(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2009-507268
(P2009-507268A)
(43)公表日　平成21年2月19日(2009.2.19)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B017
G06Q 50/00	(2006.01)	G06F	17/60	132	5B285
G06F 21/24	(2006.01)	G06F	12/14	520A	

審査請求 未請求　予備審査請求 未請求　（全 32 頁）

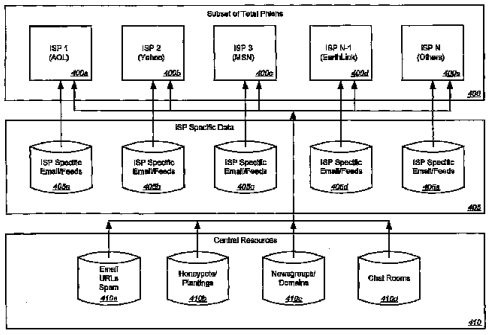
(21)出願番号　特願2008-519703 (P2008-519703)
(86)(22)出願日　平成18年6月30日 (2006.6.30)
(85)翻訳文提出日　平成20年2月18日 (2008.2.18)
(86)国際出願番号　PCT/US2006/026039
(87)国際公開番号　WO2007/005868
(87)国際公開日　平成19年1月11日 (2007.1.11)
(31)優先権主張番号　60/696,006
(32)優先日　平成17年7月1日 (2005.7.1)
(33)優先権主張国　米国 (US)

(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】改良された不正行為監視システム

(57)【要約】
本発明の種々の実施形態は、改良された不正行為検出および／または防止のシステムならびに方法を提供する。一組の実施形態は、例えば、企業（オンライン会社、銀行、ＩＳＰなど）が不正行為のフィード（一例の名前を挙げると、これら会社の顧客に宛てられた第三者からの電子メール・メッセージのフィード）をセキュリティ・プロバイダ提供する設備を提供し、さらに、そのような設備を実現するシステムおよび方法を提供する。一部の実施形態では、フィード（メッセージなど）が解析されて正規化された直接データおよび／または派生データが作成され、このデータは当該企業が（可能性としては有料で）利用し得る。



【特許請求の範囲】
【請求項１】
改良された不正行為監視を提供する方法であって、該方法は、
不正オンライン活動に関する直接情報を第１エンティティから受信することと、
該直接情報を解析することと、
該不正オンライン活動に関連した一組の正規化データを作成することであって、該一組の正規化データは、複数のエンティティにより読み取り可能な形式である、ことと、
該一組の正規化データを格納することと
を含む、方法。
【請求項２】
前記直接情報を解析することは、前記不正オンライン活動に関する一組の派生情報を生成することを含む、請求項１に記載の方法。
【請求項３】
前記不正オンライン活動に関する前記一組の派生情報を生成することは、前記直接情報と、他の不正オンライン活動に関して以前保存された情報とに基づく、請求項２に記載の方法。
【請求項４】
前記保存された情報は、直接情報および派生情報を含む、請求項３に記載の方法。
【請求項５】
前記一組の正規化データは、前記直接情報および前記派生情報を含む、請求項２に記載の方法。
【請求項６】
前記複数のエンティティのうちの第２エンティティから、前記格納された正規化データにアクセスするためのリクエストを受信することと、
該格納された正規化データへの該第２エンティティによるアクセスを制御することと
をさらに含む、請求項１に記載の方法。
【請求項７】
前記格納された正規化データへの前記第２エンティティによるアクセスを制御することは、前記第１エンティティと該第２エンティティとの間の取り決めに基づく、請求項６に記載の方法。
【請求項８】
前記格納された正規化データの少なくとも一部を前記第２エンティティに提供することをさらに含む、請求項６に記載の方法。
【請求項９】
前記直接情報を前記第１エンティティから受信することは、アプリケーション・プログラム・インターフェイス（ＡＰＩ）を介して該直接情報を受信することを含む、請求項６に記載の方法。
【請求項１０】
前記格納された正規化データにアクセスするための前記リクエストを受信することは、前記ＡＰＩを介して該リクエストを受信することを含む、請求項９に記載の方法。
【請求項１１】
前記格納された正規化データは前記第１エンティティにより保持されており、前記ＡＰＩは、該第１エンティティから該格納された正規化データをリクエストするための機能を前記第２エンティティに提供する、請求項１０に記載の方法。
【請求項１２】
前記格納された正規化データはセキュリティ・サービスにより保持されており、前記ＡＰＩは、前記直接情報を該セキュリティ・サービスに提供するための機能を前記第１エンティティに、該セキュリティ・サービスから該格納された正規化データをリクエストするための機能を前記第２エンティティに提供する、請求項１０に記載の方法。
【請求項１３】

