを決定する場合には、相関エンジン１２５は、イベントマネージャ１３５に、イベントが電子メールメッセージにおいて作成されるべきであるという信号を送り得る。特定の実施形態においては、相関エンジン１２５および／またはイベントマネージャ１３５は、当該分野において周知の簡易ネットワーク管理プロトコル（「ＳＮＭＰ」）を使用して通信するように構成され得、相関エンジンの信号は、解析されたメッセージおよび／またはデータは、さらに調査されるべきである詐欺の可能性のあるイベントを指示していることを指示するＳＮＭＰの「トラップ」を含み得る。信号（例えば、ＳＮＭＰトラップ）に応答して、イベントマネージャ１３５は、イベント（これは、ＳＮＭＰイベントを含み得、独自のフォーマットであり得る）を作成し得る。

【００５６】

イベントを作成すると、イベントマネージャ１３５は、メッセージ／情報に含まれるおよび／またはメッセージ／情報に関連する、メッセージ／情報および／またはＵＲＬの情報収集操作（調査）１４０を開始し得る。以下に詳細に記載されるように、調査は、ＵＲＬに関連するドメインおよび／またはＩＰアドレスについての情報を収集すること、ならびにＵＲＬにより参照されるリソース（例えば、ウェブページなど）をホストするサーバに問い合わせすることを含み得る。（本明細書で使用される場合、用語「サーバ」は時折、個人情報が交換され得るＩＰベースのサービスを提供することまたはオンラインの取引を指揮することが可能な任意のコンピュータシステム、および特に個人情報の詐欺的な収集（例えば、個人情報を要求するウェブページを提供することによって）に従事させ得る

コンピュータシステム、を示すコンテキストとして使用される。それゆえに、このようなサーバのもっとも一般的な例は、ハイパーテキストトランスファープロトコル（「ＨＴＴＰ」）および／または任意のいくつかの関連サービスを使用して操作するウェブサーバであり、一部の場合ではあるが、サーバは、データベースサービスなどのような他のサービスを提供し得る）。特定の実施形態においては、１つの電子メールメッセージ（または情報ファイル）が複数のＵＲＬを含む場合には、個別のイベントが各ＵＲＬに対して生成され得る。他の場合には、１つのイベントは特定のメッセージにおけるＵＲＬの全てを覆い得る。メッセージおよび／または調査が、イベントが特定の顧客に関連することを指示する場合には、イベントはその顧客に関連し得る。

【００５７】

イベントマネージャはまた、自動化した報告１４５を準備し得（および／または、報告を生成するための報告モジュール（示されていない）のような別の処理を引き起こし得）、報告１４５は、モニタリングセンタ１３０（またはそういうことならば任意の他の位置）における追加の技術者により解析され得、イベントに対して、報告は調査の概略および／または調査により取得された任意の情報を含み得る。一部の実施形態においては、処理は完全に自動化され得、それゆえ人間による解析は必要ではない。所望される場合には（および、可能性として顧客ポリシー１１５によって指示される場合には）、イベントマネージャ１３５は、影響を受けた顧客にイベントを知らせる通知１５０を自動的に作成し得る。顧客通知１５０は、報告１４５からの情報の一部（または全て）を含み得る。あるいは、顧客通知１５０は、顧客が報告のコピーへアクセスすることを可能にする（例えば、ウェブブラウザ、クライアントアプリケーションなどを通じて）イベントを顧客に通知し得るだけである（例えば、電子メール、電話、ページャなどを通じて）。顧客はまた、その顧客を含むイベントを示す専用のウェブサイトのようなポータルを使用することに重要なイベントを見得る（例えば、ここでイベントは顧客の商標、製品、ビジネスアイデンティティなどを使用する詐欺に関連する）。

【００５８】

調査１４０が、ＵＲＬによって参照されるサーバが個人情報を収集するための詐欺的な試行に関連していることを明らかにする場合には、技術者は禁止（ｉｎｔｅｒｄｉｃｔｉｏｎ）応答１５５（本明細書では「技術応答」ともいう）を開始し得る。（あるいは、イベントマネージャ１３５は技術者による介入なしで自動的に応答を開始するように構成され得る）。状況および実施形態に依存して、種々の応答が適切であり得る。例えば、当業者は、一部の場合にはサーバが危うくされ得（すなわち「ハックされ」）、その場合にはサーバが、サーバの操作者の制御下ではなしにアプリケーションを実行し、および／またはサービスを提供する。（本コンテキストで使用される場合には、用語「操作者」は、所有する実体、維持する実体、および／またはそうでないならばサーバに責任のある実体を意味する）。調査１４０が、サーバが危険であると思われることを明らかにした場合には、サーバの操作者は単に無意識の犠牲者であり、詐欺のスキームにおける関係者であるように、適切な応答が、サーバの操作者にサーバが危険であることを伝えることを単純に含み得、可能性としては、危険性が許容される任意の脆弱性をどのように修復するかを説明することを含み得る。

【００５９】

他の場合においては、他の応答がより適切であり得る。このような応答は、一般的に、以下により完全に記載されるように、本質的には管理的１６０または技術的１６５のいずれかとして分類され得る。一部の場合には、システム１００はダイリューションエンジン（示されていない）を含み得、ダイリューションエンジンは、以下により完全に記載されるように、技術応答に着手するために使用され得る。一部の実施形態においては、ダイリューションエンジンはコンピュータ上で実行するソフトウェアアプリケーションであり得、とりわけ、本発明の方法に従って、フィッシング詐欺に対する応答を作成および／またはフォーマットするように構成され得る。ダイリューションエンジンは、相関エンジン１２５、イベントマネージャ１３５などと同一のコンピュータ上に存在し得（および／また

は組み込まれ得）、および／または個別のコンピュータ上に存在し得、ダイリューションエンジンは任意のこれらの構成要素と通信し得る。

【００６０】

上記したように、一部の実施形態においては、システム１００は、フィードバック処理を組み込み得ることにより、どちらのプラント位置／手法が、スパム生成に比較的により効果的であるかの決定を円滑にする。単なる例として、システム１００は、アドレスプランタ１７０を含み得、アドレスプランタ１７０は、上記したようにプラントされたアドレスについての情報を追跡するためのメカニズムを提供し得る。これに対して、イベントマネージャ１３５は、電子メールメッセージ（および特定の、結果としてイベントを生じるメッセージ）を解析するように構成され得ることにより、メッセージがプラントする操作から生じたかどうかを決定する。例えば、メッセージのアドレスは、もしあれば、どちらがシステム１００によりプラントされた１つ以上のアドレスに対応するかを決定するために評価され得る。メッセージが１つ以上のプラントされたアドレスに対応していることが決定される場合には、プラントされたアドレスのデータベースはプラントの状況を決定するために閲覧され、システム１００はこの情報を技術者に表示し得る。このようにして、技術者は、よい結果を生む（ｆｒｕｉｔｆｕｌ）位置に追加のアドレスをプラントすることを選択し得る。あるいは、システム１００は、アドレスプランタ１７０に自動的なフィードバックを提供するように構成され得、アドレスプランタ１７０は、代わりに、このような位置に追加のアドレスを自動的にプラントするように構成され得る。

【００６１】

本発明の様々な実施形態に従って、結果として、オンラインの詐欺の可能性についてのデータのセット（これは電子メールメッセージ、ドメインレジストレーション、ＵＲＬ、および／または任意の他のオンラインの詐欺についての関連データであり得る）は受信され得、解析され得ることにより、詐欺的な活動の存在を決定し、詐欺的な活動の例は、フィッシングスキームであり得る。本明細書で使用される場合には、用語「フィッシング」は、しばしば、ユーザが正当であると思われるウェブサーバのようなサーバにアクセスすることを要求する望まれない電子メールメッセージ（または、電話のコール、ウェブページ、ＳＭＳメッセージなど一部の他の通信）を送信することによって、ユーザに、それ以外の場合にはユーザがとらない行動をとるようにさせる（例えば、彼または彼女の個人情報を提供する、違法の製品を購入するなど）ための詐欺的なスキームを意味する。そうである場合には、任意の関連する電子メールメッセージ、ＵＲＬ、ウェブサイトなどは、調査され得、および／または応答の行動がとられ得る。追加の特性および他の実施形態は、いかにさらなる詳細として記載される。

【００６２】

（２．例示的な実施形態）

上記したように、本発明の特定の実施形態は、オンラインの詐欺に対処するためのシステムを提供する。図２のシステム２００は、実施形態の１つのセットの例示が考慮され得る。システム２００は、一般的にネットワークされた環境において実行され、ネットワークされた環境は、ネットワーク２０５を含み得る。多くの場合においては、ネットワーク２０５はインターネットであり、一部の実施形態の場合ではあるが、ネットワーク２０５は、一部の他の公共のおよび／またはプライベートなネットワークであり得る。通常は、任意のコンピュータ間のデータ通信をサポートすることが可能なネットワークで十分である。システム２００は、マスタコンピュータ２１０を含み、マスタコンピュータ２１０は、本明細書で議論される、任意の手順または方法を行うために使用され得る。特定の場合には、マスタコンピュータ２１０は様々なデータ供給源をクロール／モニタするように、おとりの電子メールアドレスをシードするように、おとりの電子メールアドレスに伝送された電子メールアドレスを収集および／または解析するように、イベントを作成および／または追跡するように、ＵＲＬおよび／またはサーバを調査するように、イベントについての報告を準備するように、イベントについて顧客に通知するように、ならびに／あるいは、例えば、電気通信リンクを通じて、モニタリングセンタ２１５と通信するように（お

よびより詳しくは、モニタリングセンタ内のモニタリングコンピュータ２２０と通信するように）、構成され得る（例えば、ソフトウェアアプリケーションを通じて）。マスタコンピュータ２１０は、複数のコンピュータであり得、複数のコンピュータの各々は、様々な実施形態に従って、特定の処理を行うように構成され得る。単なる例として、１台のコンピュータは、ハニーポットに関して上記した機能を行うように構成され得、別のコンピュータは相関エンジンに関連するソフトウェアを実行するように構成され得る（例えば、電子メールのメッセージ／データファイルの解析を行うこと）。第３のコンピュータはイベントマネージャとして役立つように構成され得（例えば、詐欺の疑いのある出来事を調査することおよび／またはそれに応答すること）、および／または第４のコンピュータは、ダイリューションエンジンとして機能するように構成され得る（例えば、技術応答を生成および／または伝送すること、技術応答は、以下にさらに詳細に記載されるように、単なる例として１つ以上のＨＴＴＰ要求を含み得る）。同様に、モニタリングコンピュータ２２０は、任意の適切な機能を行うように構成され得る。

【００６３】

モニタリングセンタ２１５、モニタリングコンピュータ２２０および／またはマスタコンピュータ２１０は、１人以上の顧客２２５と（例えば、電気通信リンクを経由して）通信する。電気通信リンクは、音声および／またはデータ通信を提供することが可能な任意の媒体（例えば、電話線、無線接続、ワイドエリアネットワーク、ローカルエリアネットワーク、仮想的なプライベートネットワークおよび／または同様のもの）を経由する接続を含み得る。このような通信は、データ通信および／または音声通信であり得る（例えば、モニタリングセンタにいる技術者が、顧客における人物と電話通信を行い得る）。顧客２２５との通信は、イベント報告、イベントの通知、および／または詐欺的な活動の応答についての相談の伝送を含み得る。

【００６４】

マスタコンピュータ２１０は、複数のデータ供給源（上記したデータ供給源１０５を含むがこれに限定はされない）を含む（および／または複数のデータ供給源と通信する）。他のデータ供給源は、同様に使用され得る。例えば、マスタコンピュータは、証拠データベース２３０および／または「安全なデータ」のデータベース２３５を含み得、それらは、以下に詳細に議論するような使用において、１つ以上の架空の（または真実の）識別子のためのおとりの電子メールアドレスおよび／または個人情報を生成および／または記憶するために使用され得る。（本明細書で使用される場合には、用語「データベース」は、データを記憶する任意の手段（伝統的なデータベース管理ソフトウェア、オペレーティングシステム、ファイルシステムおよび／または同様のものを含む）を含むように広く解釈されるべきである）。マスタコンピュータ２１０はまた、調査されるべきインターネットおよび／または任意のサーバについての情報の１つ以上の供給源と通信し得る。このような情報の供給源は、ドメインＷＨＯＩＳデータベース２４０、ゾーンデータファイル２４５などを含み得る。当業者は、ＷＨＯＩＳデータベースがしばしば、中央のレジストレーションオーソリティ（例えば、Ａｍｅｒｉｃａｎ Ｒｅｇｉｓｔｒｙ ｆｏｒ Ｉｎｔｅｒｎｅｔ Ｎｕｍｂｅｒｓ（「ＡＲＩＮ」）、Ｎｅｔｗｏｒｋ Ｓｏｌｕｔｉｏｎｓ，Ｉｎｃなど）により維持されることと、マスタコンピュータ２１０はこれらのオーソリティを照会するように構成され得ることと、あるいはマスタコンピュータ２１０は、他の供給源（例えば、プライベートに維持されるデータベースなど）からこのような情報を取得するように構成され得ることと、を認識する。マスタコンピュータ２１０（および／または任意の他の適切なシステム構成要素）は、これらのリソースを使用し得、他のもの（例えば、公共利用可能なドメインネームサーバ（ＤＮＳ）データ、ルーティングデータおよび／または同様のもの）を、詐欺的な活動を行っている疑いのあるサーバ２５０を調査するために使用し得る。上記したように、サーバ２５０は、オンライン取引の処理、ウェブページを提供することおよび／またはそうでなければ個人情報を収集することが可能な任意のコンピュータであり得る。

【００６５】

システムはまた、１つ以上の応答コンピュータ２５５を含み、応答コンピュータ２５５は、以下に詳細に記載するように詐欺的な活動への技術応答を提供するために使用され得る。特定の実施形態においては、１つ以上の応答コンピュータ２５５は、ダイリューションエンジンを備え得、および／またはダイリューションエンジンと通信し得、ダイリューションエンジンは、フィッシング詐欺への応答を作成および／またはフォーマットするために使用され得る。（応答コンピュータ２５５の機能はまた、マスタコンピュータ２１０、モニタリングコンピュータ２２０等により行われ得ることに注意する）。特定の実施形態においては、複数のコンピュータ（例えば、２２５ａ～２２５ｃ）は、分散型の応答を提供するために使用され得る。応答コンピュータ２５５、ならびにマスタコンピュータ２１０および／またはモニタリングコンピュータ２２０は、必要なタスクを行うためのハードウェア、ファームウェアおよび／またはソフトウェアの命令を有する専用コンピュータであり得る。あるいは、これらのコンピュータ２１０、２２０、２５５は、オペレーティングシステムを有する汎用コンピュータ（例えば、Ｍｉｃｒｏｓｏｆｔ　Ｃｏｒｐ．のＷｉｎｄｏｗｓ（登録商標）および／またはＡｐｐｌｅ　Ｃｏｒｐ．のＭａｃｉｎｔｏｓｈ™のオペレーティングシステムの任意の適切なフレーバーを実行するパーソナルコンピュータおよび／またはラップトップコンピュータ、ならびに／あるいは任意の種々の市販されるＵＮＩＸ（登録商標）またはＵＮＩＸ（登録商標）に似たオペレーティングシステムを実行するワークステーションコンピュータを含む）であり得る。特定の実施形態においては、コンピュータ２１０、２２０、２５５は、任意の種々の無料のオペレーティングシステム（例えば、ＧＮＵ／Ｌｉｎｕｘ、ＦｒｅｅＢＳＤなど）を実行し得る。

【００６６】

コンピュータ２１０、２２０、２５５はまた、種々のサーバアプリケーション（ＨＴＴＰサーバ、ＦＴＰサーバ、ＣＧＩサーバ、データベースサーバ、Ｊａｖａ（登録商標）サーバなどを含む）を実行し得る。これらのコンピュータは、他のコンピュータ（ウェブアプリケーションを含むがこれに限定はされない）からの要求および他のコンピュータとの相互作用に応答してプログラムまたはスクリプトを実行可能な１つ以上の汎用コンピュータであり得る。このようなアプリケーションは、任意のプログラミング言語（単なる例として、Ｃ、Ｃ＋＋、Ｊａｖａ（登録商標）、ＣＯＢＯＬあるいはＰｅｒｌ、Ｐｙｔｈｏｎ、またはＴＣＬまたはこれらの任意の組み合わせのような任意のスクリプト言語）で書かれた１つ以上のスクリプトまたはプログラムとしてインプリメントされ得る。コンピュータ２１０、２２０、２５５はまた、データベースサーバソフトウェア（Ｏｒａｃｌｅ™、Ｍｉｃｒｏｓｏｆｔ™、Ｓｙｂａｓｅ™、ＩＢＭ™などから商用に入手可能なパッケージを含むがこれらに限定はされない）を含み得、データベースサーバソフトウェアは、ローカルにおよび／または他のコンピュータ上で実行するデータベースクライアントからの要求を処理し得る。単なる例として、マスタコンピュータ２１０は、本発明の実施形態に従って、タスクを行うための独自のアプリケーションソフトウェアを実行するように構成されたＧＮＵ／ＬｉｎｕｘオペレーティングシステムおよびＰｏｓｔｇｒｅＳＱＬデータベースエンジンを操作するＩｎｔｅｌ™プロセッサマシンであり得る。

【００６７】

一部の実施形態においては、１つ以上のコンピュータ１１０は、調査報告を表示することなどに必要な場合に、ウェブページを動的に作成し得る。これらのウェブページは、１台のコンピュータ（例えば、マスタコンピュータ２１０）と別のコンピュータ（例えば、モニタリングコンピュータ２２０）との間のインターフェースとして役立ち得る。あるいは、コンピュータ（例えば、マスタコンピュータ２１０）はサーバアプリケーションを実行し得、一方で別の（例えば、モニタリングコンピュータ２２０）デバイスは専用のクライアントアプリケーションを実行し得る。サーバアプリケーションは、それゆえ、クライアントアプリケーションを実行するユーザデバイスのインターフェースとして役立ち得る。あるいは、特定のコンピュータは他のコンピュータと通信する「シン（ｔｈｉｎ）クライアント」またはターミナルとして構成され得る。

【００６８】

システム２００は、１つ以上のデータ記憶装置を含み得、データ記憶装置は、１つ以上のハードドライブなどを備え得、ハードドライブなどは、例えば、データベース（例えば、２３０、２３５）を記憶するために使用され得る。データ記憶装置の位置は任意に決定される。単なる例として、データ記憶装置は、記憶媒体上にコンピュータの１つ以上に対してローカルに存在し（および／または常駐し）得る。あるいは、データ記憶装置は、データ記憶装置がこれらの１つ以上と通信する（例えば、ネットワーク２０５を経由して）間は、これらの任意のまたは全てのデバイスから離れ得る。一部の実施形態においては、データ記憶装置は、当業者に馴染み深い記憶領域ネットワーク（「ＳＡＮ」）に存在し得る。（同様に、コンピュータ２１０、２２０、２５５に起因する機能を行うための任意の必要なファイルは、コンピュータ読み取り可能な記憶媒体に、各々のコンピュータにローカルにおよび／または各々のコンピュータから離れて、適切に記憶され得る）。

【００６９】

図３は、本明細書に記載される、本発明の方法および／またはマスタコンピュータ、モニタリングコンピュータ、および／または応答コンピュータの機能を行い得るコンピュータシステム３００の一実施形態の一般化された概略図を提供する。図３は、様々な構成要素の一般化された図を提供することのみを意図されており、任意の構成要素は適切に利用され得る。コンピュータシステム３００は、バス３０５を通じて電気的に結合され得る、１つ以上のプロセッサ３１０と、１つ以上の記憶デバイス３１５と、を含むハードウェア構成要素を含み得る。記憶デバイス３１５は、ディスクドライブ、光学記憶デバイス、固体素子記憶デバイス（例えば、ランダムアクセスメモリ（「ＲＡＭ」）および／または読み取り専用メモリ（「ＲＯＭ」））を含むがこれらに限定はされない。これらは、プログラム可能であり得、素早いアップデートが可能であり得および／または同様のものであり得る（上記されるように、これらはデータ記憶装置として機能し得る）。１つ以上の入力デバイス３２０（入力デバイス３２０はマウス、キーボードおよび／または同様のものを含むがこれらに限定はされない）と、１つ以上の出力デバイス３２５（出力デバイス３２５はディスプレイデバイス、プリンタおよび／または同様のものを含むがこれらに限定はされない）と、通信サブシステム３３０（通信サブシステム３３０は、モデム、ネットワークカード（無線または有線）、赤外線通信デバイスおよび／または同様のものを含むがこれらに限定はされない）はまた、バス３０５と通信し得る。

【００７０】

コンピュータシステム３００はまた、現在ワーキングメモリ３３５内に位置するように示されるソフトウェア要素（オペレーティングシステム３４０、ならびに／あるいは上記したような、および／または本発明の方法をインプリメントするように設計されたアプリケーションプログラムのような他のコード３４５）を備え得る。当業者は、実質的な変更が、特定の実施形態および／または要求に従ってなされ得ることを認識する。例えば、カスタマイズされたハードウェアはまた、使用され得、および／または特定の要素は、ハードウェア、ソフトウェア（アプレットのようなポータブルソフトウェアを含む）、またはその両方においてインプリメントされ得る。

【００７１】

実施形態の別のセットは、オンラインの詐欺に対抗する方法を提供し、方法は、一部の場合には、コンピュータによりインプリメントされ得、コンピュータソフトウェアプログラムにおいて具体化され得る。これらの方法は、コンピュータソフトウェアアプリケーションとして、および／またはコンピュータシステム（上記のシステムを含む）によって、インプリメントされ得るが、必ずしもインプリメントされる必要はない。図４～図８は、いくつかのこのような方法を集団的に図示しており、このような方法は、個別におよび／またはお互いに関連して（他の方法と同様に）インプリメントされ得る。これらの方法の一部として記載される手順の一部または全ては、図１Ａに関連して記載されたものに類似する、可能性としては１人以上の人間の技術者からの相互作用を用いて、システムの様々な構成要素により行われ得る（が、行われる必要はない）。

【００７２】

図４Ａ、図４Ｂおよび図４Ｃは、オンラインの詐欺の可能性のある出来事についての情報を収集する方法を図示している。例えば、図４Ａは、本発明のある実施形態に従って、入来する電子メールメッセージを誘起すること、受信することおよび／または分類することのための方法４００を図示している。一部の場合には、ハニーポットおよび／または相関エンジンは、方法４００を行うために使用され得る。特定の実施形態においては、アドレスジェネレータ（例えば、図１Ｂに対して記載されるアドレスジェネレータ１７０）は、特定の操作（このようなおとりの電子メールアドレスをプラントすること、フィードバックループをインプリメントすることなど）を行うために使用され得る。例示的な方法４００は、１人以上の顧客に対して顧客プロファイルを確立することを含み得る（ブロック４０２）。顧客プロファイルは、入力電子メールメッセージが顧客をスプーフすることを試行していることを指示し得る特定のキーワードのブラックリストを識別し得る。例えば、金融サービス業界の顧客にとって、キーワードは、「ローン」、「アカウント」、「クレジットカード」および／または同様のものであり得る。顧客プロファイルはまた、顧客ならびにデフォルトの構成情報（例えば、電子メールメッセージをフィッシュとして考慮するための顧客の（例えば、比較的寛大なまたは比較的厳しい）閾値、および／または詐欺的な活動に応答するための顧客の優先度（例えば、管理上の応答のための優先度、技術応答の優先レベルなど））を含むフィッシング活動に関連することが知られているサーバ、ＵＲＬ、ドメイン、および／またはＩＰアドレスを識別し得る。

【００７３】

ブロック４０４において、１つ以上の「安全なアカウント」が、例えば、顧客のシステム内に作成され得る。これらの安全なアカウントは、任意の本当のアカウント名義人には対応しない有効なアカウント（例えば、使用中のクレジットカードアカウント）であり得、安全なアカウントは、任意の本当のアカウント名義人に対応しないが、顧客のシステムによって有効であるとして受容され得る有効な（または明らかに有効な）識別子（例えば、アカウント番号、社会保障番号、クレジットカード番号など）を含む、架空の個人情報に関連し得る。安全なアカウントは、その後、任意の取引またはアクセス試行をモニタされ得る（ブロック４０６）。安全なアカウントは本当のアカウント名義人には対応しないので、任意の取引、アクセス試行など（「アカウント活動」）は不正な使用を表す。加えて、安全なアカウントは、以下にさらに詳細に記載されるように、識別子の使用をトレースする（ｔｒａｃｅ）ためおよび／または追跡するために使用され得、詐欺的な活動の証拠となる記録をコンパイルするために使用され得る。

【００７４】

方法４００はまた、おとりの電子メールアドレスを生成および／またはプラントすることを含み得、おとりの電子メールアドレスは、スパムおよび／またはフィッシュメッセージを引き込むために使用され得る。一部の場合には、おとりのアドレスは、フィッシュメール送信者に魅力的なもの（例えば、魅力的なドメインから、および／またはユーザＩＤとして英語の適切な名前を使用して）であるように、および／または収集されたリスト上で優先されるもの（例えば、番号、文字ａ、またはアルファベットではないキャラクタなどにより始まるユーザＩＤを有する）であるように選択され得る。このようにして、フィッシュメール送信者が、フィッシュメッセージを収集されたリスト上のアドレスの各々に送信する場合には、おとりのアドレスがフィッシュメッセージを、メーリング処理において比較的に早く受信する高い確率があり得、多くの実際の受信者がフィッシュに応答して個人情報を提供する機会を有する前に、システムに応答行動をとらせる。

【００７５】

従って、一部の実施形態においては、電子メールアドレスを作成することは１つ以上のユーザＩＤ要素（例えば、上記したもの、上記したものは電子メールアドレスを作成するために使用され得る）を選択すること（ブロック４０８）を含み得る。ユーザＩＤ要素の選択は、アドレスプランタ（上記したような）によって、任意の他の適切なツールによって、および／または手動で行われ得る。所望される場合には、２つ以上のユーザＩＤ要素は、連結され得、そうでない場合はユーザＩＤを形成するために組み合わされ得る（ブロ

ック４１０）。特定の実施形態においては、ユーザＩＤは単に１つのユーザＩＤ要素を備え得る。

【００７６】

方法４００は、おとりのアドレスに対してホストネームおよび／またはドメインネームを選択することをさらに包含し得る（ブロック４１２）。本明細書で記載されるように、ドメインの選択にはいくつかの要因が考慮され得る。単なる例として、特定のドメインは、スパムおよび／またはフィッシュメッセージをより引き付ける可能性があるとして優先順位を付けられ得る（例えば、ドメインネームの性質によって、そのドメインを使用する電子メールアドレスは過去においては比較的多くのフィッシュメッセージを引き込むので、など）。多くの場合には、ドメインはアドレスをプラントすることに対する責任がある実体によって所有および／または管理されるドメインである（または、このような実体がアクセスするドメイン）。特定の場合には、有名な消費者ＩＳＰドメイン（例えば、「ａｏｌ．ｃｏｍ」、「ｍｓｎ．ｃｏｍ」など）が使用され得る。このようなドメインの所有者は、プラントするアドレスに責任のある実体と連携し得る。あるいは、アドレスプランタ（または別のツール）は、適切なＩＳＰにおいてアカウントを作成するために、および／または受信されたメッセージをハニーポットなどに自動転送するためのアカウントを構成するために使用され得る。

【００７７】

ドメインネームが、次いで、ユーザＩＤに付加され得ることにより、電子メールアドレスを作成する（ブロック４１４）。（この時点において、電子メールアドレスが、適切なホスト上にユーザＩＤを作成すること、ＩＳＰにアカウントを開くことなどを可能にするための任意の必要なステップは、自動的にまたは技術者によってのいずれかでとられ得る。しかしながら、多くの場合には、本明細書に記載されるように、選択されたドメインに対するメール交換が、任意のユーザＩＤに入来するメールを許容するように構成され得るので、特定のユーザＩＤに対してステップがとられる必要はないことが認識され得る）。

【００７８】

生成された電子メールアドレスに対して、１つ以上のプラントする位置が選択され得る（ブロック４１６）。プラントする位置は、ウェブサイト、ニュースグループおよび／または本明細書に記載される、収集されるプラントされたアドレス、ならびに／あるいはスパムおよび／またはフィッシュの電子メールを受信するプラントされたアドレスを結果として生じる可能性があり得る他の位置を含み得る。一部の場合には、１つの位置のみに各々の電子メールアドレスをプラントすることが望まれ得る（例えば、以下に、および図１Ｂに関連して記載される、追跡およびフィードバック処理を円滑にするために）。他の場合においては、例えば、各々の生成されたアドレスの効果を最大にすることが望まれる場合には、特定のアドレスが複数の位置にプラントされ得る。特定の実施形態においては、以下に詳細に記載するように、プラントする位置の選択は、どちらのプラントする位置がフィッシュ／スパムメッセージを生成したかを見積もる三角測量（ｔｒｉａｎｇｕｌａｔｉｏｎ）の手順を円滑にするように設計され得る。

【００７９】

次いで、ブロック４１８において、おとりの電子メールアドレスは、上記したように適切な位置にプラントされ得る。（おとりの電子メールアドレスは、生成されたアドレスであり得、購入されたドメインに関連するアドレス、先在するアドレスなどであり得る）。一部の場合には、プラントする位置は、ブロック４１６にて選択された位置であり得る。おとりのアドレスをプラントするタスク（本明細書では「シードする」ともいわれる）は、自動化され得（例えば、ハニーポット、アドレスジェネレータなどのようなコンピュータシステムにより行われる）、および／または手動で行われ得る。単なる例として、図１Ｂに関連して記載されるアドレスジェネレータ１７０に類似する、アドレスジェネレータは、特定の実施形態においては、図１Ｂに関連して詳細に記載される類似した処理を用いて、おとりの電子メールアドレスをプラントするために使用され得る。上記したように、特定の実施形態においては、各々の作成されたアドレスを１つの位置のみにプラントする

ことが望まれ得る（例えば、フィードバックループを追跡および／またはインプリメントすることを補助するために）。他の場合には、各々の生成されたアドレスの効果を最大にするために、各々のアドレスを複数の位置にプラントすることが望まれ得る。

【００８０】

他の実施形態においては、種々の自動化の、および／または手動の処理がおとりのアドレスをプラント（シード）するために使用され得（おとりのアドレス自体は、アドレスジェネレータによって、手動でおよび／または他の自動化処理を介して生成され得る）、単なる例として、自動化の処理は、ニュースグループにおとりの電子メールアドレスを含むアイテムを送り得、管理上のコンタクトとしておとりの電子メールアドレスを有するドメインレジストレーションを作成し得、収集されたアドレスのリストなどとして見られるようにフォーマットされたおとりのアドレスのリストをコンパイルおよび／または分配し得る。一部の状況においては、電子メールアドレスをプラントすることは、追加の情報を提供することをさらに包含し得る。単なる例として、アドレスをプラントすることが、管理上のコンタクトとしてアドレスによってＷＨＯＩＳ記録を作成することを包含する場合には、プラントする操作は、ＷＨＯＩＳ記録内に含まれる他の関連する情報（例えば、電話番号、コンタクトネーム、アドレスなど）を提供することを包含し得る。他の例においては、例えば、ニュースレターに加入する場合に、ファーストネームおよび／またはラストネームがおとりのアドレスに提供され得る。この情報は手動で供給され得、および／または自動化様式（例えば、アドレスプランタによって）で、可能性としてはユーザＩＤの生成に類似した様式で、生成され得る。一部の場合には、以下に記載するように、このような追加の情報は、どちらのプラントする位置がスパム／フィッシュ電子メールを生じたかを決定する処理を効率化（ｒｅｆｉｎｅ）するために使用され得る。結果として、追加の情報は、各々のプラントする位置において異なる情報を提供するために（おとりのアドレスが同一である場合でさえも）有用であり得る。

【００８１】

プラントする位置は、例えば、上記したように追跡データベースの使用を介して追跡され得る（ブロック４２０）。さらに、プラントされたアドレスと共に提供された任意の情報はまた、追跡され得る。プラントする位置の追跡は、以下に記載するように、フィードバック処理を円滑にし得る。

【００８２】

おとりの電子メールアドレスがプラントされた後に、おとりのアドレスに入来する任意の電子メールメッセージは、任意の受容可能な手順（上で議論されたような手順を含む）を使用して収集され得る（ブロック４２２）。一部の実施形態に従って、例えば、入来する電子メールメッセージを収集することは、ハニーポット／メールサーバから入来する電子メールメッセージをダウンロードすること、および／または電子メールメッセージをデータファイルに変換することを包含し、データファイルは、電子メールメッセージのヘッダ情報、電子メールメッセージの本体部分、電子メールメッセージに含まれる任意のＵＲＬ、および／または電子メールメッセージの任意の添付ファイルに対応する個別の部分および／またはフィールドを有し得る。電子メールメッセージを収集することは、解析のために、電子メールメッセージ、および／または電子メールメッセージをダウンロードする相関を相関エンジンに伝送することをさらに包含する。任意の収集された入来する電子メールメッセージ（および／または対応するデータファイル）は、メッセージがおそらくフィッシュである（すなわち詐欺的な電子メールメッセージ）として分類されるべきかどうかを決定するために解析され得る（ブロック４２４）。電子メールメッセージを解析するための１つの例示的な処理は、図５を参照することによって以下に記載される。

【００８３】

特定の実施形態に従って、プラントする処理はフィードバックループ（例えば、上記したものを含む）をインプリメントし得る（ブロック４２６）。単なる例として、入来する電子メールメッセージが解析される場合には、入来する電子メールメッセージのアドレスは、そのアドレスが調べられ得ることにより、任意の生成されたおよび／またはプラント

されたアドレスに相関するかどうかを決定する。相関する場合には、ルックアップが（例えば、追跡データベースを検索することによって）行われ得ることにより、アドレスがどこにプラントされたかを決定し、フィードバックはアドレスジェネレータ（および／またはアドレスをプラントする責任がある任意の他のツールまたは実体）に提供され得ることにより、そのアドレスに対するプラントする位置が、スパムおよび／またはフィッシュ電子メールメッセージの供給源となる可能性があることを指示する。次いで、所望される場合には、このような位置は追加のプラントする操作のための位置として優先順位が決定され得る。

【００８４】

一部の実施形態においては（例えば、ここで生成されたアドレスは複数の位置にプラントされる）、フィードバック処理はさらに洗練され得る。例えば、特定のアドレスが複数の位置にプラントされた場合には、ただ単に入来するフィッシュ／スパムメッセージのアドレスを確認することだけでは、プラントする位置のどちらがメッセージを生じたかを決定するためには不十分であり得る。このような場合においては、任意のいくつかの手順が、どちらのプラントする位置がメッセージを生成したかについてのさらなる情報を提供するために使用され得る。単なる例として、三角測量手順が使用され得る。アドレスＡが位置ＸおよびＹにプラントされた一方で、アドレスＢが位置ＹおよびＺにプラントされ、アドレスＣは位置ＸおよびＺにプラントされたという状況を考慮する。フィッシュメッセージがアドレスＡおよびＣにより受信される場合には、位置Ｘはフィッシュメッセージを生成したプラント位置であった可能性がある。同様に、フィッシュメッセージがアドレスＡおよびＢによって受信される場合には、位置Ｙはフィッシュメッセージを生成したプラント位置であった可能性があり、以下同様である。（特定の生成されたアドレスに対するプラント位置の選択は、このような三角測量を行うための能力を強化するように構成され得ることに注意されるべきである）。

【００８５】

別の例示的な手順は、どちらのプラントする位置がフィッシュメッセージを生成したかを識別する情報について、入力メッセージを解析することを含み得る。単純な場合においては、メッセージが発信されたドメインは、アドレスがプラントされたドメインと相関し得る。（一部の場合には、本明細書の他の箇所に記載されるように、ドメイン解析はこの解析を洗練するために使用され得る。単なる例として、プラントする位置に対するＷＨＯＩＳ記録は、フィッシュメッセージが発信されたドメインについて対応するＷＨＯＩＳ情報にマッチする任意の情報を見出すために解析され得る）。他の場合には、フィッシュメッセージは、プラントされたアドレスに提供される情報（例えば、名、姓など）と相関され得、このような情報は、どちらのプラントする位置がメッセージを生じたかを決定するために使用され得る。本明細書の開示に基づいて、当業者は、種々の手順が、いくつかのプラントする位置のどれがフィッシュメッセージを生じたかを確認するために使用され得ることを理解する。

【００８６】

図４Ｂは、潜在的な詐欺的な活動（フィッシング／スプーフィング詐欺を含む）についての情報を取得するために使用され得る別の方法４３５を図示している。図４Ｂの方法４３５は、一部の場合においてはハニーポット、相関エンジンおよび／またはイベントマネージャ（例えば、上記したような）を使用してインプリメントされ得、方法４３５は、任意の適切なデータ供給源（上記したデータ供給源１０５を含むがこれに限定はされない）から情報を獲得するために使用され得る。一部の実施形態に従って、方法４３５は、データ供給源にアクセスすることを含み得る（ブロック４４０）。データ供給源にアクセスすることは、データ供給源のタイプ、所望される情報のタイプおよび／または他の適切な因子に依存する任意の種々の手順を包含し得る。単なる例として、一部の実施形態においてはデータ供給源にアクセスすることは、データ供給源をクロールするために処理（この処理は無人のものおよび／または自動化されたものであり得る）を使用することを包含し得る。従って、例えば、データ供給源がウェブサイトである場合には、ウェブサイト上の１

つ以上のファイルがクロールされ得（すなわちアクセスされ得および／またはダウンロードされ得）、このようなファイルはオプションとして、詐欺防止システムにローカルにセーブされ得る。他の場合には、ウェブ検索エンジン（例えば、Ｇｏｏｇｌｅ™、Ｌｙｃｏｓ™など）が情報を検索するために使用され得る。データ供給源がアクセス制限されたデータ供給源である場合には、データ供給源にアクセスすることは、１つ以上の認証手順（例えば、ユーザネームおよび／またはパスワードを提供すること）を含み得、認証手順は、手動で、相互作用的に、および／または自動化様式で行われ得る。別の例として、例えば、データ供給源がオンラインのチャットルームである場合には、データ供給源にアクセスすることは、チャットルームにログオンすることを含み得る。さらなる場合には、データ供給源にアクセスすることは、例えば、定期的ベースまたは必要に応じたベースで、データ供給源全体をダウンロードすること、および／またはダウンロードされたデータ供給源にアクセスすること（読み込むこと、解析すること、検索することなど）を含み得る。単なる例として、ドメインレジストレーションゾーンファイルは定期的ベースでローカルにダウンロードされ得、ゾーンファイルに対する検索は、より素早くおよび／またはオフラインの様式で行われ得る。

【００８７】

特定の実施形態においては、データ供給源にアクセスすることは、そのデータ供給源をモニタリングすることを含み得る。データ供給源をモニタリングすることは、一部の場合においては、定期的ベースでデータ供給源にアクセスすることを含み得る。一部の実施形態に従って、データ供給源をモニタリングすることは、データ供給源の以前のアクセス以来発生する変化（例えば、追加のおよび／またはアップデートされた情報）に対してデータ供給源の評価をすることを包含し得る。単なる例として、ドメインレジストレーションゾーンファイルがモニタされ得ることにより、ドメインレジストレーションに対する変更を見出す（以下にさらに詳細に記載される）。他の実施形態においては、データ供給源をモニタリングすることは、データ供給源がアクセスされている間に発生するデータ供給源に対する変化を追跡することを包含し得る。一例として、データ供給源がオンラインのチャットルームである場合には、データ供給源をモニタリングすることは、チャットルーム内で起こるオンラインの「会話」を見ることと、ダウンロードすることと、コピーすることなどを、含み得る。多少類似しているが、データ供給源がニュースグループである場合には、ニュースグループは新しい通知、返信などについてモニタされ得る。

【００８８】

方法４３５はまた、アクセスされた／モニタされたデータ供給源から情報を獲得することを含み得る（ブロック４４５）。データ供給源にアクセスすること／モニタリングすることと同様に、情報を獲得することは、種々の形式をとる。例えば、データ供給源がファイルまたはファイルのセット（例えば、ウェブサイト、ドメインレジストレーションファイル、ニュースグループ）である場合には、情報を獲得することは、ファイルを（例えば、キーワードなどで）検索することを包含し得る。単なる例として、情報は、ＵＲＬおよび／または関連する用語（例えば、「フィッシュ」、「スプーフ」、「詐欺」など、ならびにこのような単語の変形）の検索によって獲得され得る。特定の顧客の名前はまた、これらの名前の存在が、顧客に関与し得る、詐欺的な活動の可能性を指示し得る場合には、検索用語であり得る。このような単語を含むファイルは、さらなる解析のためにダウンロードされ得、および／または分類され得る。他の場合においては、情報を獲得することは、ＵＲＬおよび／または関連用語を備える情報を含む関連情報を含むオンラインのチャットセッションの記録をコピーすることおよび／またはログすることを包含し得る。

【００８９】

例えば、データ供給源がモニタされる場合を含む特定の実施形態においては、情報を獲得することは、データ供給源に対する任意の変更をダウンロードすることを、および／またはデータ供給源がモニタされない場合には、その記録を作成することを包含し得る。このことは一般的に（すなわちデータ供給源の全変更に関して、および／またはデータ供給源に含まれる情報に関して）および／またはオプションとして（すなわち関連情報に関し

てのみ）なされ得る。単なる例として、ドメインレジストレーションゾーンファイルがモニタされる場合には、レジストレーション記録に対する全ての変化は、記され得および／またはダウンロードされ得る。あるいは、特定の判定基準（例えば、クライアントのドメインネームおよび／または商標に怪しげに類似する新しいドメイン、あるいはスパムメール送信者、フィッシュメール送信者および／またはスプーフ送信者に応じると考えられる新しいドメイン）に合う変化のみが、記され得および／またはダウンロードされ得る。特定の場合において、有用なドメインネームの有効期限が切れる（例えば、ドメインネームが「有効期限切れ」とマークされ、および／またはドメインネームがドメインレジストレーションゾーンファイルから消える）場合には、その情報は、図４Ｃの参照によってさらに詳細に記載されるように、記され得る。

【００９０】

通常の場合には、情報を獲得することは、任意の行動を包含し得、任意の行動によって、情報はデータ供給源から取得され得る。さらに、本明細書の開示に基づいて、当業者は、データ供給源にアクセスすることを獲得することおよび情報を獲得することの手順が、１つの手順に統合され得ることを認識する。一部の場合には、情報を獲得することの処理はまた、新しい情報が獲得され、かつ評価されることが必要であると、管理者に通知すること（および／または自動化処理）を含み得る。この通知は、電子メールメッセージ、中間処理ソフトウェアメッセージ、アプリケーションの呼び出しなどを含むがこれらに限定はされない。特定の場合においては、獲得された情報は、特定の位置（例えば、データベースまたは他のデータ構造、ファイルシステムの特定のディレクトリなど）に配置され得、および／または処理は、評価されるべき新しい情報の位置をモニタし得る。それゆえ、通知は、正確な位置に情報を配置することを、単純に包含し得る。

【００９１】

一旦情報が獲得されると、その情報は評価され得る（ブロック４５０）。情報の評価は、自動化処理によって、および／または人間の技術者によって行われ得る。一部の場合には、評価は情報を獲得する処理の間に行われ得る。通常の意味においては、情報を評価することは、情報がさらなる行動を要求する可能性があるかどうかの決定を行うこと、および／またはどのタイプの行動が要求され得るかを決定することを包含し得る。それゆえ、情報を評価するための手順は、獲得された情報のタイプの少なくとも一部に依存して、顧客の優先度（例えば、顧客ポリシーに記されるように）を変更する可能性がある。

【００９２】

単なる例として、情報が疑わしいフィッシング詐欺に関する場合には、情報の評価はＵＲＬに対する情報を解析することを包含し得る。ＵＲＬが見出される場合には、そのことは、ＵＲＬのさらなる調査が行われるべきであることを指示し得る。同様に、情報が、スパム供給源および／または収集操作の可能性を指示する場合には、情報は、収集するためのおとりの電子メールアドレスをプラントする確率をさらに調査するために適切であり得る。他の実施形態においては、獲得された情報は、ドメイン活動（例えば、新しいレジストレーション、有効期限が切れたレジストレーションなど）を指示し得、情報の評価は、ドメイン活動がさらなる行動を正当とするかどうかを評価することを含み得る。