前記ＡＰＩは、前記直接情報の受信、該直接情報の解析、前記一組の正規化データの作成、および前記格納された正規化データへの複数のデータ属性を介したアクセスを提供する、請求項１０に記載の方法。

【請求項１４】

前記データ属性は、前記第１エンティティまたは前記第２エンティティのいずれかに固有のエンティティ固有属性を含む、請求項１３に記載の方法。

【請求項１５】

前記データ属性は、前記第１エンティティおよび前記第２エンティティにより確立された許可に基づき、該第１エンティティと該第２エンティティとの間で共有され得る共有属性を含む、請求項１３に記載の方法。

【請求項１６】

前記ＡＰＩは、前記データ属性を定義するスキーマをさらに含む、請求項１３に記載の方法。

【請求項１７】

前記スキーマは、拡張可能なマーク付け言語（ＸＭＬ）スキーマを含む、請求項１６に記載の方法。

【請求項１８】

前記スキーマは、前記データ属性にタグ付けされたメタデータをさらに含む、請求項１６に記載の方法。

【請求項１９】

前記メタデータは、タグ付けされた前記データ属性を追跡する、請求項１８に記載の方法。

【請求項２０】

一組の命令が格納された機械可読媒体であって、該命令は、プロセッサにより実行されると、

不正オンライン活動に関する直接情報を第１エンティティから受信することと、

該直接情報を解析することと、

該不正オンライン活動に関連した一組の正規化データを作成することであって、該一組の正規化データは、複数のエンティティにより読み取り可能な形式である、ことと、

該一組の正規化データを格納することと

によって、該プロセッサに、改良された不正行為監視を実現させる、機械可読媒体。

【請求項２１】

前記複数のエンティティのうちの第２エンティティから、前記格納された正規化データにアクセスするためのリクエストを受信することと、

該格納された正規化データへの該第２エンティティによるアクセスを制御することと

をさらに含む、請求項２０に記載の機械可読媒体。

【請求項２２】

前記格納された正規化データへの前記第２エンティティによるアクセスを制御することは、前記第１エンティティと該第２エンティティとの間の取り決めに基づく、請求項２１に記載の機械可読媒体。

【請求項２３】

前記格納された正規化データの少なくとも一部を前記第２エンティティに提供することをさらに含む、請求項２１に記載の機械可読媒体。

【請求項２４】

前記直接情報を前記第１エンティティから受信することは、アプリケーション・プログラム・インターフェイス（ＡＰＩ）を介して該直接情報を受信することを含む、請求項２１に記載の機械可読媒体。