【００９３】

単なる例として、特定の場合に、獲得された情報が疑わしいドメインが登録されていることを指示する場合には、ドメインをモニタすることは適切であり得る（ブロック４５５）。（一部の場合には、ドメインをモニタリングすることは、評価の処理の一部として考慮され得る）。特定の実施形態に従って、ドメインをモニタリングすることは、ドメインを活動について、可能性としては定期的に（例えば、１５分ごとに、１時間ごとに、１日ごとになど）チェックすることを包含し得る。活動についてドメインをチェックすることは、ドメインにおけるウェブサイトへのアクセスを（例えば、ＨＴＴＰ　ＧＥＴ要求を、ドメイン自体および／またはドメインにおける一般的なホストネーム、ｗｗｗ、ｗｅｂなどのいずれかに送信することによって）試行することと、サーバに対してドメインを問い合わせることと、ドメインレジストレーション記録および／またはＤＮＳ記録などをモニ

タリングすることと、を包含し得る。ドメインが「生きて」いる場合には（すなわち、サーバがそのドメインにおいて操作を始める）、そのことは詐欺的な活動の可能性のさらなる調査に対する必要性を指示し得る。

【００９４】

情報の評価（および／またはドメインのモニタリング）が、さらなる調査が必要であることを指示する場合には、このような調査は行われ得る。一部の実施形態に従って、例えば、イベントマネージャにおいて、調査はイベントを作成することにより開始され得（ブロック４６０）、および／またはそうでない場合にはさらなる調査の必要性の記録を作成する。図６（以下に記載される）は、詐欺的な活動の可能性を調査する例示的な方法の一部を図示しており、ブロック６０５（同じく以下に記載される）はイベントを作成するための１つの手順を図示している。一部の実施形態においては、イベントは、調査および／または応答に対する優先順位が付けられ得る。一部のイベントは、他のイベントよりも相対的に決定的ではないように判断され得、どちらのイベントがより決定的であると考慮されるかの決定が任意に決定される。単なる例として、一部のタイプのオンラインの詐欺（例えば、偽の時計の販売）が、他のタイプよりも有害でないように判断され得る（例えば、個人情報を収集するための試行）。一部の場合においては、大域的なパラメータ（ｇｌｏｂａｌ　ｐａｒａｍｅｔｅｒ）は、全ての顧客に対して、異なるタイプのイベントの相対的な緊急性を定義し得る。他の場合においては、特定の顧客のプロファイルが、その顧客に対して、どちらのイベントが相対的により緊急なものとして扱われるべきかを指示するように構成され得る。いくつかのレベルの緊急性があり得、かつ／または上記レベルは、色（例えば、黄、オレンジ、赤）、数字（例えば、１～５）、および／またはシステム、技術者および／または任意の他の関心のあるパーティを特定のイベントの比較的な緊急性を識別することにおいて援助するための任意の他の適切なスキームを使用して、識別され得る。

【００９５】

本発明の特定の実施形態に従う、方法４００がどのようにドメインをモニタするために使用され得るかの例として、以下のシナリオを考慮する。会社「Ａｃｍｅ　Ｐｒｏｄｕｃｔｓ」が、そのブランド名に関連するフィッシングスキームを回避したいと願う場合には、会社（および／または、例えば、第三者のセキュリティサービスプロバイダ）は、データ供給源としてゾーンファイルをモニタすることを選択し得る。データ供給源のモニタリングを介して、ドメイン＜ａｃｍｅｐｒｏｄｕｃｔ．ｃｏｍ＞が登録されていることが発見される。本発明の方法に従って、例えば、定期的にＨＴＴＰ　ＧＥＴ要求をドメインに対して（および／または、ｗｗｗ．ａｃｍｅｐｒｏｄｕｃｔ．ｃｏｍのようなそのドメイン上のホストに対して）作成することによって、モニタリングシステムはそのドメインをモニタし得る。一旦ドメインが利用可能になると（すなわち、ＨＴＴＰ　ＧＥＴ要求が故障以外の何かを返す）、システムはウェブサイトをクロールするように構成され得、ウェブサイト上の１つ以上の（可能性としては全ての）利用可能なページの「スナップショット」をとる。スナップショットは、ページ自体のコピー、ならびに／あるいは例えば、ページのコンテンツから算出される、１つ以上のチェックサムおよび／またはハッシュ値、を単に備え得る。この手順は、定期的に継続され得（例えば、１分に１回、１時間に１回、１日に１回など）、かつ／またはこのような定期的なスナップショットは、一方が他方と比較され得る（例えば、戻されたページなどに対してハッシュ値を素早く比較することによって）。当業者は、開始の段階において、ドメインが、通常はウェブサイトが「構築中」などであることを指示する「パーク」ページを有することを認識する。それゆえに、ウェブサイトが「稼動」する（すなわち、ウェブサイトがパークページ以外のいくつかのコンテンツを有する）場合には、定期的なスナップショットの比較が、この変化を明らかにする。ウェブサイトが稼動する時点で、ウェブサイトの調査および／または解析が行われ得る。例えば、特定の実施形態においては、イベントがイベントマネージャにおいて開かれ得、かつ／または本明細書の他の箇所に記載される調査／解析手順が行われ得る。従って、ドメインをモニタすることによって、フィッシング操作の可能性は、フィッシュメ

ッセージが送信される前に（および、結果として任意の顧客がフィッシング操作によって騙される前に）明らかにされ得る。

【００９６】

本発明の他の実施形態は、追加の入来するスパムメッセージを促進するために使用され得る方法を提供する。図４Ｃは、１つのこのような方法４６５を図示している。このような方法によって促進されたメッセージは、一部の実施形態においては、図４Ａに関して記載される様式と類似した様式で処理され得、かつ／または以下にさらに詳細に記載されるように解析され得る。通常は、方法４６５は、有効期間切れのドメインの獲得およびこれらのドメインに対してアドレスされた電子メールメッセージの収集に関連する。当業者が認識するように、一旦ドメインが有効切れになると、そのドメインにおける受信者に対してアドレスされた電子メールは、通常は、受信者に対してもはや発送されない。このような受信者は、それゆえ通常は、新しい電子メールアドレスを獲得し、これらの新しいアドレスを彼らの文通者（ｃｏｒｒｅｓｐｏｎｄｅｎｔ）に通知し、文通者はその後有効期限切れのドメインにおけるアドレスではない新しいアドレスを使用する。従って、多くの場合には、未だに有効期限切れのドメインに送信されている任意の電子メールメッセージは、スパムメッセージであるという平均よりも高い確率を有する。

【００９７】

方法４６５は、ドメイン情報にアクセスすることを包含し得る（ブロック４７０）。多くの場合には、ドメイン情報にアクセスすることは、関連するデータ供給源（例えば、ドメインレジストレーションゾーンファイル）にアクセスすることおよび／またはそのデータ供給源から情報を獲得することを包含し得る。上記した手順は、この様式でドメイン情報にアクセスするために使用され得る。他の場合には、種々のリソースは、ドメイン情報（単なる例として、有効期限切れのドメイン（および／または有効期限切れ間近のドメイン）を識別するニュースレターの購読を含む）、ドメインを無断占拠する（ｄｏｍａｉｎ－ｓｑｕａｔｔｉｎｇ）ウェブサイト（これはしばしば有効期限切れのドメインを売りに出す広告を出す）、および／または同様のものにアクセスするために使用され得る。

【００９８】

方法４６５は、スパムメッセージを引き込むためのドメインの適合性を評価することをさらに包含し得る（ブロック４７５）。単なる例として、スパムメール送信者は、時折メッセージを人口統計学によって送信し、このようなスパムを引き込むための任意の試行は、このような人口統計学をシミュレートすることを試行し得る。例えば、特定のドメイン（例えば、＜ｍｕｓｃｌｅｃａｒｓ．ｃｏｍ＞）は、そのドメインにおいて電子メールを受信するユーザが自動車のファンである可能性があることを指示し得、および／または別のドメイン（例えば、＜ｆｉｎｅａｒｔｓ．ｃｏｍ＞）は、そのドメインにおいて電子メールを受信するユーザが芸術のファンである可能性があることを指示し得る。他のドメインは、他の適当な人口統計学（例えば、女性のユーザ、男性のユーザ、若者のユーザなど）を指示し得る。

【００９９】

他の要因は、ドメインの適合性を評価することにおいて考慮され得る。単なる例として、比較的に長期間登録されているドメインは、比較的に短い歴史を有するドメインよりも多くの量のスパムを受信する可能性が高い。従って、ドメインの適合性を評価することは、ドメインが登録されているおよび／またはドメインが存在する時間の長さの解析を含み得る。このような解析は、関連するドメインレジストレーション記録の調査、アーカイブされたウェブサイトなどを記憶する様々なアーカイブサイト（単なる例として、＜ａｒｃｈｉｖｅ．ｏｒｇ＞を含む）のレビューを含み得る。さらに、ドメインレジストレーションが既に有効切れである場合には、ドメインが最後に使用されてからの時間の長さが要因として考慮され得る。最近有効切れになったドメインは、長く有効期限切れであるドメインに比べてスパムを受信する可能性が比較的高い。

【０１００】

ドメインレジストレーションが既に有効期限切れである場合には、方法４６５は、ドメ

インレジストレーション記録（および／または有効期限切れのデータ供給源）をモニタリングすることを含み得る（ブロック４８０）。単なる例として、当業者は、典型的なドメインレジストレーション記録（例えば、ゾーンファイル内の記録）が、しばしば、ドメインの有効期限の日付の指示を提供することを理解する。適切なドメインが見出される場合には、有効期限の日付は記され得、かつ／またはデータ供給源（例えば、ゾーンファイル）は、スケジュールされた有効期限の日付あたりでモニタされ得ることにより、ドメインレジストレーションが更新されるか、または有効期限が切れるかを決定する。同様に、ゾーンファイルアップデートは、有効期限切れのドメイン（上で議論された）に対してモニタされ得、このようなドメインは、適合性に対して評価され得る。結果として、様々な実施形態に従って、ドメインの適合性を評価するための手順およびドメインの有効期限をモニタリングするための手順が、任意の適切な順序において発生し得る。ある実施形態においては、ドメインの有効期限をモニタリングすることは、例えば、上記された手法を用いて、ドメインにおける任意の活動をモニタリングすることを含み得る。

【０１０１】

適切な有効期限切れの（そうでなければ利用可能の）ドメインが見出される場合には、そのドメインが獲得され得る（ブロック４８５）。一部の場合には、ドメインを獲得することは、適切な登録機関によって、当業者に馴染みの手順によって、ドメインを登録することを包含し得る。この手順は自動化され得かつ／または技術者によって手動で行われ得る。他の場合には、ドメインを獲得することは、第三者からドメインを購入することを包含し得る。このような場合には、ドメインの再登録が要求され得る。選択的に、ドメインに関連するおとりの電子メールアドレスは、例えば、収集のためにシードおよび／またはプラントされ得る（ブロック４９０）。おとりのアドレスをシードする／プラントするための１つの例示的な手順は、図４Ａに関連して上で議論される。他の手順は、同様に使用され得る。

【０１０２】

メールサーバ（これはハニーポットであり得る）は、ドメインにおける受信者に対してアドレスされたメールを受信するように構成され得、かつ／またはドメインに対して送信された電子メールメッセージは、メールサーバによって受容され得る（ブロック４９５）。受容されたメッセージは、次いで本明細書で議論される他の方法に関連して記載されるように、および／または所望されるように処理され得る。特定の実施形態に従って、システムは、入力メッセージが有効な受信者に対してアドレスされているかどうかにかかわらず、そのドメインに対する全ての入力メッセージが受容されるように構成され得る。実際は、無効な受信者のアドレスに対してアドレスされたメッセージは、スパムおよび／またはフィッシングの試行である可能性が高くあり得る。例えば、一部のメッセージはそのドメインの以前のユーザにアドレスされたことが予測され得、上記したように、このようなメッセージが大量送信のメールであることは、比較的に可能性が高い。

【０１０３】

本発明のさらなる実施形態は、任意の受信される情報および／またはメッセージ（上記される方法の結果として受信される情報／メッセージを含むがこれらに限定はされない）を解析するために、調査するために、および／またはそれらに応答するために使用され得る。例えば、図５は、本発明のある実施形態に従って、入力電子メールメッセージ（またはデータファイル）を解析する方法５００を詳細に図示している。（図５の議論においては、用語データファイルおよびメッセージは、相互転換可能に使用される。なぜならば、解析の方法はメッセージおよびデータファイルに等しく適用し得るからである。上記したようにメッセージおよびデータファイルは、受信される電子メールメッセージに対応し得るが、それらは任意の他のデータセットにも対応し得る。任意のデータセットは、種々の異なるデータ供給源（ニュースグループの通知、ウェブページ、および／または同様のもの）から獲得され得る。同様に、本明細書で議論される他の方法は、このようなデータセットおよび／またはデータ供給源に対応するデータファイルに適用され得る）。図５に図示される手順の一部は、特定の実施形態においては、図５により図示される方法５００（

例えば、入力電子メールメッセージを収集すること（ブロック５２５）を含む）における他の点において発生し得ること、ならびにこれらの方法における手順（および実際は、本明細書に記載される全ての方法）の組織化は、単に記載を簡単にするためのみであることに注意されるべきである。特定の手順は、本明細書で記載されるものに比べて順序において異なって発生し得、実際は、様々な手順が本発明の様々な実施形態に従って、追加されおよび／または省略され得る。

【０１０４】

図５によって図示される方法５００は、メッセージ（および／または解析されるべき任意の他のデータ）にタイムスタンプすることと、および／またはメッセージ／データに識別子を割り当てること（これはメッセージを一意的に識別するのに十分であり得る）とを含み得（ブロック５０５）、これはメッセージの識別（例えば、本明細書で議論される処理の全体にわたって）を支援し得、メッセージが受信される場合に永続的な指示を提供し得、および／または異なるメッセージの比較を円滑にし得る。識別子を発生するための手順は任意に決定される。単なる例として、識別子は、いつメッセージ／データの解析をするかについての情報（例えば、タイムスタンプ）、メッセージの供給源の指示子などを含み得る。あるいは、識別子（および／または識別子の構成要素）は、連続的におよび／またはランダムに割り当てられ得、かつ／または識別子は解析されるためのデータのタイプを識別し得る（例えば、ドメインレジストレーション、電子メールメッセージなど）。

【０１０５】

方法５００はまた、一部の実施形態においては、可能性としては上記された様式でメッセージからデータファイルを作成すること（ブロック５１０）を含み得る。（上記されたように、文脈上他に明確に示さない場合には、電子メールメッセージ、他のデータ（例えば、ドメインレジストレーション、受信されるＵＲＬなど）、およびこのようなメッセージ／データから作成されるデータファイルは、類似の様式で処理され得、本明細書の手順の記載は、通常は、必要な場合には適切な変更を行い、任意のこれらのアイテムに等しく適用され得る）。データファイルは、例えば、データファイルを相関エンジンに伝送することによって、および／またはデータファイルを収集されたコンピュータ（例えば、ハニーポット）からデータファイルをダウンロードする相関エンジンによって、収集され得る（ブロック５１５）。（一部の場合には、データファイルを収集することは必要ではあり得ない。例えば、相関エンジンおよびハニーポットは、１つのソフトウェアプログラムまたはプログラムモジュール内に組み込まれ得、および／または同一のコンピュータ上で実行し得る）。

【０１０６】

データファイルは、次いで、相関エンジンによって解析または読み取られ得る（ブロック５２０）。解析は、データファイルを、様々なセクションおよび／またはフィールドに分割し得、解析はデータファイルのフィールドおよび／またはセクションが、相関エンジンによって解析されることを可能にし得る。例えば、電子メールメッセージに関して、例えば、ヘッダ情報が解析され得ることにより、ヘッダに供給源および／またはあて先が作り出されるかどうかを決定する（ブロック５２５）。そうである場合には、電子メールがフィッシュであることは、比較的に可能性が高い。別の例として、メッセージヘッダ内のルーティング情報は解析され得ることにより、メッセージが疑わしいドメインから発生したか、および／またはメッセージが疑わしいドメインを通って発送されたかどうかを決定し、さらにメッセージがフィッシュである可能性が強化される。

【０１０７】

電子メールメッセージの本体を含むがこれに限定はされない任意のテキスト（すなわち、データファイルの本体フィールド）は、次いで解析され得る（ブロック５３０）。本体の解析は、本体をブラックリストおよび／またはホワイトリストに列挙される用語で検索することを含み得る。単なる例として、ブラックリストに列挙される用語は、フィッシュメッセージにおいて共通に見出される用語（例えば、「自由旅行」）、メッセージが個人情報を参照することを指示する用語（例えば、「クレジットカード」、「認可」、「確認

」など）、および／またはブランド名、顧客の名前などを含み得る。逆に、ホワイトリストに列挙される用語は、メッセージがフィッシュではないことを共通に指示する用語である。メッセージがフィッシュであると最終的に決定される場合には、ブラックリストに列挙される用語のリストは、そのメッセージのテキスト（またはそのテキストの一部分）が含まれるように自動的にアップデートされ得るように、システムがフィードバックループを提供するように構成され得ることに、この点で注意されるべきである。さらに、相関エンジン（および／または任意の他の適切な構成要素）は、一般的なフィッシュ戦術（例えば、明らかなスペル間違い、不要情報のテキストおよび同様のもの）を打ち負かすように設計されている発見的アルゴリズムを含み得る。同様に、システムは基語（ｒｏｏｔ　ｗｏｒｄ）の共通の文法上の変更を識別するように、「ステミング（ｓｔｅｍｍｉｎｇ）」論理をインプリメントし得る（例えば、「行っている（ｇｏｉｎｇ）」、「行く（ｇｏｅｓ）」、「行った（ｇｏｎｅ）」などの単語は、「行く（ｇｏ）」の変形として識別され得、逆もまた同様である）。

【０１０８】

メッセージの本体を解析することは、他の形式の解析を同様に含み得る。単なる例として、本体が、ＵＲＬまたは他の形式のあて先変更を含む場合には、これらのデバイスの存在はまた、メッセージがフィッシュである（または逆にメッセージがフィッシュではない）より高い可能性を指示し得る。（加えて、ＵＲＬおよび他のあて先変更のデバイスは、以下に記載されるように個別に解析され得る）。さらに、他の要因（例えば、電子メールメッセージの本体の長さ、本体が画像を含むかなど）は、電子メールメッセージの本体の解析において考慮され得る。

【０１０９】

加えて、メッセージがＵＲＬを含む場合には（あるいは任意の他の形式の参照および／またはあて先変更）、ＵＲＬは解析され得る。（この解析はまた、別の供給源から受信されるＵＲＬ（例えば、ＩＳＰによって伝送されるＵＲＬのリスト、疑わしいウェブページのＵＲＬ、疑わしいドメインレジストレーションに関連するＵＲＬなど）に適用され得る）。例えば、ＵＲＬに関連するドメインに対するネットワークデータ（ＤＮＳおよび／またはＷＨＯＩＳデータ、ならびにネットワーク記録（例えば、ＡＲＩＮ）を含むがこれらに限定はされない）は、アクセスされ得る。このデータが、ＵＲＬがドメインに分離されないことを指示する場合には（例えば、ＵＲＬがＩＰアドレスにのみ分離される）、ＵＲＬはフィッシング詐欺の一部であり得る。同様に、当業者は、フィッシング詐欺はしばしば米国の外のサーバ／ドメインに基地を置くこと、同様に特定のドメインはフィッシング詐欺をホストする可能性があることが公知であり得ることを認識し得る。それゆえ、ＵＲＬが疑わしいドメインまたはグローバルトップレベルドメイン（「ｇＴＬＤ」）に分離される場合には、ＵＲＬはフィッシング詐欺の一部であり得る。別の例として、ＵＲＬ（および／またはＵＲＬに関連するドメインおよび／またはＩＰアドレスに対するネットワークデータ）は、電子メールヘッダ内の情報（例えば、供給源のアドレス、「ＦＲＯＭ」フィールドなどを含む）および／またはこのようなヘッダ情報に関連するネットワークデータと比較され得る。この比較が矛盾を明らかにする場合には、そのメッセージがフィッシュであることは比較的に可能性が高くあり得る。逆に、この情報が一貫している場合には、メッセージがフィッシュではないことが、比較的に高い可能性であり得る（が、必ずしもそうではない）。

【０１１０】

一部の実施形態においては、ＵＲＬ（任意の供給源から取得される）を解析することは、１つ以上の詳細なテストを含み得る。図５Ｂは、種々のこのようなテスト（任意のこのようなテストは、実施形態に依存して、様々な順序および／または組み合わせで行われ得る）を含む例示的な方法５６０を図示している。例えば、１つのテストは、ＵＲＬをテストすることを包含することにより、ＵＲＬが「生きている」（すなわち、ＵＲＬによって参照されるウェブページなどが利用可能である）ことを決定する（ブロック５６２）。このテストは、ウェブブラウザ、ＨＴＴＰ　ＧＥＴ要求などを使用して行われ得る。さらに

、ＵＲＬによって参照されるサーバおよび／またはドメインに対するＤＮＳ情報は（任意のいくつかの共通な方法を使用して）取得され得、および／または解析され得る（ブロック５６４）（例えば、ＵＲＬが参照するサーバのＩＰアドレスおよび／またはネットワークブロックを決定するために）。同様に、ドメインに対するＷＨＯＩＳ情報が、取得され得および／または解析され得ることにより、例えば、誰がドメインを所有するかを決定する（ブロック５６６）。特に、ドメインに対する任意の特定の識別情報（例えば、コンタクトネーム、住所、電子メールアドレス、電話番号など）が記され得る。これらの手順により取得される任意の情報は、将来の参照のために記憶され得、および／または以前の解析を介して取得される類似の情報と比較され得る。このようにして、例えば、繰り返しの違反者（ｏｆｆｅｎｄｅｒ）が、効果的に識別され得る。単なる例として、解析されたＵＲＬに関連するドメインが、オンラインの詐欺と関連があると先に見出されたドメインと、同じコンタクト電子メールアドレスを有する場合には、現在のＵＲＬは詐欺と関連があるという、比較的高い可能性があり得る。

【０１１１】

一部の実施形態に従って、ＵＲＬをホストするサーバの地理的な位置が決定され得る（ブロック５６８）。当業者は、サーバの地理的な位置を決定するための（例えば、そのドメイン名および／またはＩＰアドレスに基づく）種々の公知の手順があり、かつ任意のこれらの手順が使用され得ることを認識する。サーバの地理的な位置は、サーバが詐欺的な活動に従事している可能性があるかどうかの指示を提供し得る。単なる例として、東ヨーロッパに位置するサーバが、アメリカに位置する会社に関連すると称するウェブサイトをホストしている場合には、ウェブサイトは詐欺であることが比較的高い可能性であり得る。加えて、サーバの位置を決定することは、どの管理上の応答および／または技術応答が、そのサーバによって提供されるウェブページに対して利用可能であるかの指示を提供し得る。

【０１１２】

ＵＲＬ自体の構成はまた、ＵＲＬが詐欺のウェブサイトを参照する可能性があるかを明らかにする。単なる例として、多くの場合には、正当な会社のウェブサイトを参照するＵＲＬは、ウェブサーバに対するルート（デフォルト）パス（例えば、「／」または可能性としてはルートパスのサブディレクトリ（例えば、「／ｖｅｒｉｆｙ／」））のようなかなり単純なディレクトリパスを有する。回旋状のまたは異常なディレクトリパスを有する任意のＵＲＬは、それゆえに、詐欺的な活動に従事しているという可能性が高くあり得、ＵＲＬ自体の検査は、この事実のいくつかの指示を提供し得る。従って、方法５６０は、一部の場合には、ＵＲＬのディレクトリパスを評価することを含み得る（ブロック５７０）。単なる例として、ＵＲＬがユーザディレクトリ（例えば、「／～ｊｓｍｉｔｈ／」）を参照する場合には、ＵＲＬは不正なウェブサイトを参照するという可能性が比較的に高くあり得る。なぜならば、正当な会社のウェブサイトがユーザのディレクトリ内に存在することは予想されないからである。詐欺師はこの事実を認識しているので、詐欺師は時折、例えば、ＵＲＬのあて先変更を用いてウェブサイトのディレクトリパスを不明瞭にすることを試行し、これはしばしば比較的に慣習的でないＵＲＬという結果を生じる。従って、ＵＲＬのコード化はまた、検査され得る（ブロック５７２）。ＵＲＬが慣習的でないコード化（例えば、ディレクトリパスの位置におけるキャラクタ文字列など）を有する場合には、このような慣習的でないコード化は、ＵＲＬが暗黙のあて先変更（例えば、不明瞭なパスへと）を含むことを指示し得、ＵＲＬは不正なウェブサイトを参照する可能性が比較的に高くあり得ることを意味する。

【０１１３】

一部の場合には、反不正使用情報の供給源（例えば、反不正使用のニュースグループ、電子メールリストなど）は、解析されるＵＲＬに対する参照のために（および／またはホスト、ドメイン、ＩＰアドレスおよび／またはＵＲＬに関連するネットワークブロックのために）検索され得る（ブロック５７４）。これらの反不正使用供給源の１つにおける参照は、ＵＲＬが詐欺的なウェブサイトを参照するということ指示し得る。

【０１１４】
考慮され得る別の要因は、ＵＲＬが暗号化接続（例えば、当業者に公知のＳｅｃｕｒｅｄ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ（「ＳＳＬ」）暗号化スキームによって守られる接続）を参照するかどうかである（ブロック５７６）。例えば、ＵＲＬによって明らかにされるプロトコルが「ｈｔｔｐｓ」である場合には、ＵＲＬは通常は安全な接続とリンクする。あるいは、ＵＲＬによって参照されるリソースをホストするサーバが問い合わせられ得ることにより、例えば、ＵＲＬによって参照されるホストネーム（またはＩＰアドレス）に対するＨＴＴＰＳ　ＧＥＴ要求を提示することによって、サーバが安全な接続を受容するかどうかを決定する。他の手順は同様に使用され得る。暗号化または他のセキュリティの使用は、参照されるウェブサイトが、詐欺的な活動に従事するという可能性が比較的に高く（または低く）あるということを指示し得る。

【０１１５】
安全な接続のテストに加えて、ＵＲＬが参照するサーバおよび／またはウェブサイトは、追加のテストの対象とされ得る。（このようなテストはまた、ウェブサイト／サーバ調査（例えば、図７に関して記載される調査）の一部として行われ得る）。単なる例として、サーバ上のアクティブなポートは、例えば、ポートスキャナおよび／または他の診断ツール（ＮＭＡＰおよびＮｅｓｓｕｓのような上で議論されるものを含むが、これらに限定はされない）を使用して、確認され得る（ブロック５７８）。サーバが「高い」または「未知の」ポート（例えば、１０２４を超える番号が付けられた任意のポート）をリスニング（ｌｉｓｔｅｎｉｎｇ）する場合には、このようなポートの活動は、ウェブサイトが不正なものであるという可能性が比較的に高いことを指示し得る。（加えて、ＵＲＬはさらに評価され得ることにより、ＵＲＬが高いまたは未知のポート番号を参照するかを決定し、これらは類似の指示を提供する）。さらに、サーバがセキュリティの脆弱性を許容することが公知のポート上でリスニングする場合には、サーバが危険にさらされる可能性が比較的に高くあり得、これは詐欺的な活動の向上した可能性を指示し得る。

【０１１６】
一部の場合には、ＵＲＬ（および／または、参照されるページ、最初の１０ページ、リンクの最初のレベルなどのようなウェブサイトの一部）によって参照されるウェブサイトをクロールすることが適切であり得る（ブロック５８０）。この手順は、図７に関連してより詳細に記載される。ダウンロードされたページは、ウェブサイトが、正当であるかどうかの追加の指示を提供し得る。単なる例として、ページは、綴りのおよび／または文法上のエラーをチェックされ得る（ブロック５８２）。このようなエラー（特に、エラーが比較的に多数である場合には）の存在は、ウェブサイトがプロフェッショナルに設計および／または維持されていないこと、それゆえ、詐欺である可能性が比較的に高いことを指示し得る。同様に、方法は任意のＨＴＭＬ形式（および／または該形式のコンテンツ）の存在をテストし得（ブロック５８４）、これは、ウェブサイトの正当性の指示を提供し得る。形式をテストすることは、図７および図８に関連してさらに詳細に記載され、同様の手順がこのコンテキストにおいて使用され得る。

【０１１７】
ダウンロードされたページはまた、ページが他のページ、特にウェブサイトの外のページ（正当なビジネスおよび／または他の詐欺的なサイトに関連するページを含むがこれらに限定はされない）を参照するＵＲＬを含むかを決定するためにチェックされ得（ブロック５８６）、同様に、他のサイト上にホストされる画像を参照するページかどうかを決定するためにチェックされ得る（ブロック５８８）。これらのタイプの参照のいずれかの存在が、ウェブサイトが不正であることが比較的に高い可能性があることを指示し得る。単なる例として、ウェブサイトが銀行のウェブサイトをスプーフしている場合には、スプーフするサイトは銀行の実際のウェブサイトへの外部ＵＲＬリンクを有し得、および／または銀行のウェブサイトによってホストされた画像を（より信頼できると思わせるために）備え得る。

【０１１８】

しばしば、詐欺師は、複数の詐欺を行うこと、および／または保護／告発を回避することの試行において、様々なサーバの中から詐欺的なウェブサイトを（および／またはそのサイトからページを）移動する。さらに、一部の詐欺師は、詐欺を行うためのサーバ上にホストされ得る、予め構築されたウェブページ／ウェブサイトを備える、「ターンキー（ｔｕｒｎｋｅｙ）」詐欺キットを購入（そうでなければ獲得）する。それゆえ、複数の調査からのＵＲＬおよび／またはウェブサイトを比較するための効果的な方法を提供することが有用であり得ることを伴う。単なる例として、一部の場合においては、方法５６０は、ＵＲＬによって参照されるＵＲＬおよび／またはページ（例えば、ＵＲＬによって直接参照されるページおよび／またはブロック５８０においてクロールされるページ）に関連するチェックサムおよび／またはハッシュ値を、生成および／または（例えば、データベース、ファイルシステムなどに）記憶することを含み得る（ブロック５９０）。単なる例として、ＵＲＬ文字列に対する値および／または参照されるページのコンテンツに対する値を計算するためにハッシングアルゴリズムが用いられ得る。あるいは、チェックサム値はこれらのページのコンテンツに対して計算され得る。これらの手順のいずれか（または双方）が、ＵＲＬ、ウェブページおよび／またはウェブサイトの効果的な「スナップショット」を提供するために使用され得る。（一部の場合には、個々のチェックサム／ハッシュが、ＵＲＬ、サイト全体および／またはそのサイトからの個別のページに対して生成され得る）。チェックサム／ハッシュ値は、次いで、以前に調査されたＵＲＬ／ウェブサイトに対して計算される他のこのような値（これは上記されるように、データベース、ファイルシステムなどに記憶され得る）と比較され得る（ブロック５９２）。チェックサム／ハッシュ値が以前に詐欺であると見出されたウェブサイトの値とマッチする場合には、現在のサイトが同様に詐欺であることへの見込みは良好である。

【０１１９】

図５Ａに戻って、ＵＲＬが分離されるドメインについての情報が、個別のステップまたはＵＲＬ解析の一部のいずれかとして解析され得る（ブロック５４０）。さらに、ドメインが疑わしいかを決定する場合に、ドメインはメッセージの本対に含まれる任意のブランド情報と比較され得る。例えば、メッセージの本体が顧客のブランド名を含む場合には、およびその顧客によって所有されるおよび／またはその顧客に関連するドメインと異なるドメインにＵＲＬが分離される場合には、ＵＲＬは疑わしいと考慮され得る。

【０１２０】

（上記されるようにメッセージの任意の部分の、および／またはメッセージ全体の）解析が完了すると、データファイル／メッセージは、一部の実施形態においてスコアを割り当てられ得る（ブロック５４５）。スコアをデータファイル／メッセージに割り当てることは、メッセージがフィッシュである可能性の定量的な測定を提供し得、このような実施形態においては、スコアが閾値スコアと比較され得ることにより、特定の閾値と合うスコアは、さらなる解析および／または調査を結果として生じ得る一方で、その閾値と合わないスコアは、電子メールがフィッシュである可能性がないという判断を指示し得る。一部の実施形態においては、メッセージの解析の全体が１つのスコアの割り当てという結果を生じ得る。

【０１２１】

他の実施形態においては、各々のタイプの解析（例えば、ヘッダの、本体の、ＵＲＬの、および／または関連するドメインの解析）は、個別のスコアの割り当てという結果を生じ得、かつ／またはこれらの個別のスコアは、メッセージに割り当てられ得る複合のスコア（ｃｏｍｐｏｓｉｔｅ　ｓｃｏｒｅ）を形成するために統合され得る。さらに、各々のタイプの解析に対する個別のスコアは、それ自体が複合のスコアであり得る。単なる例として、図５Ｂに関連して記載されるテストの各々（同様に可能性としては他のテストの場合にも）は、スコアという結果を生じ得、これらのテストのスコアは、複合のＵＲＬスコアを形成するように統合され得る。

【０１２２】

さらなる実施形態においては、各々のデータファイルまたは電子メールメッセージの解

析は、階層的な様式で行われ得る。ヘッダ情報は、解析およびスコアされ得、そのスコアがある閾値と合う場合に限って、相関エンジンは本体を解析することにとりかかる。そのスコアが閾値と合わない場合には、メッセージはフィッシュではないと考慮され、解析は終了する。同様に、本体解析から生じるスコアのみが、ある閾値に到達する場合には、ＵＲＬが解析などをされる。

【０１２３】

様々な所見に対するスコアの値は任意であり得、それらは解析における様々な要因の相対的な重要性の判定を反映し得る。さらに、本明細書の開示に基づいて、当業者はメッセージの様々な部分に対するスコアのスケーリングは（および／または解析の次の段階へと進むための閾値スコアは）、メッセージが実際に、フィッシュであるか、ならびにフィッシュメッセージの可能性の識別において所望の精度であるかを決定する各々の部分の解析の相対的な信頼性に依存して調節され得ることを認識し得る。さらに、相関エンジンは、上記したように自動フィードバックループを使用し得、例えば、特定の要因がメッセージの分類における信頼性のある指示子であることが判明するような所望される場合には、相関エンジンが自己同調（ｓｅｌｆ－ｔｕｎｉｎｇ）することを可能にし、相関エンジンはその要因にさらに重みを与えることを自動的に開始し得る。

【０１２４】

どのように階層的なスコアリングシステムが一部の実施形態に従ってインプリメントされ得るかを理解するために、以下の単純化された例を考慮する。作り出されたヘッダを有する電子メールメッセージは、１５０というスコアを与えられ得、１００を超えるスコアが本体の解析を進めるために要求される場合には、その解析は行われる。本体における顧客の名前の存在は、１０００というスコアの価値があり得、用語「あなたのクレジットカードの確認」の存在は、２０００というスコアの価値があり得る。２５００を超えるスコアがＵＲＬ解析に進むために要求され得、メッセージが両方の用語を含む場合には、メッセージは３１５０というスコアを有し、ＵＲＬ解析に進む。最後に、ＵＲＬがＩＰアドレスに分離される場合には、それは１００００というスコアの価値があり得る。メッセージがフィッシュの可能性があると考慮されるための閾値の複合のスコアが１２０００である場合には、メッセージの複合のスコア（１３１５０）は、電子メールがおそらくフィッシュであることを指示する。（図解のために、この例は閾値スコアを超える割り当てられたスコアを要求する一方で、他の実施形態においては、スコアは、閾値に合うように、閾値のスコアよりも低くなる必要があり得ることに注意されるべきである。すなわち、割り当てられるスコアと閾値のスコアとの間に要求される関係は任意に決定される。ホワイトリストに列挙される用語の存在のようなある要因がスコアを減らし得ることにも注意されるべきである）。

【０１２５】

メッセージ／データファイルの解析が完了された後に、メッセージはフィッシュとして分類され得る（ブロック５５０）。一部の実施形態においては、上で議論されたものに類似のスコアリングアルゴリズムが、メッセージを分類するために使用され得る。一部の場合には、分類はメッセージに対する全体のおよび／または複合のスコアに依存し得、一方で他の場合には、分類は特定のセクション（例えば、本体部分、ＵＲＬなど）に対するスコアにのみ依存し得る。分類の他の方法は、同様に使用され得る。例えば、単なる任意の特定のブラックリストに列挙される用語の存在、疑わしいドメインに分離されるＵＲＬなどは、メッセージをフィッシュとして分類させ得る。分類のための判定基準の選択は任意に決定される。

【０１２６】

上記したスコアリングの方法論は、広いコンテキストにおいても同様にデータ（電子メールメッセージ、ＵＲＬ、ウェブサイトなどを含む）の分類に適用され得る。単なる例として、一部の実施形態に従って、類似のスコアリングシステムが、ビジネス製品、商標、ビジネスアイデンティティなどが不適切な様式などで使用されているかを決定するために、ダイレクト電子メールマーケティングを（例えば、競争市場の観点から）識別するため

に使用され得る。本開示の利益によって、当業者は、このロバストなスコアリングの方法論が、広範囲のアプリケーションにおけるこのようなデータの解析のために、種々の異なるスコアリング判定基準を活用し得ることを認識する。

【０１２７】

図６は、疑わしい詐欺的な活動の調査のための方法６００を図示している。一部の場合においては、詐欺的な活動は、受信される電子メールメッセージおよび／またはデータ供給源から（例えば、上で議論されるような、クロールすること／モニタリングすることの活動を通じて）取得されるデータの解析を介して発見され得る。

【０１２８】

一旦、疑わしい詐欺の例が明らかにされると、イベントはイベントマネージャにおいて作成され得る（ブロック６０５）。上記されたように、本発明の一部の実施形態に従って、イベントマネージャは、疑わしい詐欺的な活動を追跡するように構成され得るコンピュータシステム（および／またはソフトウェアアプリケーション）であり得る。特定の実施形態においては、イベントマネージャがワークフロー能力を有し得ることにより、イベントが疑わしい活動についての全ての利用可能な情報のコンテナとして作成され得る。単なる例として、イベントの作成は当業者に公知の「トラブルチケット（ｔｒｏｕｂｌｅ ｔｉｃｋｅｔ）」の作成に類似し得、それによりイベントは、最終的な分離（例えば、疑わしい活動を詐欺でないと分類すること、疑わしい活動の休止など）が、イベントムート（ｅｖｅｎｔ ｍｏｏｔ）と表現されるまで開いたままになり、イベントムートにおいてイベントは閉じられ得る。その間に、様々な調査的なおよび／または応答的な手順（以下に詳細に記載されるものを含むが、これらに限定はされない）は、イベントマネージャにより（自動的におよび／またはユーザの相互作用によって）開始され得、かつ／またはこのような手順の結果の記録は、イベントマネージャによって記憶および／または追跡され得る。この情報の全ては、イベントオブジェクトの中に含まれ得る。上記したように一部の場合には、イベントマネージャがポリシー主導であり得ることにより、顧客ポリシーが特定のイベントが扱われる方法に影響する。それゆえ、イベントは１つ以上の顧客ポリシーにリンクされ得、これらはイベントマネージャおよび／またはイベントを扱う技術者の挙動を通知し得る。

通常は、各々のイベントが調査され得る（ブロック６０５）。一部の場合に、イベントが開かれている場合には、技術者は（例えば、イベントに関連するウェブサイトを訪問することおよび／または解析することによって）イベントを評価し得る。他の場合には、さらに厳しい調査が、例えば、イベントマネージャによって行われ得る。

【０１２９】

図７は、調査の一部として着手され得る様々な手順を詳述する例示的な方法７００を図示している。ブロック７０５において、メッセージに含まれるＵＲＬによって参照されるサーバのＩＰアドレスは、ＤＮＳ照会（またはＵＲＬがホストネームの代わりにＩＰアドレスを参照する場合には、ＵＲＬ自体）のような任意のいくつかの周知の方法を通じて獲得され得る。

【０１３０】

さらに、ＵＲＬによって参照されるサーバに対する見かけのアドレスが識別され得る。当業者は、ＵＲＬが「アンカ（ａｎｃｈｏｒ）」に関連し得、アンカがテキスト、画像などであり得ることにより、アンカがＵＲＬによって参照されるサーバのアドレスであると考えられ、一方で実際のＵＲＬは無関心の観察者には隠されたままであることを認識し得る。（言い換えると、ユーザは、ＵＲＬによって参照されるサーバに、あて先変更されるように、ウェブブラウザ、電子メールクライアントなどにおいてアンカを選択し得る）。このようにして、アンカはＵＲＬによって参照されるアドレスとは実際には異なる「見かけのアドレス」を備え得る。見かけのアドレス（例えば、アンカにおけるアドレス）およびＵＲＬにおいて参照されるサーバのアドレス（すなわちＵＲＬにおける実際のアドレス）の両方が、ホストネーム（通常はドメインを含む）および／またはＩＰアドレスを備え得る。さらに、アンカは、信頼されている実体の識別子（会社名など）を備え得る。見か

けのアドレスがＵＲＬによって実際に参照されるアドレスと異なる（および／または見かけのアドレスが信頼されている実体の識別子を備え、一方でＵＲＬによって実際に参照されるアドレスはその信頼されている実体に関連しない）場合には、ＵＲＬが詐欺であること、および／またはＵＲＬによって参照されるサーバが詐欺的な活動に従事することの可能性が高くあり得る。

【０１３１】

方法７００はまた、例えば、ドメインＷＨＯＩＳ照会を介して、ＵＲＬが分離されるドメインについての情報を調査することを包含し得る（ブロック７１０）。この情報は、ドメインの所有者、ドメインに対して割り当てられるネームサーバ、ドメインの地理的な位置およびドメインに対する管理上のコンタクト情報を示し得る。さらに、ドメインが割り当てられるべきＩＰブロックについての情報が調査され得（ブロック７１５）、ドメインＷＨＯＩＳ照会に対する類似の情報、ならびにドメインが関連すべきＩＰブロックの指示を引き出し得る。さらに、例えば、ＤＮＳ照会を介して（または、ＵＲＬがホストネームの代わりにＩＰアドレスを含む場合にはＵＲＬを通じて）取得されるＩＰアドレスと、ドメインが所属するべきＩＰブロックとを比較することによって、ＵＲＬによって参照されるドメイン情報が認証され得る（ブロック７２０）。ドメイン情報における任意の矛盾は、ドメインがメッセージにおいてスプーフされていることを指示し得、メッセージがフィッシング試行であるという可能性があるというさらなる証拠を提供する。

【０１３２】

ブロック７２５において、ＵＲＬが参照するサーバは、ポートスキャナなどのような種々の市販されているツールを使用して問い合わされ得る。一部の実施形態においては、ＮＭＡＰアプリケーションおよび／またはＮｅｓｓｕｓアプリケーションが、サーバに問い合わせるために使用され得る。実施形態の特定のセットにおいては、これらのツールは、サーバのさらにロバストな問い合わせを提供するように独自のアプリケーション（上で議論したように、他の調査をも行い得る）に組み込まれ得る。サーバの問い合わせは、どのサービスをサーバが実行するか（これはサーバが詐欺的な活動に従事しているかのいくつかの指示を提供し得る）を指示し得る。例えば、サーバが通常のポート上のＨＴＴＰ要求を受容する場合には、そのサービスは、サーバが詐欺的な活動に従事していることを指示し得る（または指示し得ない）。サーバの問い合わせはまた、セキュリティの脆弱性を示し得、これはサーバが危険にさらされ得、それゆえサーバの操作者が知ることなしに詐欺的な活動に従事し得ることを指示し得る。さらに、サーバへのルートは周知の様式でトレースされ得、サーバ、サーバの位置およびサーバが存在するドメイン／ＩＰブロックについてのさらなる情報を提供する。

【０１３３】

サーバに問い合わせすることは、そのサーバによって提供されるウェブページの一部または全て、特に他のサーバ上のページを装っていると思われる任意のページ（スプーフページ）を（例えば、ＷＧＥＴコマンドおよび／または任意の他のＨＴＴＰ　ＧＥＴ機能を使用して）ダウンロードすることを含み得る（ブロック７３０）。ダウンロードされたページは、ページが任意の個人情報を要求するか、および／またはページが個人情報を提供するためにユーザに対してフィールドを提供するかを決定するために解析され得る（ブロック７３５）。さらにダウンロードされたページはアーカイブされ得（ブロック７４０）、これは、ページが実際に詐欺的に個人情報を要求するかの任意の必要な人的評価を助けるために、技術者および／または顧客がページを見ることを可能にし得る。一部の場合には、ページの表現が、本明細書で詳細に記載されるようにセーブされ得る。

【０１３４】

最後に、イベント報告が生成され得る（ブロック７４５）。イベント報告は調査を介して取得される任意のまたは全ての情報を含み得、任意のアーカイブされたページを含む。イベント報告は、技術者により閲覧され得、かつ／または応答戦略を策定することを助けるために顧客に提供され得る。一部の場合には、イベント報告の編集済みのバージョンが顧客に提供され得る。