【請求項２５】

前記格納された正規化データにアクセスするための前記リクエストを受信することは、前記ＡＰＩを介して前記リクエストを受信することを含む、請求項２０に記載の機械可読

媒体。
【請求項２６】
前記格納された正規化データは前記第１エンティティにより保持されており、前記ＡＰＩは、前記第１エンティティから該格納された正規化データをリクエストするための機能を前記第２エンティティに提供する、請求項２５に記載の機械可読媒体。
【請求項２７】
前記格納された正規化データはセキュリティ・サービスにより保持されており、前記ＡＰＩは、前記直接情報を該セキュリティ・サービスに提供するための機能を前記第１エンティティに、該セキュリティ・サービスから該格納された正規化データをリクエストするための機能を前記第２エンティティに提供する、請求項２５に記載の機械可読媒体。
【請求項２８】
前記ＡＰＩは、前記直接情報の受信、該直接情報の解析、前記一組の正規化データの作成、および前記格納された正規化データへの複数のデータ属性を介したアクセスを提供する、請求項２５に記載の機械可読媒体。
【請求項２９】
前記データ属性は、前記第１エンティティまたは前記第２エンティティのいずれかに固有のエンティティ固有属性を含む、請求項２８に記載の機械可読媒体。
【請求項３０】
前記データ属性は、前記第１エンティティおよび前記第２エンティティにより確立された許可に基づき、該第１エンティティと該第２エンティティとの間で共有され得る共有属性を含む、請求項２８に記載の機械可読媒体。
【請求項３１】
改良された不正行為監視を提供するシステムであって、該システムは、
通信ネットワークと、
該通信ネットワークに通信可能に繋がれ、不正オンライン活動に関する直接情報を提供するように適合されている第１クライアントと、
該通信ネットワークに通信可能に繋がれ、不正オンライン活動に関する直接情報を前記第１クライアントから受信し、該直接情報を解析し、該不正オンライン活動に関連する一組の正規化データを作成し、該一組の正規化データを格納するように適合されているサーバであって、該一組の正規化データは、複数のクライアントにより読み取り可能な形式である、サーバと
を含む、システム。
【請求項３２】
前記サーバは、前記不正オンライン活動に関する一組の派生情報を生成するようにされに適合されている、請求項３１に記載のシステム。
【請求項３３】
前記サーバは、前記直接情報と、他の不正オンライン活動に関して以前保存された情報とに基づき、前記不正オンライン活動に関する前記一組の派生情報を生成するようになっている、請求項３２に記載のシステム。
【請求項３４】
前記保存された情報は、直接情報および派生情報を含む、請求項３３に記載のシステム。
【請求項３５】
前記一組の正規化データは、前記直接情報および前記派生情報を含む、請求項３２に記載のシステム。
【請求項３６】
第２クライアントをさらに含み、前記サーバは、前記格納された正規化データにアクセスするためのリクエストを該第２クライアントから受信し、該格納された正規化データへの該第２クライアントによるアクセスを制御するようにさらに適合されている、請求項３１に記載のシステム。

【請求項３７】
前記サーバは、前記格納された正規化データへの前記第２クライアントによるアクセスを、前記第１クライアントと該第２クライアントとの間の取り決めに基づき制御するように適合されている、請求項３６に記載のシステム。
【請求項３８】
前記サーバは、前記格納された正規化データの少なくとも一部を前記第２クライアントに提供するようにさらに適合されている、請求項３６に記載のシステム。
【請求項３９】
前記サーバは、アプリケーション・プログラム・インターフェイス（ＡＰＩ）を介して前記第１クライアントから前記直接情報を受信するように適合されている、請求項３６に記載のシステム。
【請求項４０】
前記サーバは、前記格納された正規化データにアクセスするための前記リクエストを、前記ＡＰＩを介して受信する、請求項３９に記載のシステム。
【請求項４１】
前記ＡＰＩは、前記直接情報の受信、該直接情報の解析、前記一組の正規化データの作成、および前記格納された正規化データへの複数のデータ属性を介したアクセスを提供する、請求項４０に記載のシステム。
【請求項４２】
前記データ属性は、前記第１クライアントまたは前記第２クライアントのいずれかに固有のエンティティ固有属性を含む、請求項４１に記載のシステム。
【請求項４３】
前記データ属性は、前記第１クライアントおよび前記第２クライアントにより確立された許可に基づき、前記第１クライアントと前記第２クライアントとの間で共有され得る共有属性を含む、請求項４１に記載のシステム。
【請求項４４】
改良された不正行為監視を提供するシステムであって、該システムは、
通信ネットワークと、
前記通信ネットワークに通信可能に繋がれ、不正オンライン活動に関する直接情報を生成し、前記直接情報を解析し、前記不正オンライン活動に関連する一組の正規化データを作成し、該一組の正規化データを格納するように適合されている第１クライアントであって、該一組の正規化データは、複数のクライアントにより読み取り可能な形式である、第１クライアントと、
該通信ネットワークに通信可能に繋がれ、格納された該格納された正規化データへのアクセスをリクエストするように適合されている第２クライアントと、
該通信ネットワークと通信可能に繋がれ、該格納された正規化データにアクセスするためのリクエストを前記第２クライアントから受信し、該格納された正規化データへの該第２クライアントによるアクセスを制御するように適合されているサーバと
を含む、システム。
【請求項４５】
前記サーバは、前記格納された正規化データへの前記第２クライアントによるアクセスを、前記第１クライアントと前記第２クライアントとの間の取り決めに基づき制御するように適合されている、請求項４４に記載のシステム。
【請求項４６】
前記第１クライアントは、前記格納された正規化データの少なくとも一部を前記第２クライアントに提供するようにさらに適合されている、請求項４４に記載のシステム。
【請求項４７】
前記サーバは、アプリケーション・プログラム・インターフェイス（ＡＰＩ）を介して前記リクエストを受信することにより、前記格納された正規化データにアクセスするための前記リクエストを前記第２クライアントから受信するように適合されている、請求項４