【０１３５】
もう一度、図６に戻って、調査の結果が、例えば、イベント報告のコピーをモニタリングセンタ（または任意の他の位置）の技術者に表示することによって、報告され得る（ブロック６１５）。オプションとして、技術者が報告を解析し得ることにより、調査において取得される情報への現実直視（ｒｅａｌｉｔｙ　ｃｈｅｃｋ）を提供し、かつ／または応答戦略を策定する（ブロック６２０）。自動化された電子メールメッセージ、技術者からの電話呼び出しなどによって、顧客は、イベントについて、および／または調査結果について通知され得る（ブロック６２５）。技術者はまた、顧客と相談し得ることにより、試行される詐欺にどのように応答するかについて顧客が決定することを可能にする（ブロック６３０）。あるいは、顧客プロファイルは、特定の応答戦略が追求されるべきであることにより、顧客が応答戦略を策定する前に相談される必要がないことを指示し得る。

【０１３６】
調査および／またはイベント報告が、サーバが詐欺的な活動に従事していることを指示する場合には、方法６００は詐欺的な活動へ応答することを含み得る。任意のこのような応答は、自動的におよび／または手動で（すなわち、技術者の指示で）、開始および／または追求され得る。応答は種々の形態をとり得る。単なる例として、顧客、顧客ポリシーおよび／または技術者は、管理上の応答（ブロック６３５）が適切であることを決定し得る。管理上の応答は、サーバに対する直接の応答を伴わない任意の応答を含み得る。例えば、１つの管理上の応答の可能性は、サーバが詐欺的な活動に従事していることを、サーバをホストするＩＳＰおよび／またはサーバのドメインの登録機関に通知することである。別の管理上の応答は、統一ドメインネーム紛争解決ポリシー（Ｕｎｉｆｏｒｍ　Ｄｏｍａｉｎ－Ｎａｍｅ－Ｄｉｓｐｕｔｅ　Ｒｅｓｏｌｕｔｉｏｎ　Ｐｏｌｉｃｙ）（ＵＤＲＰ）下の場合として詐欺的な活動についての法的権限を通知すること、および／または証拠を準備することであり得る。調査が、サーバが危険にさらされ得ることを明らかにする場合には、管理上の応答は、サーバが危険にさらされていることを（可能性としては、イベントの調査の間に取得されるコンタクト情報を通じて）サーバ操作者に通知すること、および／または将来の危険性を避けるためにサーバをどのように守るかについての助言を提供することを含み得る。

【０１３７】
管理上の応答に加えて（または、管理上の応答の代替案として）、サーバに対する直接の技術応答を追求することが望まれ得る（ブロック６４０）。図８は、サーバに対する技術応答の追求のための例示的な方法８００を図示している。方法８００は、スプーフされたウェブページを解析することを含み得ることにより、ユーザが個人情報を提供し得るフィールドを識別する（ブロック８０５）。当業者は、オンライン形式（例えば、ＨＴＭＬ形式など）が１つ以上のフィールドを備えることと、それらのフィールドが通常は入力されるべき情報を指示するラベルを含むことと、を認識する。それゆえ、一部の実施形態に従って、ウェブページから要求されるフィールドのセットが解析され得る（ブロック８１０）。例えば、各々のフィールドに添付するラベルが解析され得ることにより、フィールドが個人情報を要求するかどうかを決定し、および情報がどのフォーマットが提示されるべきであるかを決定する。この解析は、「ファーストネーム」、「クレジットカード」、「有効期限」などのような一般的な単語の検索、ならびにフィールドによって課される任意の制限（例えば、データタイプ、データの長さなど）の解析を含み得る。「安全な」データのセットが生成され得ることにより、個人情報を要求するフィールド（および／または任意の他の必要なフィールド）を存在させる（ブロック８１５）。一部の実施形態においては、安全なデータは上で議論したように安全なアカウントに対応し得る。任意のイベントにおいては、安全なデータは、有効であると思われる（および、安全なデータが有効なアカウントに対応するという点では、実際に有効であり得る）が、任意の本当のアカウント名義人または他の人物に関係しないデータを備え得る。安全なデータは、安全なデータのデータベースおよび／または辞書（例えば、偽のファーストネームおよびラストネーム、アドレスなど）から引き出され得、および／またはアルゴリズム的に生成され得（例

えば、アカウント番号、クレジットカード番号、有効期限の日付など）、および／または２つのいくつかの組み合わせであり得る。

【０１３８】

要求されるフィールドの解析に基づいて、安全なデータが要求されるフィールドに写像され得ることにより、データがユーザに対する実際の個人情報であると考えられるようにフォーマットされる（ブロック８２０）。単なる例として、フィールドがクレジットカード番号を要求する場合には、明らかに有効なクレジットカード番号（例えば、「４」で始まる１６桁の番号、これは有効なＶｉｓａ^{TM}のクレジットカード番号であると思われる）を表す安全なデータが、そのフィールドに写像され得る。応答メッセージは、スプーフされたウェブページから抜き出された形式に類似するように生成および／またはフォーマットされ得（ブロック８２５）、次いでサーバに提示され得る。この処理は、必要に応じて繰り返され得、複数の「安全な」応答を作成する。

【０１３９】

多くの場合においては、フィッシュメール送信者は、送信者の獲得されたデータの収集上の安全なデータの有害な効果を回避するために、「ｍａｒｋｅｄ　ｍｏｎｅｙ^{TM}」（これは以下でさらに詳細に議論される）の罠を避けるために、および／または他の理由のために、応答にフィルタを掛けることを試行する。フィッシュメール送信者は、受信される応答にフィルタを掛けるために種々のデバイスを使用することを試行し得る。フィルタリングの１つのタイプは、フィッシュ送信容疑者がフィッシング詐欺への本当の応答ではあり得ない特定のＩＰアドレスおよび／またはドメイン（またはアドレス／ドメインのセット）からの応答の検査および／またはフィルタリングを含む。本発明の方法は、対応策（以下で議論されるものを含むがこれらに限定はされない）をインプリメントし得ることにより、このタイプのフィルタ掛けを回避する。

【０１４０】

１つのタイプのフィルタ掛けは、おおまかに「データ認証」と呼ばれ、それは、一貫性のための提示された応答をチェックするための様々な手法の使用を含む。単なる例として、フィッシュメール送信者のウェブサイトが、規格（これは工業規格、公開された規格などであり得る）に従ってフォーマットされるデータを収集する場合には、フィッシュメール送信者が制御（これはフィッシュメール送信者のウェブサイト上、フィッシュ電子メール内などに存在するソフトウェアアプリケーションおよび／またはポータブルソフトウェアであり得る）をインプリメントし得ることにより、このような規格を有する一貫性のための提示された応答をチェックする。それゆえ、安全な応答のフィルタ掛けを回避するために、方法８００は、適用可能であり得る任意のこのような規格を識別すること、および／または評価することのような対応策をインプリメントし得る（ブロック８３０）。例えば、方法８００が応答フィールドの各々を評価することを含み得ることにより、任意の規格をそのフィールドに適用するかを決定し、適用する場合には規格がどのようにインプリメントされ得るかを決定する。単なる例として、上で議論したように、クレジットカードネットワークは、一貫性および／またはクレジットカード番号の有効性を確実にするための規格を発展させている。結果として、フィールドがクレジットカード番号を求める場合には、方法８００は適切な応答のための適当な規格を識別することを含み得る。同様の規格が、銀行のルーティング（「ＲＴＮ」）番号などに存在する。別の、可能性としては単純な例として、ウェブサイトが電子メールアドレスの提示を要求する場合には、方法８００は有効な電子メールアドレス（例えば、ｕｓｅｒ＠ｄｏｍａｉｎ．ｔｌｄ）の要求を識別することを含み得る。（電子メールアドレスの有効化を含む他の手順は、以下で議論される）。一部の場合には、それゆえ、システムは共通のフィールドタイプを識別するための、および／またはそれらのフィールドタイプをそれらのフィールドタイプに応答して提示されるデータの適切な規格と相関させるための論理構造および／またはデータ構造を備え得る。

【０１４１】

フィッシュメール送信者はまた、時折、応答を有効にするために１つ以上の統合された

テストを使用し、方法８００は、それゆえ、このような統合されたテストを打ち負かすための対応策を備え得る。このような対応策は、このような統合されたテストを識別することおよび／または解析することを含むが、これらに限定はされない（ブロック８３５）。単なる例として、ウェブサーバおよび／または電子メールメッセージは、ポータブルコード（例えば、Ｊａｖａ（登録商標）アプレット、Ｊａｖａ（登録商標）スクリプト、ＣＧＩアプリケーションなど）、および／またはフィッシュメールを送ることおよび／または繰り返し送ることの結果として生成されない応答を追跡、識別および／または無視するように設計された他のデバイスを含み得る。このようなデバイスは、再び単なる例として、カウンタ、タイマ、クッキー、ハッシュ値およびそれらと同様のものを含み得る。このようなデバイスを識別することおよび／または解析することは、このようなコードの存在のための電子メールメッセージおよび／またはウェブサイトをスキャンすること／解析すること、サンドボックスにおいてこのようなコードをダウンロードすることおよび／またはコードを実行することにより、コードがどのように働くかを決定すること、および／またはコードを分解して模倣すること（ｒｅｖｅｒｓｅ－ｅｎｇｉｎｅｅｒｉｎｇ）により、応答がどのように有効化されるかを決定すること、を含み得る。単純な例として、ウェブサイトが特定のコンピュータを識別するクッキーをセットし得ることにより、特定のコンピュータからの複数の応答がフィッシュメール送信者によって識別および／またはフィルタされ得る。このデバイスを識別および／または解析することは、クッキーのコンテンツを検査することを含み得、ゆえに変更されたクッキー（例えば、これは識別情報を変化および／または除去し得る）は、各々の応答と共に送信され得る。他の場合には、デバイスは、特定のコンピュータからウェブサイトへの各々のアクセスを増加させるカウンタを含み得、そのタイマが識別され得ることにより、適切な対応策がとられ得る。さらに他の場合においては、タイマは、複数の応答が、あるタイムフレーム内で送信されることを防ぐようにインプリメントされ得、および／またはハッシュアルゴリズムは、例えば、応答を識別するために、応答などに適用され得る。

【０１４２】

他の場合には、フィッシュメール送信者は、応答をトリガするように設計されるフィッシュ電子メールについての情報、および／またはフィッシュ電子メールに含まれる情報に基づいて、応答を有効にすることを試行し得、しばしば応答する電子メールを用いて、応答が一部の様式に適合することを要求する。このような戦略は、「ラウンドトリップ（ｒｏｕｎｄ－ｔｒｉｐ）」情報を含むと言われ得る。すなわち、電子メールアドレスにおいて特定のデータがフィッシュメール送信者によって送信され、対応するデータがウェブサーバの「ラウンドトリップ」中に戻されることが予期される。例えば、このような応答は偽であり、および／または安全なデータを備えるという仮定の下で、フィッシュメール送信者によって送信される任意の電子メールに相関するとは思えない応答にフィルタを掛けるために、これらの手法は使用され得る。従って、方法８００は、フィッシュメール送信者による、応答にフィルタを掛けるためのユーザのこのようなラウンドトリップの情報に対する試行を打ち負かすための対応策を備え得る。このような対応策は、例えば、任意のこのような「ラウンドトリップの」情報を識別することおよび／または解析することを含み得る（ブロック８４０）。ラウンドトリップの情報は、種々の手順を介して識別されおよび／または解析され得る。

【０１４３】

単なる例として、フィッシュメール送信者は特定のフィッシュメッセージが送信されたアドレスのリストを維持し得、フィッシュメール送信者はまた、応答が、電子メールアドレスを含むことを要求し得る。フィッシュメール送信者が、次いで電子メールアドレスによって応答にフィルタを掛け得ることにより、フィッシュメール送信者によって維持されるリスト上に含まれない電子メールアドレスが列挙される任意の応答が偽であると考慮される。あるいは、フィッシュメール送信者は、フィッシュメッセージの各々に応答コードを含ませ得、応答コードを提供する応答を要求し、次いで応答コードを含まない全ての応答をフィルタリングする。（特定の場合には、応答コードは、例えば、フィッシュメッセ

ージにおけるポータブルコードを用いることによって、フィッシュメッセージが伝送されたアドレスへのフィッシュの伝送日、および／または任意の他の変数と調和され得、および／またはラウンドトリップの情報を解析することは、このようなポータブルコードを上で議論したものと類似する様式で解析することを包含する）。

【０１４４】

このようなラウンドトリップの情報を識別および／または解析することは、フィッシュメッセージおよび／または応答ウェブページを解析することを含み得る。多くの場合には、フィッシュメッセージと応答ウェブページとの比較は、ラウンドトリップの情報の使用を明らかにする。さらに、フィッシュメッセージの収集は（フィッシュメッセージの各々は、可能性としては、上記されるようにハニーポットによって、および／または他の方法によって収集される）、ラウンドトリップの情報の識別および／または解析を可能にする類似性および／またはパターンを明らかにし得る。単なる例として、共通の電子メール「ブラスト（ｂｌａｓｔ）」から発生すると考えられる複数のフィッシュ電子メール上の受信者のアドレスが比較され得ることにより、（受信者のアドレスおよび／またはドメインにおける、応答コードにおける、含まれるポータブルコードにおける、などの）共通性および／または差異を見出す。この比較はフィッシュメール送信者によってフィルタされない応答の策定を助け得る。

【０１４５】

特定の場合には、フィッシュメール送信者は、応答にフィルタをかけるために、試行において、上記の手法の１つ以上を用い得る。さらに、フィッシュメール送信者がしばしば、危険にさらされているサーバ（上で議論したように）上のフィッシュメール送信者のウェブサイトを操作するので、フィッシュメール送信者はしばしば、危険にさらされているサーバ（これは例えば、サーバの操作者に危険性を警告し得る）上に有意な負荷を課すことを回避するために、フィルタリング手順を可能な限り「軽く」させるような動機を有する。それゆえ、フィッシュメール送信者がしばしば、それらのフィルタリング手法を一般化することを試行することにより、さらに効果的な検索を可能にする。単なる例として、伝送されたフィッシュ電子メールに対応する特定の電子メールアドレスのフィルタリングの代わりに、フィッシュメール送信者は、「ａｏｌ．ｃｏｍ」のような１つのドメインにおけるアドレス（または複数の選択されたドメイン）に、特定のスパムを制限し得、対応するウェブサイトに提示される応答の一部として電子メールアドレスを要求し得る。電子メールブラストがアドレスされるドメインと異なるドメインを有する電子メールアドレスを列挙する任意の応答は、次いでフィルタされ得る。この手順は、実際に個別の電子メールアドレスを比較することに比べて、（リソースを算出する立場から）かなり効果的であることを証明し得る。ラウンドトリップの情報（および／または任意の他のデバイス）を識別する手順は、このような「ショートカット」を指示するパターンを明らかにし得、および／またはこれらのショートカットは、応答の形成において利用され得る。単なる例として、フィッシュ電子メールの収集の解析が、特定のブラストが特定のドメインにおけるユーザに向けられたことを指示する場合には、そのドメインにおいて電子メールアドレスを提供する（および／またはそのドメインのホストから発生していると考えられる）ことを用いる任意の応答は、フィッシュメール送信者のフィルタリング手順によって受容される場合であり得る。

【０１４６】

それゆえ、方法８００は、フィッシュメール送信者のウェブサーバに伝送される応答がブロック８３０～８４０において識別および／または解析される判定基準（および／または他の識別された有効判定基準）と合うことを確実にすることを含み得る（ブロック８４５）。本明細書の開示に基づいて、当業者は、応答が所与の判定基準に合うことは、しばしば、識別される判定基準の本質上で、大いにあることを認識する。単なる例として、判定基準が、特定の戻り値が工業規格（例えば、クレジットカード番号）に一致しなければならないことである場合には、方法８００は、全ての応答が有効にフォーマットされたクレジットカード番号に含まれたことを確実にすることを含む可能性がある。別の例として

、ラウンドトリップの情報の解析が、フィッシュ電子メールブラストがあるドメインおよび／またはＩＳＰにおいてユーザにメッセージを伝送することだけが考えられることを指示する場合には、方法８００は、提示される全ての応答がそのドメインに関連するアドレスを含むことを確実にし得る。さらに別の例として、統合されたテストが識別される場合には（例えば、上で議論したように、ポータブルコードを分解して模倣することによって）、方法８００は、各々の応答が、そのポータブルコードによって（例えば、コードに従う応答を作成することによって、および／または結果をテストするためにウェブサーバに伝送する前に応答上のコードを実行することによって）評価される場合には有効であると考慮されることを確実にし得る。

【０１４７】

それゆえ、方法８００は、フィッシュメール送信者によってインプリメントされた任意のフィルタリング手法（および、特に任意のコンテンツベースのフィルタリング手法）を巧みに回避するように設計された対応策を含み得る。ブロック８３０～８４５に関して議論される手順が、応答がフォーマットされた後に発生するとして図示されていることに注意され得る（ブロック８２５）。しかしながら、一部の実施形態においては、方法８００の他の点（例えば、安全なデータの生成（ブロック８１５）前、および／または応答のフォーマット（ブロック８２５）前に）において行われることが比較的により効果的であり得る。

【０１４８】

安全な応答（および／または他の適切な応答および／または要求、これらは例えば、ジェネリックＨＴＴＰ要求、他のタイプのＩＰ通信／パケットなどを含み得る）は、応答戦略によって決定された数および頻度でサーバに提示され得る。例えば、「混乱させるための応答（ｒｅｓｐｏｎｄ　ｔｏ　ｃｏｎｆｕｓｅ）」戦略が使用され得、この戦略により相対的にわずかな安全な応答がサーバに提示され得る（ブロック８５０）。この戦略は、無効なデータをサーバのデータベースに導入するという効果を有し、その効果によって、収集されたデータのどちらが利用され得る有効な個人情報を実際に表すかについての、および収集されたデータのどちらが単なる不要情報であるかについての不確定性をフィッシュメール送信者に生じさせる。これだけでフィッシング詐欺の利益に有意に影響し得、これだけで実際の消費者から受信される有効な個人情報をフィッシュメール送信者が利用することを十分に防ぎ得る。加えて、安全なデータが安全なアカウントに関連し、かつフィッシュメール送信者が安全なデータを利用することを試行する場合には、フィッシュメール送信者のそのデータの使用はトレースされ得、フィッシュメール送信者の活動の証拠となる痕跡はコンパイルされ得、フィッシュメール送信者の識別を援助し、可能性としては民事訴訟または刑事告発の証拠を提供する。

【０１４９】

所望される場合には「邪魔をするための応答（ｒｅｓｐｏｎｄ　ｔｏ　ｉｍｐｅｄｅ）」戦略が遂行され得る（ブロック８５５）。この戦略においては、安全な応答は、大量の数で、および／または非常に速い速度で伝送され得る。安全な応答はまた、複数の応答コンピュータから送信され得、複数の応答コンピュータは、異なるドメインおよび／またはＩＰブロックに存在し得、フィッシュメール送信者による簡単な検出を防ぎ、その応答は安全な情報を備えている（および、結果としてフィッシュメール送信者には無用である）。「混乱させるための応答」戦略（実際にはこの戦略下で拡大される）の利点に加えて、「邪魔をするための応答」戦略は、フィッシュメール送信者に、フィッシュメール送信者の詐欺が発見されているという信号を送り得、可能性としては詐欺を継続することに対して妨害物（ｄｅｔｅｒｒｅｎｔ）を提供する。

【０１５０】

さらに積極的な応答が所望される場合には、「防ぐための応答（ｒｅｓｐｏｎｄ　ｔｏ　ｐｒｅｖｅｎｔ）」戦略が着手され得る（ブロック８６０）。防ぐための応答戦略は、多数の可能性としては広く分布する応答コンピュータから大量の安全応答を高いレートで伝送することを含み得る。実際には、応答のレートは実際の消費者または他からの任意の

相当な量の真の応答を受信することを可能にすることを効果的に防ぐために十分高くあり得、詐欺を効果的に終結させる。この戦略は、サーバが応答を受容することを停止するまで遂行され得、実際はサーバが再び応答を受容し始める場合には継続され得る。

【０１５１】

最後に、一部の場合には、「含むための応答（ｒｅｓｐｏｎｄ　ｔｏ　ｃｏｎｔａｉｎ）」戦略が使用され得る（ブロック８６５）。この戦略は、スプーフ詐欺を操作するウェブサービスに十分なＨＴＴＰ要求を提示することを含むことにより、要求を提供するためのサーバの能力を効果的に無力にする。当業者は、典型的なウェブサーバがしばしば接続テーブルをインプリメントし、接続テーブルが、サーバが任意の所与の時間においてサービスを提供し得るＨＴＴＰ接続の数を追跡および制限することを認識する。それゆえ、本発明の実施形態に従って、十分な同時発生のＨＴＴＰ要求が（可能性としては、上記したようなコンピュータの分散システムによって）提示され得ることにより、ウェブサーバの接続を「満たし」、それによりサーバが任意のさらなる要求を受容することを防ぐ。この処理は、詐欺的なウェブサイトが除去されるまで無限に継続され得る。ＨＴＴＰ要求は、安全な応答を備え得（上記したように）るが、この場合には必要ではない。任意のジェネリックＨＴＴＰ要求（例えば、ＨＴＴＰ　ＧＥＴ要求）は通常は、結合を作成するために十分であり、それにより接続テーブルを入力で占める。

【０１５２】

この手法が、システム／ネットワーク（ここからオンラインの詐欺が行われる）上の一般化されるアタック（例えば、ＩＰパケットの圧倒的な数の伝送）とは、接続テーブルを満たすために要求されるＨＴＴＰ要求の数が通常は、ネットワークのインフラストラクチャに有意な衝撃を有するほど高くはないという点で異なるということは何の価値もない。さらに、ウェブサーバを実行するシステムは、通常は、他の場合には利用可能なまま維持される－単に、システムは、ウェブサーバはＨＴＴＰ要求を提供することに及ばない。この方法においては、詐欺的活動は、ネットワークインフラなどに超過的な付帯的損害を引き起こすことなく損なわれ得、または防がれ得る。当然、（任意の種類の）一般化されたアタックはまた、この目的を達成するために使用され得るが、このようなアタックは一部の場合（例えば、倫理的なおよび／または政治的な考慮によって）には実行不可能であり得る。

【０１５３】

所望される場合には、応答の情報の使用が、追跡され得る（ブロック８７０）。上記したように、安全な応答は、任意の真のユーザに関連しない情報（例えば、明らかに有効なクレジットカード番号）を備え得る。詐欺の実行者がこのような情報を使用することを試行する場合には、その情報の使用がトレースされ得ることにより、実行者を識別する。単なる例として、顧客が銀行またはクレジットカードの発行者である場合には、「安全な」アカウント番号に関連するアカウントは開かれ得（または「安全な」アカウント番号は、そうでない場合にはモニタされ得）、そのアカウントにアクセスする任意の試行（例えば、試行される払い戻しまたはクレジットカード認証）は、さらなる調査のためにフラグが立てられ得る。この「ｍａｒｋｅｄ　ｍｏｎｅｙ」の使用は、他のコンテキストにおいて権限者により使用され（例えば、銀行強盗にマークされた現金を提供すること）、次いでｍａｒｋｅｄ　ｍｏｎｅｙの痕跡を追いかけることにより銀行強盗をトレースする。同様の概念が本発明の実施形態に従って、本明細書で記載される技術を用いてインプリメントされ得る。

【０１５４】

洗練されたフィッシュメール送信者はまた、応答の源に従って応答をフィルタすることを試行し得る。単なる例として、フィッシュメール送信者が、１つのＩＰアドレス（および／または類似のＩＰアドレスの範囲）、１つのドメインなどから、複数の応答を検出する場合には、そのフィッシュメール送信者は、１つの位置からの複数の応答が、誰かがフィッシュメール送信者の詐欺を発見していること、およびフィッシュメール送信者を識別しようと試行していること、安全な応答を提示することを試行していることなどを指示す

るという理論において、ＩＰアドレス／範囲／ドメインからの応答をフィルタし得る。それゆえに、方法８００は、フィッシュメール送信者によるこのような試行を打ち負かすように設計される１つ以上の手順を含み得る。単なる例として、上記した１つの戦略は、分散された様式で応答を伝送するために、複数のコンピュータおよび／または複数のＩＰアドレスの使用を含む。一部の場合には、色々なＩＰアドレス（これらは異なるアドレスブロックなどからであり得る）を提供することにより、本発明の方法に従って生成された応答を識別するためのフィッシュメール送信者の能力を邪魔することが有利であり得る。

【０１５５】

複数の種々のＩＰアドレスからの伝送のための１つの戦略は、例えば、複数のプロバイダから相対的に「使い捨ての」または一時的なＩＰアドレスを購入することによって（そうでなければ取得することによって）（例えば、複数の異なるＩＳＰにアカウントを開くことによって）、複数の種々のＩＰアドレスを獲得することを含み得る（ブロック８７５）。一部の場合には、リテールＩＳＰ（例えば、ＭＳＮ、ＡＯＬなど）に関連する（に割り当てられる）ＩＰアドレスを取得することが有利であり得る。なぜならば、このようなアドレスからの応答が、しばしばフィッシュメール送信者の主な目標である消費者から発生すると推定され得るからである。（リテールＩＳＰは、消費者に対するインターネット接続性を提供する任意のＩＳＰと、それらとは対照的に、ビジネスに対してのみ、接続性および／または他のサービスを提供する任意のＩＳＰと考慮され得る）。一部の場合には、配置は、単にアドレスを一時的に使用するためにこのようなＩＳＰと共になされ得る。方法８００は、次いで、例えば、本発明の方法に従って応答を生成するように、および／またはこのような応答をフィッシュメール送信者のウェブサーバに伝送するように（ブロック８８０）、構成されたコンピュータに複数のＩＰアドレスの各々を割り当てることをさらに含み得る。一部の実施形態においては、これらのコンピュータの各々が、ＩＰアドレスを使用するために適切なＩＳＰ（例えば、割り当てられたＩＰアドレスが関連するＩＳＰ）にログオンされ得ることにより、コンピュータによって伝送された任意の応答がＩＳＰを経由して伝送される。さらに、特定の実施形態においては、これらのコンピュータは、１つ以上の中央コンピュータによって制御され得る。他の実施形態においては、応答は１つ以上の中央コンピュータにおいて生成され得、次いで複数のＩＰアドレスを割り当てられたコンピュータに送信され得、次いで、応答を（可能性としてはある変更とともに）転送することにより、応答がこれらのコンピュータ／ＩＰアドレスから発生していると考えられる。

【０１５６】

本発明の実施形態に従って使用され得る別の戦略は、１つのコンピュータ（またはコンピュータのセット）からの応答を提供するためのメガプロキシ（ｍｅｇａｐｒｏｘｙ）（または類似の技術）の使用（ブロック８８５）であるが、ここで応答の各々は、異なるＩＰアドレス、ドメインおよび／またはネットワークブロックから発生すると考えられる。このような手順の例は、米国仮特許番号第６０／６１０，７１６号に記載され、既に参考として本明細書に援用されている。これらの手順および類似の手順を使用して、要求のグループが種々の供給源から発生していると考えられるようになされ得、応答にフィルタを掛けることのフィッシュメール送信者の試行を挫折させ、かつ／または本発明の方法に従って生成される安全な応答をブロックすることを試行することにおいて、実際の消費者の応答をフィッシュメール送信者にブロックさせる。

【０１５７】

単なる例として、図９Ａはフィッシング詐欺に応答を提示するために使用され得るシステム９００を図示している。システム９００は、１つ以上の実体９０５に割り当てられる１つ以上のネットワークブロック（例えば、ＩＰアドレスのブロック）を用いることにより働き、実体９０５は一部の場合には、主要な消費者ＩＳＰ（例えば、Ｃｏｍｃａｓｔ、Ａｍｅｒｉｃａ Ｏｎｌｉｎｅ（「ＡＯＬ」）、Ｍｉｃｒｏｓｏｆｔ Ｎｅｔｗｏｒｋ（「ＭＳＮ」）など）を含み得る。ネットワークブロックは、反フィッシングソリューションに使用するためのこれらの実体によって「寄付され」得る。（用語「寄付される」は記

載の簡単のために、本明細書で使用されるが、ネットワークブロックに対する所有権はセキュリティプロバイダに必ず移されること、またはブロックが報償なしで提供されることを推量すべきではない。例えば、一部の実施形態においては、セキュリティプロバイダは本発明の実施形態に従う使用のためのブロックを購入し得または借り得、そうでなければブロックはこのような使用のためにセキュリティプロバイダに一時的に貸し付けられ得る。他の実施形態においては、ＩＳＰは、ブロックが使用されるべきであるという目的に気付くことさえ必要ではない。当業者は、ビジネスの使用のためにＩＳＰから会社までの専用のネットワークブロックの割り当てが珍しくないことを認識する）。

【０１５８】

寄付されたブロックは、セキュリティプロバイダなどに相対的に永久的に割り当てられ得、かつ／またはアドホックベースで割り当てられ得る。このようなブロックは、内部ルーティングプロトコルを経由してこれらの実体９０５によって提供され得、かつ／または寄付されたブロックの記録は、反詐欺システム９００による使用のために、データベース９１０に記憶され得る。反詐欺システム９００はまた、ネットワークのミートミー（ｍｅｅｔ－ｍｅ）センタ９１５を含み得、ミートミーセンタ９１５は、ネットワークブロックとインターネットの他の部分（特に、オンライン詐欺の実行者）との間の不明瞭な接続を提供する任意の設備であり得る。ミートミーセンタ９１５は、複数の応答／要求９３０（例えば、ＨＴＴＰ　ＰＯＳＴまたはＨＴＴＰ　ＧＥＴ指令）を提示する能力を詐欺師のサーバ２５０に提供し得る。例によって、応答９３０は上で議論される応答に類似し得る。

【０１５９】

ミートミーセンタ９１５は、ダイリューションエンジン９２０を備え得、ダイリューションエンジン９２０は、上記したダイリューションエンジンと同様の様式で機能し得る。（あるいは、ミートミーセンタ９１５はセキュリティプロバイダによって維持されるダイリューションエンジンと、可能性としてはシステム（例えば、図１Ａのシステム１００および／または図２のシステム２００）の一部として通信し得る）。単なる例として、ダイリューションエンジン９２０は、応答／要求９３０、ならびにメガプロキシ９２５を作成および／またはフォーマットするように設計される（可能性としては上で議論される様式で）ソフトウェアアプリケーションであり得、これはデータベース９１０に記憶されるネットワークブロック内に含まれる任意のＩＰアドレスから発生していると考えられる応答／要求９３０を作成し得る。それゆえ、操作において、ダイリューションエンジン９２０は、多くの応答／要求９３０を備え得る。上記されるように、これらの要求／応答９３０がフィッシング詐欺への正当な応答であると考えられるようにフォーマットされ得、かつ／または単に、他の要求を提供するためのサーバの能力を占めるように設計されるジェネリックな要求であり得る。メガプロキシ９２５はそれらの応答／要求９３０を、任意の適切なアドレス（例えば、上記したようにデータベース９１０に記憶されるブロック内のＩＰアドレス）を発生元のアドレスとして用いて、スプーフを行う人のウェブサイト９４０に転送する。上記したように、応答／要求９３０は不正確な個人情報をウェブサイト９４０にフィードするように、および／または単にウェブサイトを占めることにより他者をだますための能力を邪魔するように設計され得る。詐欺師は、応答／要求９３０をブロックすることを試行するためにフィルタ９３５（例えば、特定のＩＰアドレス、ドメインなどからの通信をブロックするように設計されるファイアウォールアプリケーション）を使用し得るが、これは詐欺師にとって、以下の理由の１つ以上のために問題であると判明する。

【０１６０】

まず、応答／要求９３０は、種々の異なるＩＰアドレスから（および、多くの場合には、種々の異なるドメインおよび／またはＩＳＰ）発生していると考えられるので、詐欺師にとって、受信する応答／要求のどちらがシステム９００からであるか、およびどちらが普通の消費者からであるかを決定することは困難である。一部の場合には、どちらの応答／要求がシステム９００からであるかを決定することは技術的に可能であり得るが、このような決定を行うことは、通常は、相対的に高価な設備および有意な処理電力を含み、当

業者は、オンライン詐欺スキームがしばしばこのような設備に投資する金融資源を持たない人々によって操作されることを認識する。さらに、多くのオンライン詐欺のサイトが、詐欺師ではなく無実の第三者によって操作される危険にさらされたサーバ上で操作されるので、スプーフされたメール送信者にとって、深い解析を行うために要求される算出リソースを、少なくともサーバの所有者に危険性を警告することなしに結集することは困難である。

【０１６１】

さらに、詐欺師がシステム９００から要求／応答９３０を識別することに成功し、これらの要求／応答９３０の一部を何とかブロックする場合でさえ、これらの要求／応答９３０はしばしば主要な消費者ＩＳＰ（例えば、９０５）から発生していると考えられることは事実で、詐欺師は、詐欺師の主要なターゲット（普通の消費者）に関連するＩＰアドレスをブロックしなければならない困難な位置にいる。このようにして、システム９００は、詐欺師にとって要求／応答９３０をブロックすることを困難にするおよび／または高価にするだけでなく、詐欺師に対する要求／応答９３０をブロックする詐欺師の試行を、詐欺師に、普通のユーザに割り当てられるアドレスをも含むネットワークブロックをブロックさせることによって使用すること、という複数の利点を提供し得、これにより詐欺師が引き込みたいと願う多くの人々からの応答をブロックする。

【０１６２】

図９Ｂの９５０は、ウェブサーバに対する応答を提示する方法を図示している。本発明の方法は任意の特定のハードウェアまたはソフトウェアインプリメンテーションに制限はされないが、方法はシステム（例えば、図９Ａのシステム９００）を用いてインプリメントされ得る。方法９５０は、１つ以上のＩＰブロックを獲得することを含み得る（ブロック９５５）（すなわち、利用可能なＩＰアドレスのブロック）。上記したように、一部の場合において、ＩＰブロックにとって、方法９００によって生成される応答がこのようなＩＳＰから発生していると考えられるように複数のＩＳＰ（リテールＩＳＰを含む）から（特定の場合においては、消費者のようなリテールＩＳＰの顧客から）獲得されることは有用であり得る。ＩＰブロックを獲得するための様々な戦略は上で議論され、任意のこれらの戦略は本発明の実施形態に従って使用され得る。一部の実施形態に従って、獲得されたＩＰアドレスおよび／またはブロックの記録は（例えば、データベース内に）記憶され得る（ブロック９６０）。

【０１６３】

方法９５０は、メガプロキシ（例えば、図９Ａに関連して記載されるメガプロキシ９２５に類似のメガプロキシ）および／または種々の異なる供給源から発生していると考えられるＩＰパケット（および、特定の場合にはＨＴＴＰ要求）を伝送することが可能な任意の他のデバイスまたはソフトウェアアプリケーションをさらに含み得る（ブロック９６５）。メガプロキシを提供することは、メガプロキシをネットワークミートミーセンタに位置することを包含し得、これは例えば、複数のＩＳＰにおいて内部ルーティングプロトコルを用いて通信するための能力を提供するピアリング（ｐｅｅｒｉｎｇ）設備であり得る。他の実施形態においては、メガプロキシは、メガプロキシが獲得されたＩＰアドレスを用いてパケットを伝送可能である限りは、他の場所に位置され得る。

【０１６４】

例えば、上で議論された方法を用いて、一旦不正なウェブサイトが識別されると（ブロック９７０）、例えば、上で議論された方法を用いて、応答（例えば、ＨＴＴＰ要求）が作成され得る（ブロック９７５）。メガプロキシは次いで、ＩＰアドレスを取得し得（例えば、獲得されたＩＰアドレスのデータベースを検索することによって）（ブロック９８０）、応答を不正なウェブサーバに伝送することにより、応答がメガプロキシによって取得されたＩＰアドレスから発生する（ブロック９８５）。この処理は、複数の応答の間繰り返され得る（図９Ｂに破線によって指示されるように）。一部の場合には、新しいＩＰアドレスが伝送されるべき各応答に対して取得され得る。他の場合においては特定のＩＰアドレスが複数の応答を伝送するために使用され得る。このようにして、複数の応答（こ

れらは一部の場合には上で議論されたように「安全な」データを備え得る）は、不正なウェブサーバに伝送され得る。

【０１６５】

図８に戻って、不正なウェブサイトに応答するための別の戦略が「プロキシチェーニング（ｐｒｏｘｙ　ｃｈａｉｎｉｎｇ）」をインプリメントし得る（ブロック８８５）。プロキシチェーニングは、フィッシュメール送信者のウェブサーバに対する最後のパケット伝送の前に、種々のプロキシサーバを通る応答パケットの伝送を含む。プロキシチェーニングの一実施形態においては、詐欺防止システム（例えば、上記されるシステム１００）は、複数の専用の接続、モデム接続などを経由する、種々の異なるＩＳＰ（および特にリテールＩＳＰ）への接続を含み得る。応答はこのような接続を介して送信され得、このような接続によってこれらのＩＳＰのプロキシサーバを、詐欺防止システムに代わって実際に要求を提示するために利用する。フィッシュメール送信者が応答を受信する場合には、応答はそれらのリテールＩＳＰから発生していると考えられ、フィッシュメール送信者が、応答が発生する実際のマシンを決定することを（および、結果としてブロックを簡単に可能にすることを）防ぐ。別の実施形態においては、要求は複数のプロキシサーバを介して、可能性としては連続的な様式で送信され得、フィッシュメール送信者にとって応答の発生源を決定することをさらに困難にする。

【０１６６】

図１０は、プロキシチェーニング戦略を用いて応答を提示するために使用され得るシステム１０００を図示している。システム１０００は、詐欺防止システム１００５を備え、詐欺防止システム１００５は、図１Ａ、図２および／または図１１によって図示されるシステムに類似し得（および／またはこれらのシステムに関連して記載されるものに類似する構成要素を含み得る）、かつ／または本発明の様々な方法を行い得る。特に、詐欺防止システム１００５は、不正なウェブサーバ２５０に対する技術応答（例えば、ダイリューション応答）を実行するように構成され得る。詐欺防止システム１００５は、１つ以上のプロキシ１０１０を含み得、１つ以上のプロキシ１０１０は当業者が認識するように、詐欺防止システム１００５からの応答を転送するために使用され得る。プロキシ１０１０は、ＳＯＣＫＳプロキシ、ＨＴＴＰプロキシ、ＣＧＩプロキシ、および／または任意の他のタイプの当該分野で公知のインターネットプロキシであり得る。

【０１６７】

当業者が認識するように、不正なウェブサイト２５０への伝送に対する応答を作成および／またはフォーマットするコンピュータ（例えば、ダイリューションエンジンおよび／または応答コンピュータ）を識別するために使用され得るヘッダ情報を偽装するために、プロキシは使用され得る。一部の実施形態においては、プロキシ１０１０は、ウェブサイト２５０に応答を直接伝送するために使用され得る。しかしながら、このような実施形態においては、プロキシ１０１０は、詐欺師によって、詐欺防止システム１００５の一部として識別され得る。（なぜならば、プロキシ１０１０は、例えば、サーバ２５０にダイリューション応答を伝送するからである）。このような識別を防ぐために、応答は、（プロキシ１０１０を介してまたは直接のいずれかで）詐欺検出システム１００５によってサーバ２５０に対する伝送のために他のプロキシに伝送され得る。

【０１６８】

単なる例として、詐欺防止システム１００５－および／または詐欺防止システム１００５をホストするＩＳＰ（示されていない）－は、１つ以上のデータセンタ１０１５（これら自体はＩＳＰであり得、および／またはＩＳＰによってホストされ得る）とピアリング関係（当該分野で公知）を有し得る。応答は、これらのデータセンタ１０１５に、直接のピアリング接続を介して、またはインターネット２０５を経由してのいずれかで、伝送され得、データセンタ１００５はこれらの応答をサーバ２５０に、しばしばそれらが所有するプロキシ１０２０を介して伝送し得る。

【０１６９】

本明細書で議論される全てのプロキシ同様に、プロキシ１０２０は、匿名プロキシであ

り得る。さらに、特定の実施形態においては、本明細書で議論されるプロキシは「歪んでいる」プロキシであり得、これは誤ったデータまたは擬似ランダムなデータを、「ＨＴＴＰ＿ＶＩＡ」および「ＨＴＴＰ＿Ｘ＿ＦＯＲＷＡＤＲＤＥＤ＿ＦＯＲ」のようなＨＴＴＰ要求（これはダイリューション応答を備え得る）における特定のフィールドに省略し得、かつ／または書き換え得、これによってこれらがプロキシとして提供されること、および／またはＨＴＴＰ要求の実際の供給源として詐欺防止システム１００５（および／またはそのシステムの構成要素）を分かりにくくするという事実を偽装する。データセンタプロキシ１０２０（および本明細書で議論される他のプロキシ）は、結果として詐欺防止システムに相対する応答を「匿名化する」ために提供し得、さらに詐欺防止システム１００５をサーバ２５０（またはサーバ２５０上の詐欺の操作者）による検出から隔離する。

【０１７０】

本発明の一実施形態に従って、詐欺防止システム１００５は、構内交換設備（ＰＢＸ）システム１０２５（および／または詐欺防止システム１００５と通信する利用可能な１本以上の電話（ＰＯＴＳ、ＩＳＤＮ、またはその他）線を提供する任意の他の手段）を組み込み得る。ＰＢＸ１０２５は、モデムプール１０３０（または類似のデバイス）と通信し得、結果として、図１０上に破線によって示される、１つ以上のＩＳＰ１０３５との通信を提供するために使用され得る。（他の実施形態においては、ＩＳＰ１０３５との通信を提供するための他の手段が同様に使用され得る）。それゆえ、応答は１つ以上のＩＳＰ１０３５を介して発送され得（および、一部の実施形態においては、ＩＳＰ１０３５によって操作される１つ以上のプロキシ１０４０へ伝送され得）、ＩＳＰ１０３５は応答をサーバ２５０に転送する。一部の場合においては、ＩＳＰ１０３５の１つ以上はリテールＩＳＰであり得、上で議論されるようにＩＳＰの消費者顧客から発生すると考えられる応答を作成する追加の利点を提供する。

【０１７１】

特定の実施形態においては、詐欺防止システム１００５は、プロキシチェーニング手法を用いて、複数のプロキシ（図１０に描かれる任意のプロキシ１０１０、１０２０、１０４０を含む）を介して応答を発送するように構成され得る。単なる例として、ＨＴＴＰ要求のような応答は、詐欺防止システム１００５からデータセンタ１０１５ａまで（可能性としてはプロキシ１０１０ａを経由して）伝送され得、ここで要求はデータセンタのプロキシサーバ１０２０ａによって、別のデータセンタ１０２０ｂ（または、代替的に、ＩＳＰ１０３５ａ）に転送され得、ここで別のプロキシサーバ１０２０ｂは要求をウェブサーバ２５０に転送する（プロキシチェーンにおけるリンク間の転送はピアリング接続、モデム接続、インターネットなどを経由してなされ得る）。この手法は、一部の状況下で、応答のより包括的な「匿名化」を提供し得、ウェブサーバ２５０（および／またはウェブサーバ２５０を使用する詐欺師）に対して、応答の供給源を識別することを比較的により困難にする。さらに、一部の実施形態においては、詐欺防止システム１００５のプロキシサーバ１０１０（および／または、ダイリューションエンジン、応答コンピュータなどのようなシステム１００５の他の構成要素、これらは図１０には示されていない）が、複数の応答を様々なプロキシ（例えば、１０２０、１０４０）に、ランダムに、順番に、分配するように構成され得ることにより、応答の供給源をさらに偽装する。

【０１７２】

それゆえ、本発明の様々な実施形態がいくつかの異なる手順を提供することにより、フィルタリングまたはブロッキング手法を巧みに回避する（応答のコンテンツまたはこれらの応答の発信元に基づくかどうか）。これらの手順は、個別にまたは任意の組み合わせで使用され得、フィッシュメール送信者に、本発明の方法により生成された応答から、実際の騙された消費者により提示される応答を分離することを困難にさせる。このようにして、本明細書で議論される応答および／または「ｍａｒｋｅｄ　ｍｏｎｅｙ」手法、ならびに他の反詐欺処理は、より効果的にインプリメントされ得る。

【０１７３】

本発明の実施形態の別のセットにおいて、モニタリングアプライアンスは、顧客のシス

テムによって受信されるメッセージを介してフィッシング詐欺（または、顧客のオンラインアイデンティティの他の不正な使用）の通知を提供するために使用され得る。図１１は、このようなイベントを識別するために使用され得るシステム１１００を図示しており、図１２は、このようなイベントを識別するための例示的な方法を図示している。