４に記載のシステム。
【請求項４８】
前記ＡＰＩは、前記格納された正規化データへの複数のデータ属性を介したアクセスを提供する、請求項４７に記載のシステム。
【請求項４９】
前記データ属性は、前記第１クライアントまたは前記第２クライアントのいずれかに固有のクライアント固有属性を含む、請求項４８に記載のシステム。
【請求項５０】
前記データ属性は、前記第１クライアントおよび前記第２クライアントにより確立された許可に基づき、該第１クライアントと該第２クライアントとの間で共有され得る共有属性を含む、請求項４８に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本願は、同時継続出願の“Ｅｎｈａｎｃｅｄ Ｆｒａｕｄ Ｍｏｎｉｔｏｒｉｎｇ Ｓｙｓｔｅｍｓ”と題された、２００５年７月１日出願の米国仮特許出願第６０／６９０，００６号からの優先権を主張し、該出願は、本明細書において、参考として、全て本書に記載したかのように本願明細書に援用される。
本願は、以下の同一所有者の同時係属出願（“関連出願”）に関し、それぞれの開示全体を、事実上、参考として、全て本書に記載したかのように本願明細書に援用される。
【０００２】
上記出願とは、Ｓｈｒａｉｍらによる、“Ｏｎｌｉｎｅ Ｆｒａｕｄ Ｓｏｌｕｔｉｏｎ”と題された、２００４年５月２日出願の米国特許出願第１０／７０９，３９８号；Ｓｈｒａｉｍらによる、“Ｏｎｌｉｎｅ Ｆｒａｕｄ Ｓｏｌｕｔｉｏｎ”と題された２００４年１０月４日出願の米国特許仮出願第６０／６１５，９７３号；Ｓｈｕｌｌによる、“Ｍｅｔｈｏｄｓ ａｎｄ Ｓｙｓｔｅｍｓ ｆｏｒ Ｐｒｅｖｅｎｔｉｎｇ Ｏｎｌｉｎｅ Ｆｒａｕｄ”と題された、２００４年９月１７日出願の米国特許仮出願第６０／６１０，７１６号；Ｓｈｕｌｌらによる、“Ｃｕｓｔｏｍｅｒ－Ｂａｓｅｄ Ｄｅｔｅｃｔｉｏｎ ｏｆ Ｏｎｌｉｎｅ Ｆｒａｕｄ”と題された、２００４年９月１７日出願の米国特許仮出願第６０／６１０，７１５号；Ｓｈｒａｉｍらによる、“Ｏｎｌｉｎｅ Ｆｒａｕｄ Ｓｏｌｕｔｉｏｎ”と題された、２００４年１１月２３日出願の米国特許出願第１０／９９６，９９１号；Ｓｈｒａｉｍらによる、“Ｅｎｈａｎｃｅｄ Ｒｅｓｐｏｎｓｅｓ ｔｏ Ｏｎｌｉｎｅ Ｆｒａｕｄ”と題された、２００４年１１月２３日出願の米国特許出願第１０／９９６，５６７号；Ｓｈｒａｉｍらによる、“Ｃｕｓｔｏｍｅｒ－Ｂａｓｅｄ Ｄｅｔｅｃｔｉｏｎ ｏｆ Ｏｎｌｉｎｅ Ｆｒａｕｄ”と題された、２００４年１１月２３日出願の米国特許出願第１０／９９６，９９０号；Ｓｈｒａｉｍらによる、“Ｅａｒｌｙ Ｄｅｔｅｃｔｉｏｎ ａｎｄ Ｍｏｎｉｔｏｒｉｎｇ ｏｆ Ｏｎｌｉｎｅ Ｆｒａｕｄ”と題された、２００４年１１月２３日出願の米国特許出願第１０／９９６，５６６号；Ｓｈｒａｉｍらによる、“Ｅｎｈａｎｃｅｄ Ｒｅｓｐｏｎｓｅｓ ｔｏ Ｏｎｌｉｎｅ Ｆｒａｕｄ”と題された、２００４年１１月２３日出願の米国特許出願第１０／９９６，６４６号；Ｓｈｒａｉｍらによる、“Ｇｅｎｅｒａｔｉｎｇ Ｐｈｉｓｈ Ｍｅｓｓａｇｅｓ”と題された、２００４年１１月２３日出願の米国特許出願第１０／９９６，５６８号；Ｓｈｒａｉｍらによる、“Ｍｅｔｈｏｄｓ ａｎｄ Ｓｙｓｔｅｍｓ ｆｏｒ Ａｎａｌｙｚｉｎｇ Ｄａｔａ Ｒｅｌａｔｅｄ ｔｏ Ｐｏｓｓｉｂｌｅ Ｏｎｌｉｎｅ Ｆｒａｕｄ”と題された、２００４年１１月２３日出願の米国特許出願第１０／９９７，６２６号；Ｓｈｕｌｌらによる、“Ｄｉｓｔｒｉｂｕｔｉｏｎ ｏｆ Ｔｒｕｓｔ Ｄａｔａ”と題された、２００５年３月２日出願の米国特許仮出願第６０／６５８，１２４号；Ｓｈｕｌｌらによる、“Ｔｒｕｓｔ Ｅｖａｌｕａｔｉｏｎ Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄｓ”と題された、２００５年３月２日出願の米国特許仮出願第６０／６５８，０８７号；およびＳｈｕｌｌらによる、“Ｉｍｐｌｅｍｅｎｔｉｎ