【０１７４】

単なる例として、図１１のシステム１１００は、特にフィッシングイベントを、一部の場合にはフィッシング詐欺の比較的早い段階（すなわち、フィッシュメッセージが元来フィッシング詐欺における犠牲者および／または参加者になる見込みがある人物に伝送されるとき）において、取り込むように構成され得る。システム１１００は、いくつかの点においては、図２に関連して記載されるシステム２００と同様に操作するように構成され得る（図解の単純化のために、全ての構成要素は図１１に示されていないが、図１１のシステム１１００は、図２のシステム２００の構成要素に類似する構成要素を含み得ることに注意する）。システム１１００に類似するシステムは、既に参考として援用されている同一出願人による同時係属の米国仮特許番号第６０／６１０，７１５号に詳細に記載される。

【０１７５】

当業者は、フィッシングおよび／またはスプーフィング詐欺を行う場合には、詐欺師はしばしば大量の電子メール伝送を生成し、（例えば）受信者を詐欺師のウェブサイトにログオンさせるために検索され、詐欺師のウェブサイトは、正当な（しばしば周知の）会社（例えば、銀行、オンラインの商売のサイトなど）のウェブサイトであると考えられるように工作され得ることを、認識する。詐欺を強化するために、結果として、詐欺師はしばしば正当な会社からの実際の電子メールメッセージに可能な限り近く、複製および／または偽装することを試行する。それゆえ、多くの場合には、メッセージヘッダのあるフィールド（例えば、「ＦＲＯＭ：」、「ＳＥＮＤＥＲ：」、「ＲＥＴＵＲＮ　ＰＡＴＨ：」および／または「ＲＥＰＬＹ－ＴＯ：」フィールド）は、正当な会社によって送信された実際のメッセージから対応するヘッダからコピーされ、かつ／または対応するヘッダと考えられるように偽造され得る。

【０１７６】

このような間違ったヘッダ情報を含むことは、詐欺師がこのようなメッセージの受信者を混乱させることを助けるが、間違ったヘッダ情報はまた、試行される詐欺のようなオンラインの不正使用の可能性の検出を助けるために使用され得る。当業者は、メールサーバがそのメールサーバのアドレスにアドレスされる電子メッセージを受信する場合は、メールサーバはそのメッセージに関連するメールボックスにメッセージを発送することを試行することを認識する。このようなメールボックスがない場合には、メールサーバはしばしば、これらのフィールド（例えば、「ＲＥＴＵＲＮ－ＰＡＴＨ：」フィールド）の１つ以上を、メッセージの送信者に、メッセージにおいて特定されるアドレスに対してメッセージが届けられ得ないことを通知することの試行において「バウンス（ｂｏｕｎｃｅ）」メッセージを送信するために使用する。メッセージのヘッダ情報は、正当な会社がメッセージの送信者であることを示す場合には（しかしながら、例えば、詐欺師がメッセージを真正であると考えさせたい場合には）、「バウンス」メッセージは、詐欺師に戻らないように伝送されるが、代わりに正当な会社に伝送される。

【０１７７】

さらに、多くの場合には、バウンスメッセージが、詐欺師によって送信された元々のメッセージのコピー（または元々のメッセージの一部）に添付されているので、バウンスメッセージから、例えば、以下に記載される方法および／またはシステムを用いて、有意な情報は収集され得る。詐欺師はしばしば、認証されていない電子メールアドレスの集団に一気に送信するので、任意の所与の一気のメッセージは送達されないメッセージの相当な部分を含む。それゆえ、正当な会社によって受信されるメッセージの解析は、オンラインの不正使用の可能性の早期の検出を円滑にし得る。

【０１７８】

図１１のシステム１１００は、この処理のために使用され得る。図２に関連して記載される構成要素に加えて、システム１１００は、モニタリングアプライアンス１１０５を付加的に特徴とし得、モニタリングアプライアンス１１０５は、特定の実施形態において顧客２２５のサイトに位置し得る。しかしながら、他の実施形態においては、モニタリングアプライアンス１１０５は、他の場所に位置し得る（モニタリングセンタ２１５などに含まれる）。一部の実施形態に従って、モニタリングアプライアンス１１０５は、汎用コンピュータ（例えば、上記したコンピュータ）を、可能性としては顧客の電子メールシステムとインターフェースするためのおよび／または以下に記載される他のタスク（本発明の方法を含むがこれらには限定されない）を行うためのソフトウェアと共に備え得る。他の実施形態においては、モニタリングアプライアンス１１０５は、これらのタスクを行うためのハードウェア、ファームウェアおよび／またはソフトウェア命令を有する、専用マシンであり得る。

【０１７９】

モニタリングアプライアンス１１０５は、顧客の電子メールシステム１１１０と通信し得る。正当な会社（例えば、顧客）は、フィッシング詐欺に関心がある（そうでなければ、その会社から発生すると称するメールに気付きたい）任意の実体であり得、オンラインの存在を有し、かつ／または消費者、メンバなどと、電子メールを経由して通信することが予期される組織（例えば、銀行、オンラインコマースのウェブサイト、オンラインオークションサイトなど）を含むが、これらには限定はされない。電子メールシステム１１１０は、ＳＭＴＰサーバ、ＰＯＰ３サーバ、メール転送エージェント（「ＭＴＡ」）、および／または任意の他の共通に利用可能な電子メールサーバおよび／またはクライアントソフトウェアを含み得るが、これらに限定はされない。標準の電子メールシステムは、本発明の一部の実施形態に従って使用され得る。他の実施形態においては、電子メールシステム１１１０は、（例えば、モニタリングアプライアンス１１０５に統合されるように）特別に構成され得る。

【０１８０】

モニタリングアプライアンス１１０５は、顧客によって操作され得かつ／または第三者（例えば、セキュリティサービスプロバイダなど）によって操作され得る。モニタリングアプライアンス１１０５は、電子メールシステム１１１０に近接して位置され得、かつ／またはモニタリングアプライアンス１１０５が電子メールシステム１１１０と通信している限りは、電子メールシステム１１１０から離れ得る。一部の実施形態においては、モニタリングアプライアンスが、電子メールゲートウェイ、ＭＴＡ、ＳＭＴＰサーバなどと通信し得、かつ／または統合され得ることにより、モニタリングアプライアンスが電子メールシステム１１１０に入力する全ての電子メールメッセージに対するアクセスを有する。（特定の場合には、モニタリングアプライアンス１１０５は、標準のメールシステム構成要素の変更によって具体化され得、モニタリングアプライアンス１１０５は、実際に、電子メールシステム１１１０の一部である）。他の場合には、システム１１００は構成され得、電子メールシステム１１１０（および／またはその構成要素）が、特定のメッセージ（例えば、これらのメッセージを「バウンス」メッセージとして識別し得るある判定基準に合うメッセージ）のコピーをモニタリングアプライアンス１１０５に送信する。

【０１８１】

モニタリングアプライアンス１１０５は受信される電子メールメッセージを解析するように構成される詐欺防止および／または検出システム（例えば、マスタコンピュータ２１０、モニタリングコンピュータ２２０、および／または図２に関連して記載される他のシステム構成要素を含む）とさらに通信し得る。それゆえ、モニタリングアプライアンス１１０５は、相関エンジン（例えば、図１Ａに関連して記載される相関エンジン１２５）、および／またはイベントマネージャ（例えば、図１Ａのイベントマネージャ１３５）と直接的または間接的に通信し得、これらのいずれかまたは双方が、電子メールシステム１１１０によって受信される特定の「バウンス」メッセージに含まれる電子メールメッセージを、可能性としては以下にさらに詳細に記載される方法を用いて、解析するために使用さ

れ得る。相関エンジンは、より大きな詐欺検出および／または防止システムの一部であり得（しかし、必ずしもそうである必要はない）、顧客にローカルに位置され得る。しかしながら、他の場合には、相関エンジンは、サイトの外に配置され得る。そういうものとして、相関エンジンはセキュリティプロバイダによって管理され得、かつ／または種々の供給源（様々な顧客、他のデータ供給源（これらの一部が本明細書に記載される）などを含むがこれらに限定はされない）から受信されるデータに基づいて詐欺の出来事の可能性を解析するために使用され得る。

【０１８２】

以下の例は、システム１１００の操作の１つのモードを図示している。この例においては、顧客が銀行であることが仮定される。詐欺師は、複数のアドレスにアドレスされる電子メールメッセージを作成し、複数のアドレスの一部は、詐欺師が銀行の顧客であると仮定する。この「元々の」メッセージは、「貴重な顧客」にアドレスされたと考えられ、銀行から発生していると考えられ、実際は、メッセージのリターンパスはメッセージの「ＲＥＴＵＲＮ－ＰＡＴＨ：」フィールドにおいて、銀行の電子メールシステム１１００（または銀行の電子メールシステムに関連するアドレス）を列挙する。詐欺師は、この元々のメッセージを、詐欺師（または別の人）によって維持されるスパムリストから抜粋される多くの（可能性としては数十万の）アドレスに送信するために、メールサーバ１１１５を使用する。（当業者は、フィッシュメール送信者がしばしばフィッシュ電子メールを送信するために、危険にさらされている電子メールサーバ、開いているリレーなどを使用するが、この例の目的においては、このような区別は重要ではないことを認識する）。これらのアドレスの１つが＜ｊｏｅ＿ｕｓｅｒ@ｕｓｅｒ．ｃｏｍ＞であると仮定すると、詐欺師の電子メールサーバ１１１５は＜ｕｓｅｒ．ｃｏｍ＞ドメインに関連するメールサーバ１１３０に、ユーザ「ｊｏｅ＿ｕｓｅｒ」による受信のためにメッセージを伝送する。「ｊｏｅ＿ｕｓｅｒ」が＜ｕｓｅｒ．ｃｏｍ＞のメールサーバ１１３０に知られていない場合には、そのメールサーバ１１３０は、返答（上で議論されるように元々のメッセージの送信者に「バウンス」メッセージ）を、送信することを試行する。しかしながら、「ＲＥＴＵＲＮ－ＰＡＴＨ：」フィールドは銀行の電子メールシステム１１１０を向いているので、＜ｕｓｅｒ．ｃｏｍ＞メールサーバ１１３０は実際の送信者（詐欺師の電子メールサーバ１１１５）の代わりに銀行のシステム１１１０に「バウンス」メッセージを送信する。

【０１８３】

銀行の電子メールシステム１１１０がこのメッセージを受信する場合には、このメッセージは「バウンス」メッセージとして識別され、モニタリングアプライアンス１１０５に転送する。（あるいは、例えば、モニタリングアプライアンスが、メールゲートウェイおよび／またはＭＴＡに統合され、および／またはメールゲートウェイおよび／またはＭＴＡとして提供される場合には、モニタリングアプライアンス１１０５は、電子メールシステム１１１０による受信の前に、このようなメッセージの全てを遮断し得る。さらに他の実施形態においては、モニタリングアプライアンス１１０５は、バウンスメッセージを引き出すためにメールシステム１１１０にアクセスし得る）。モニタリングアプライアンス１１０５は、選択的に記憶媒体１１２５（これはＲＡＭ、ハードディスク、１つ以上のデータベースなど）を、このようなメッセージ（および／またはこのようなメッセージの特定の部分、このようなメッセージについての情報など）を、記憶するために含み得（例えば、いくつかが受信されるまでメッセージを記憶するため）、メッセージは、伝送の前に、および／または一括フォーマットにおいて伝送される前に、統合され得、要約され得るなどする。単なる例として、複数のバウンスメッセージが受信され、全てが共通の大量メール送信に関連する場合には、元々のメッセージの１つのコピーをバウンスメッセージの収集についての情報の概略（例えば、各々のメッセージの向けられる受信者、メッセージ間の差異の概略など）と共に提供することがより効果的である。モニタリングアプライアンス１１０５は、次いで、「バウンス」メッセージ（および／または概略情報）をフィッシュ検出／モニタリングシステム（例えば、図１Ａに描かれるシステム１００）に送信し

得、フィッシュ検出／モニタリングシステムは、図２のシステム２００および／またはその構成要素（相関エンジン、イベントマネージャなどを含むがこれらに限定はされない）によって具体化され得る。メッセージは、一括フォーマットで、１つ以上の統合されたメッセージなどとして個別に送信され得る。

【０１８４】

一部の実施形態に従うと、モニタリングアプライアンス１１０５は、受信されるメッセージを特定のアイテム（メッセージに含まれるユニフォームリソースロケータ（「ＵＲＬ」）を含むがこれらに限定はされない）において解析するように構成され得、フィッシュ検出／モニタリングシステムに、全体のメッセージの代わりにこれらの解析されたアイテムのみを伝送し得る。さらなる実施形態においては、相関エンジンの一部の局面が、モニタリングアプライアンス１１０５内に組み込まれ得ることにより、メッセージの解析の一部（または全て）がモニタリングアプライアンス１１０５において発生する。

【０１８５】

特定の実施形態においては、電子メールシステム１１１０（および／またはモニタリングアプライアンス１１０５および／または詐欺検出／防止システム）は、メールシステムエラーのログ１１２０（「バウンス」メッセージの記録および／またはバウンスメッセージについての情報（例えば、メッセージの抽出された部分、元々のメッセージのアドレスなど）を含むがこれらに限定はされない）を維持し得る。このログ１１２０は、検索され得ることにより、送達できないアドレスにより生じるエラーを決定する。この情報は、多くの方法において使用され得る。単なる例として、フィードバックループは利用され得ることにより、「送達できない」アドレスが他の反詐欺操作のおとりの電子メールアドレスとして使用され得る。例えば、「バウンス」メッセージ（１人以上の顧客から取得される）が、特定のアドレスおよび／またはドメインはしばしば詐欺師によって使用されることを指示する場合には、そのアドレスおよび／またはドメインを登録することを試行し、これによってそのアドレスにアドレスされるメールの直接の受信を確実にすることが望まれ得る。このようなアドレスはまた、上にさらに詳細に記載したように「ｍａｒｋｅｄ　ｍｏｎｅｙ」操作のためのトレース可能な情報をプラントするために使用され得る。

【０１８６】

図１１Ｂは、顧客のオンラインアイデンティティの不正な使用を識別する方法１１５０を図示している（例えば、顧客から送信されたと考えられる電子メールに基づいたフィッシング詐欺において）。方法１１５０は、本明細書に記載される他の方法と同様に任意の適切な様式でインプリメントされ得、特定の構造に限定されないことが理解されるべきだが、方法１１５０は図１１Ａのシステム１１００のようなシステム上でインプリメントされ得る。方法１１５０は、モニタリングアプライアンス（例えば、上記したモニタリングアプライアンス）を提供することを含み得る（ブロック１１５５）。モニタリングアプライアンスを提供することは、一部の実施形態においては、顧客の位置にモニタリングアプライアンスを設置することを含み得、かつ／または他の実施形態においては、モニタリングアプライアンスに相関エンジン（上記した）または同様の機能性を提供することを含み得る。（他の実施形態においては、上記したように、モニタリングアプライアンスは他の場所に設置され得、実際には、上記したように、詐欺防止システム、またはこのようなシステムの構成要素（例えば、相関エンジン）内に組み込まれ得る）。モニタリングアプライアンスを提供することはまた、モニタリングアプライアンスと顧客の電子メールシステムとの間の通信を提供することを含み得る。

【０１８７】

ブロック１１６０において、顧客の電子メールシステムは、通例の様式で電子メールメッセージを受信する。一部の実施形態においては、顧客の電子メールシステムは返答メッセージ（例えば、上記した「バウンス」メッセージ）としてメッセージを識別し得る（ブロック１１６５）。ブロック１１７０において、メッセージはモニタリングアプライアンスに転送され得る（および／または、他の場合にはメッセージはモニタリングアプライアンスによってアクセスされる）。上記したように、一部の場合には、「バウンス」メッセ

ージとして識別されるメッセージのみがモニタリングアプライアンスに転送される。他の場合には、顧客の電子メールシステムは全てのメッセージ（または、未知の送信者からの全てのメッセージなどのようなメッセージのサブセット）を転送するように構成され得る。さらに他の実施形態においては、モニタリングアプライアンスは顧客の電子メールシステムに（メール記憶装置、特定の電子メールアカウント、電子メールシステムログなどにアクセスすることによって）直接アクセスするように構成され得ることにより、電子メールシステムに対して、モニタリングアプライアンスにメッセージを転送することが必要ではあり得ない。同様に、電子メールシステムは、ログ（例えば、ファイアウォールログ、電子メールシステムログなど）からモニタリングアプライアンスまでの関連する入力を転送するように構成され得（ブロック１１７５）、または、代替的に全てのログ入力を転送するように構成され得る（この場合においては、モニタリングアプライアンスは、関連する入力に対してログ入力を解析するように構成され得る）。関連する入力は、バウンスのメッセージなどに関連する任意の入力を含み得る。他の実施形態においては、上記したように、モニタリングアプライアンスがこのようなログに直接アクセスするように構成され得ることにより、ログ入力を転送することが不必要である。

【０１８８】

一部の場合には、例えば、上記したような様式で、メッセージ（および、特にバウンスメッセージ）の関連する部分を引き出すことがより効果的であり得る（ブロック１１８０）。関連する部分は（バウンスメッセージが応答する）元々のメッセージをフィッシュメッセージとして識別するために使用され得るメッセージの任意の部分、メッセージの元々の送信者を識別するために使用され得るメッセージの任意の部分、および／またはメッセージの意図された受信者（受信者は実際にはフィッシング詐欺の目標であり得る）を識別するために使用され得るメッセージの任意の部分を含み得る（が限定はされない）。単なる例として、メッセージのヘッダ、任意のＵＲＬは、メッセージおよび／またはメッセージの本体からの任意の関連するテキスト（特に、バウンスメッセージの本体において再生成された元々のメッセージの任意の関連する部分を含む）に含まれる。

【０１８９】

同様に、一部の場合には、解析のために概略のメッセージをコンパイルすることが好まれ得る（ブロック１１８５）。概略のメッセージは、メッセージのグループを解析するために必要な情報を含む任意の統合されたメッセージを備え得る。（メッセージおよび／またはメッセージの部分自体とは対照的に）概略のメッセージの使用は、一部の場合には、メッセージ解析などに使用される解析、処理サイクル、および／または時間に対する、メッセージを伝送するために使用されるバンド幅における効率を提供し得る。例えば、１回の大量メール送信に関連する複数のバウンスメッセージを電子メールシステムが受信する場合には、概略のメッセージの使用は、特に有利であり得る（これは複数のバウンスメッセージの各々が、それぞれの元々のメッセージが類似の「ＲＥＴＵＲＮ　ＰＡＴＨ：」または「ＦＲＯＭ：」ヘッダを有することを各々指示する事実、および／または複数のバウンスメッセージの各々の、それぞれの本体部分が元々のメッセージの類似部分を再生成する事実によって指示され得る）。このような複数のメッセージを比較するための様々な方法（例えば、メッセージの全ておよび／または一部にチェックサムを行うこと、ハッシングを行うことなど）、およびチェックサム、ハッシュなどを比較するための様々な方法が使用され得る。メッセージを比較する他の手法は、同様に使用され得る。

【０１９０】

一部の実施形態に従って、１つ以上の電子メールメッセージ、メッセージの一部、および／または（適切である場合には）概略のメッセージが、解析のために詐欺検出システムおよび／または詐欺防止システムに転送され得る（ブロック１１９０）。同様に、ログ入力（またはこのような入力の概略）は転送され得る。転送は、任意の適切な方法（例えば、ＦＴＰ、ＮＦＳマウント、データベーストランザクション（例えば、ＳＱＬ命令文）など）によって行われ得る。一部の場合には、メッセージ、ログ、および／またはログ入力（および／または、これらの一部または概略）は、（例えば、特定のスケジュールで、お

よび／またはある数のメッセージを受信した際などにバッチ転送を可能にするために）転送の前にモニタリングアプライアンスにローカルに記憶され得る。特定の実施形態においては、メッセージを記憶することは（可能性としては、様々なヘッダフィールドおよび／または本体テキストなどに対応するフィールドを用いて）データベースにメッセージを記憶することを包含し得ることにより、メッセージを転送することがデータベースの同期を包含し得る。あるいは、メッセージはテキストファイルなどとして記憶され得、および／または解析のための詐欺防止システムへの転送は、このようなファイルを、詐欺防止システムにおけるデータベースのために適切なインポートトランザクション（またはトランザクションの連続）にインポートすることを包含し得る。別の例として、詐欺防止システムは上記した方法を行うように構成され得、かつ／またはメッセージ（または一部、概略など）を転送することは、上で議論されるこのような方法を用いて解析のために適切なフォーマットでメッセージを転送すること（かつ／またはメッセージを適切なフォーマットに変換すること）を包含し得る。例えば、メッセージはハニーポットに転送され得、結果として、メッセージの処理は上記したように進められ得る。

【０１９１】

それゆえ、方法１１５０は、メッセージ、ログ、ログ入力を解析することをさらに包含し得る（ブロック１１９４）。記したように、メッセージの解析は、上記した方法を用いる解析を備え得る。（同様に、メッセージ、ログ、ログ入力の解析が、オンライン詐欺の可能性があることを指示する場合には、応答戦略および／または上記した方法はまたインプリメントされ得る）。（例えば、メッセージが詐欺防止システムに転送された場合には）解析は、詐欺防止システム、および／または相関エンジンのような詐欺防止システムの構成要素によって行われ得る。

【０１９２】

しかしながら、記されたように、他の実施形態に従って、モニタリングアプライアンスは相関エンジンを備え得、かつ／または（同様の方法を用いる）メッセージの解析などは、モニタリングアプライアンスにおいて行われ得る。このような場合には、解析の結果がイベントマネージャおよび／またはダイリューションエンジン（または類似の構成要素）に転送され得、これは、さらなる行動のために適切に、詐欺防止システム内に組み込まれ得、かつ／または、モニタリングアプライアンス内に組み込まれ得る。

【０１９３】

特定の実施形態においては、メッセージなどの解析は、メッセージの意図された受信者を識別することを含み得る（ブロック１１９８）。この情報は、例えば、意図される受信者に対応する新しい電子メールアドレスを生成するために使用され得る。（加えて、新しい電子メールアドレスは、所望される場合には、上記されるように様々な位置にプラントされ得る）。もちろん、本開示に基づいて、アドレスに関連するドメインネームを取得すること、および／またはそのドメインネームに責任のあるプロバイダにアカウントを作成することが必要であり得ることにより、セキュリティプロバイダがそのアドレスにアドレスされる全てのメールを受信することを、当業者は認識する。フィッシュメッセージの意図された受信者のアドレスの状態によって、アドレスは既に少なくとも１人の詐欺師の目標であることが明らかであるから、これは有利であり得る。おそらく、フィッシュメッセージが送達できなかったという事実は、そのアドレスが現在は有効なアドレスではないということを指示するので、この受信者の電子メールアドレスを取得することは、実際のユーザに争いを作成しない。

【０１９４】

図示の目的のために、前述の記載において、様々な方法が特定の順序で記載された。代替的な実施形態において、方法は記載された順序と異なる順序で行われ得ることが認識されるべきである。上記した方法は、ハードウェア構成要素によって行われ得、かつ／またはマシン実行可能な命令のシーケンスで統合され得、マシン実行可能な命令は、マシン（例えば、汎用のまたは専用のプロセッサ、あるいは命令と共にプログラムされる論理回路）に方法を行わせるために使用され得る。これらのマシン実行可能な命令は、１つ以上の

マシン読み取り可能な媒体（例えば、ＣＤ－ＲＯＭまたは他のタイプの光学ディスク、フロッピー（登録商標）ディスケット、ＲＯＭ、ＲＡＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、磁気的または光学的カード、フラッシュメモリ、あるいは他のタイプの電子命令を記憶することに適したマシン読み取り可能な媒体）上に記憶され得る。単なる例として、本発明の一部の実施形態はソフトウェアプログラムを提供し、ソフトウェアプログラムは、上記した方法を行うために、１つ以上のコンピュータ上で実行され得る。例えば、特定の実施形態においては、様々なハードウェアデバイス上で実行するように構成されている、複数のソフトウェア構成要素があり得る。あるいは、方法はハードウェアとソフトウェアとの組み合わせによって行われ得る。

【０１９５】

結論として、本発明はオンライン詐欺を扱うための新規な解決策を提供する。本発明の１つ以上の実施形態の詳細な記載は上で与えられるが、様々な代替案、変更案、および同等案は、本発明の精神から変更することなしに、当業者にとって明白である。さらに、明らかに不適切な場合、または他に特に記載される場合を除いて、異なる実施形態の特性、デバイスおよび／または構成要素は、代替され得、および／または組合わされ得ることが仮定されるべきである。従って、上の記載は、本発明の範囲を限定するととられるべきではなく、本発明の範囲は添付する特許請求の範囲によって定義される。

【図面の簡単な説明】

【０１９６】

【図１Ａ】図１Ａは、本発明の様々な実施形態に従う、オンライン詐欺に対抗するためのシステムを図示する機能図である。

【図１Ｂ】図１Ｂは、本発明の様々な実施形態に従う、おとりの電子メールアドレスをプラントするためのシステムを図示する機能図である。

【図２】図２は、本発明の様々な実施形態に従う、オンライン詐欺に対抗するためのシステムを図示する概略図である。

【図３】図３は、本発明の様々な実施形態に従う、オンライン詐欺に対抗するためのシステムにおいてインプリメントされ得るコンピュータの一般化された概略図である。

【図４Ａ】図４Ａは、本発明の様々な実施形態に従う、詐欺の可能性のある活動についての情報を取得するための様々な方法を図示する処理フロー図である。

【図４Ｂ】図４Ｂは、本発明の様々な実施形態に従う、詐欺の可能性のある活動についての情報を取得するための様々な方法を図示する処理フロー図である。

【図４Ｃ】図４Ｃは、本発明の様々な実施形態に従う、詐欺の可能性のある活動についての情報を取得するための様々な方法を図示する処理フロー図である。

【図５Ａ】図５Ａは、本発明の様々な実施形態に従う、データを収集および解析する方法を図示する処理フロー図である。

【図５Ｂ】図５Ｂは、本発明の様々な実施形態に従う、ユニフォームリソースロケータおよび／またはウェブサイトを解析するための手順を図示する処理フロー図である。

【図６】図６は、本発明の様々な実施形態に従う、オンライン詐欺に対抗する方法を図示する処理フロー図である。

【図７】図７は、本発明の様々な実施形態に従う、疑わしいユニフォームリソースロケータおよび／またはウェブサイトを調査する方法を図示する処理フロー図である。

【図８】図８は、本発明の様々な実施形態に従う、試行されるオンライン詐欺に応答する方法を図示する処理フロー図である、

【図９Ａ】図９Ａは、本発明の様々な実施形態に従う、フィッシング詐欺に応答を提示するために使用され得るシステムを図示している。

【図９Ｂ】図９Ｂは、本発明の様々な実施形態に従う、フィッシング詐欺に応答を提示する方法を図示している。

【図１０】図１０は、本発明の様々な実施形態に従う、フィッシング詐欺に応答を提示するために使用され得るシステムを図示している。

【図１１Ａ】図１１Ａは、本発明の様々な実施形態に従う、顧客のオンラインアイデンテ

ィティの不適切な使用を識別するために使用され得るシステムを図示している。
【図１１Ｂ】図１１Ｂは、本発明の様々な実施形態に従う、顧客のオンラインアイデンティティの不適切な使用を識別する方法を図示する処理フロー図である。

【図１Ａ】

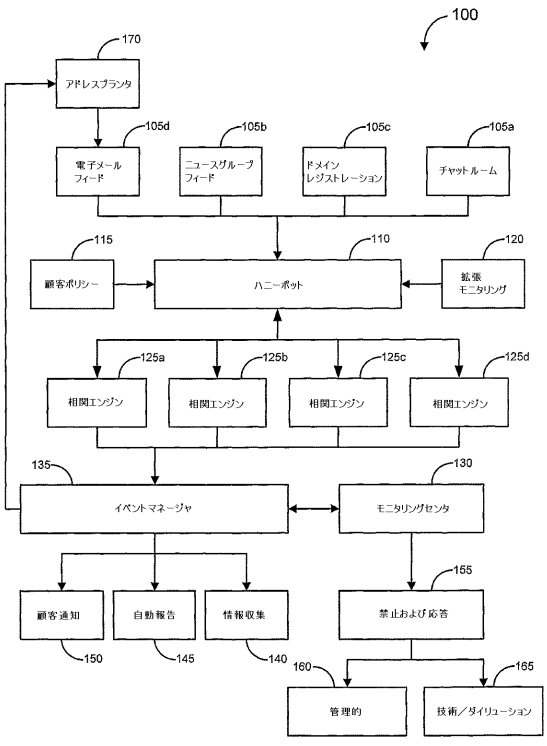


Fig. 1A

【図１Ｂ】

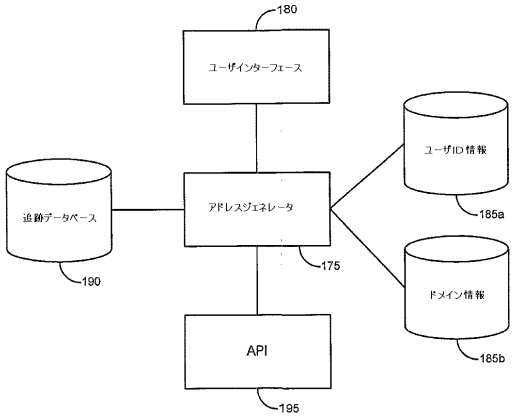


Fig. 1B

【図２】

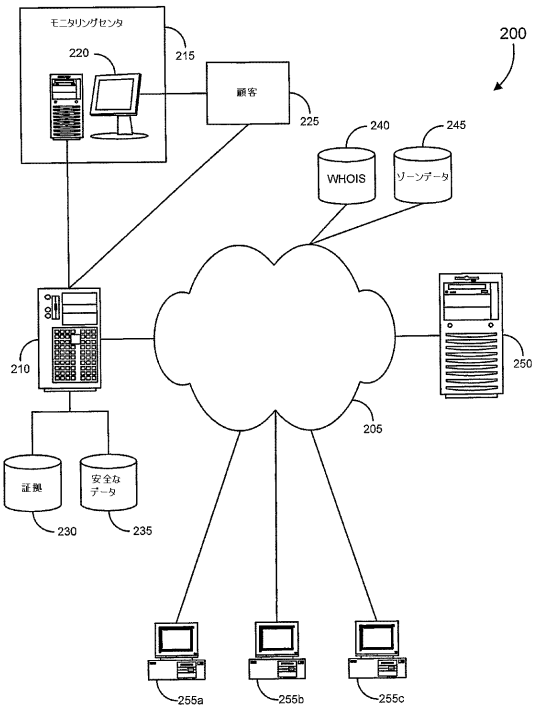


Fig. 2

【図３】

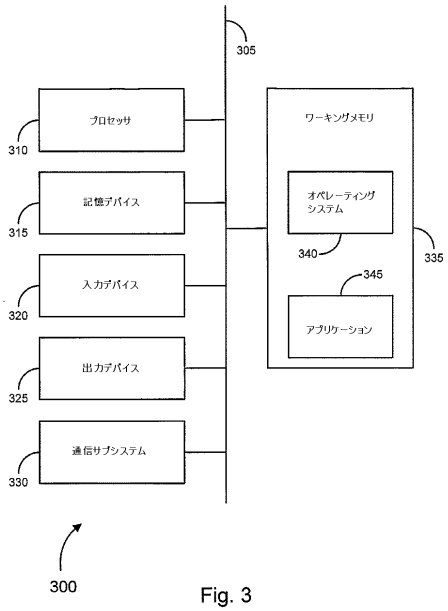


Fig. 3

【図４Ａ】

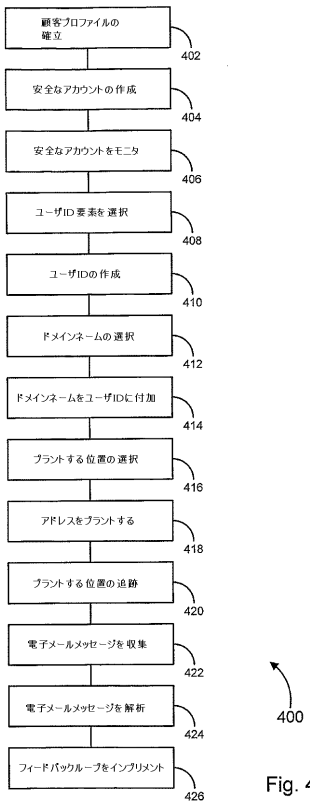


Fig. 4A

【図４Ｂ】

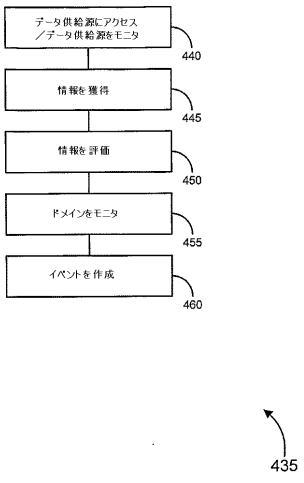


Fig. 4B

【図４Ｃ】

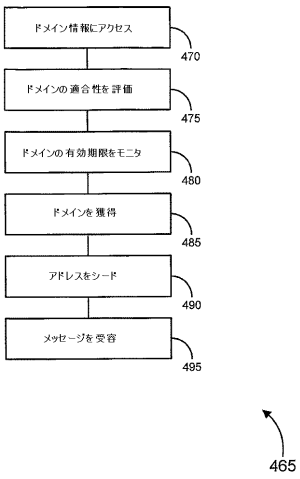


Fig. 4C

【図５Ａ】

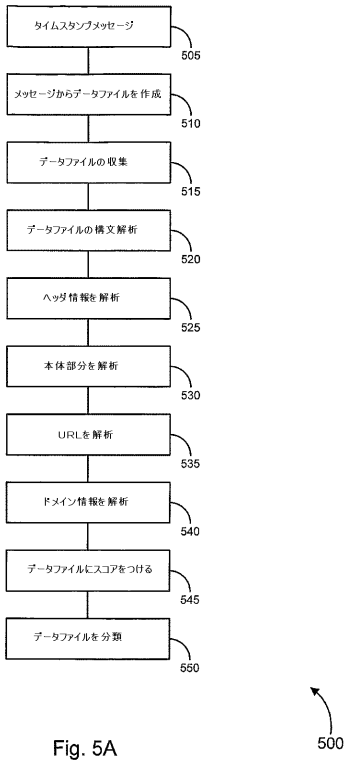


Fig. 5A

【図５Ｂ】

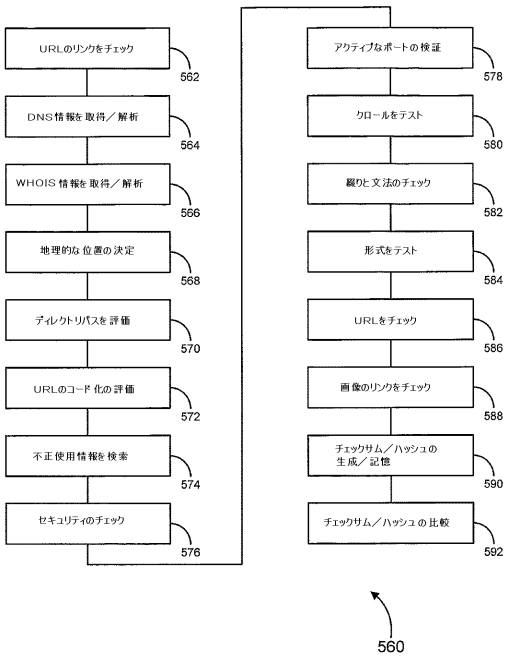


Fig. 5B

【図６】

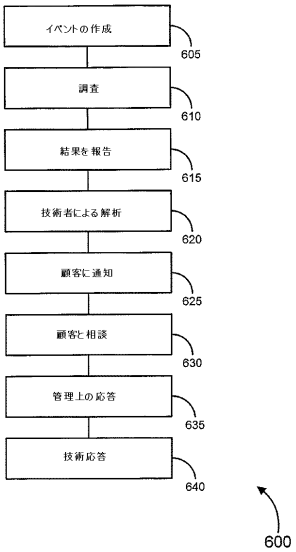


Fig. 6

【図７】

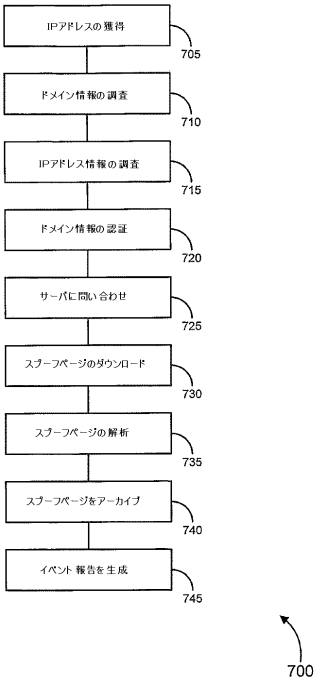


Fig. 7

【図８】

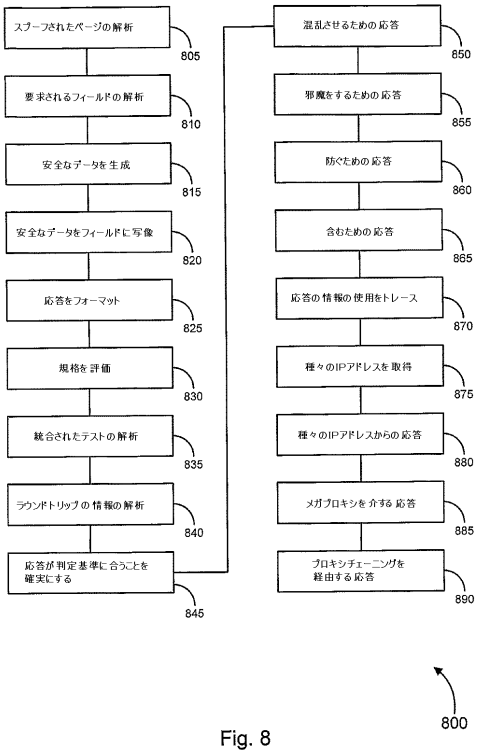


Fig. 8

【図９Ａ】

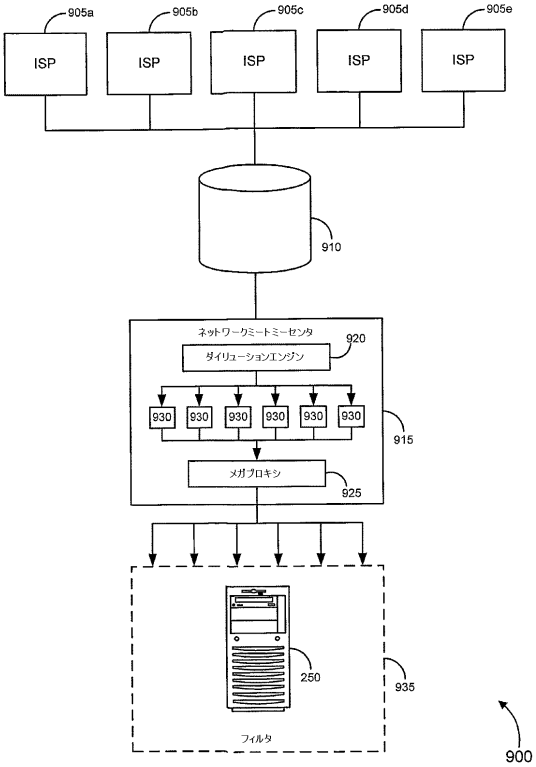


Fig. 9A

【図９Ｂ】

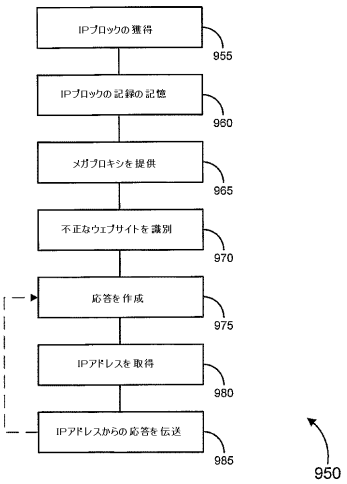


Fig. 9B

【図１０】

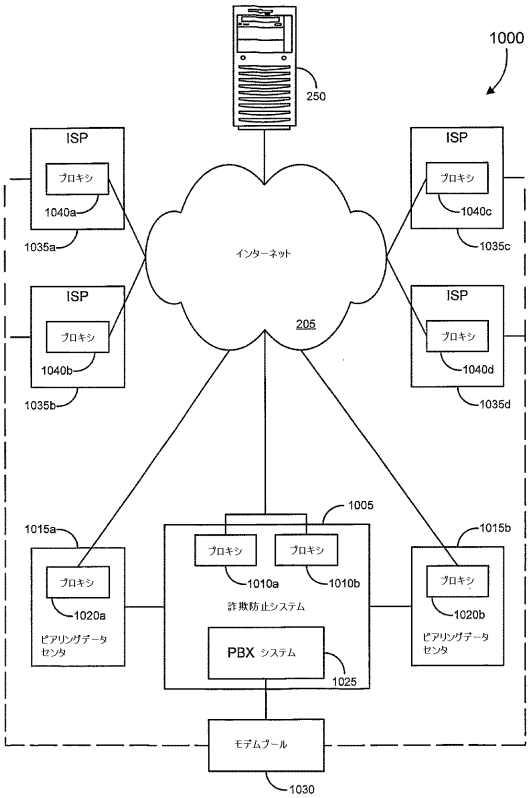


Fig. 10

【図１１Ａ】

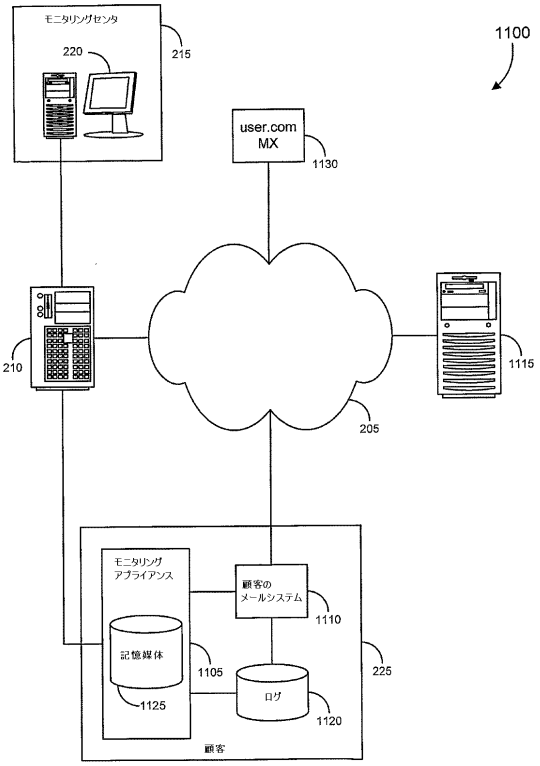


Fig. 11A

【図１１Ｂ】

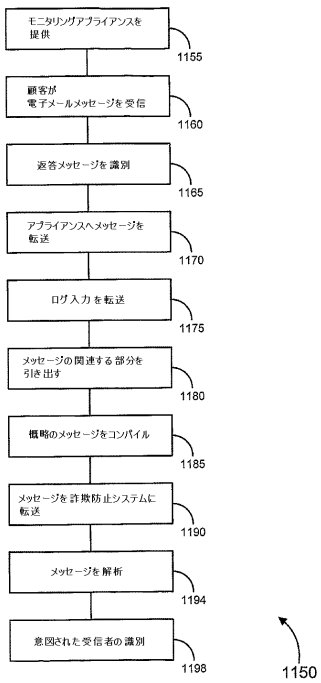


Fig. 11B

【国際調査報告】

60700820059

11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/42753

A. CLASSIFICATION OF SUBJECT MATTER
IPC: G06F 11/00(2006.01)

USPC: 726/22
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)
U.S. : 726/22

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)
EAST, IEEE, GOOGLE, ACM

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,606,659 B1 (Hegli et al) 12 Aug. 2003 (12.08.2003), Figs 6 steps 402-409,420,426, Fig 7 steps 504,508,510526,530,Fig 11 steps 854,858,860,862,Fig 13 steps 954,958 and col 2 lines 39-61,col 3 lines 43-51,col 4 lines 20-29,col 4 lines 56-67,col 5 lines 13-22,col 7 lines 5-18,col 7 lines 45-50 and col 8 lines 1-13.	1-81

☐ 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 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
02 August 2007 (02.08.2007)	12 SEP 2007
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	Authorized officer Fikremariam Yalew Telephone No. 5712723852 Jean Proctor Paralegal Specialist

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

18.12.2007

フロントページの続き

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

（特許庁注：以下のものは登録商標）
１．Ｌｉｎｕｘ

(72)発明者 シュレイム, イハブ
アメリカ合衆国 メリーランド ２０８７４, ジャーマンタウン, クイーンズタウン レーン １３３０７
(72)発明者 シュル, マーク
アメリカ合衆国 メリーランド ２０８１５, シェビー チェース, オックスフォード ストリート ２０３

Ｆターム(参考) 5B285 AA06 BA01 CA32 CA33 DA05