ｇ　Ｔｒｕｓｔ　Ｐｏｌｉｃｉｅｓ”と題された、２００５年３月２日出願の米国特許仮出願第６０／６５８，２８１号、である。

【背景技術】

【０００３】

（発明の背景）

“フィッシング”技術およびその他違法のオンライン活動を含むがこれらに限定されない、オンライン不正行為の問題は、インターネット・ユーザおよびユーザと取引を行いたい者にとっての共通の問題となっている。近年、特にインターネット・サービス・プロバイダ（“ＩＳＰ：Ｉｎｔｅｒｎｅｔ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ”）などの多数のオンライン会社が、このような実施を追跡することおよび／またはそれに対処することを試み始めた。前掲の関連出願は、このような活動を検出、防止するため、および他の方法でそれに対処するための、いくつかのシステムおよび方法について説明している。

【０００４】

しかし従来では、通常、各会社が独自のシステムおよび／または方法を使用してオンライン不正行為に対処しようとしてきた。それにも関わらずセキュリティ脅威の数および種類－ウイルス、スパイウェア、スパム、フィッシングなど－がインターネット内およびその他のネットワーク化環境内で増大するにつれ、ＩＳＰなどの間で、不正行為、セキュリティおよびその他運用上の適切な情報を交換および共有することへの関心が高まっている。

【０００５】

近年、アンチ・フィッシング・ワーキング・グループおよびデジタル・フィッシュ・ネットなど、関係者がデータを提出、取得および共有できるクリアリング・ハウスをつくろうとする複数の試みを含む、不正行為の集団的な検出および／またはそれに対する対応を可能にするための提案がいくつか提供されてきた。しかしこれらのグループは、いくつかの理由で限られた成功しか収めていない。

【０００６】

例えば、これらのグループが取得および作成するデータは、誰でも任意のフォーマットで提出でき、正規化されず、標準もしくは定義に従っておらず、一律に処理または格納されず、いかなる制御も受けず、業界または専門家による評価も受けない。言い換えれば、本来の目的に役に立つのに十分な水準または制御を達成していない。さらに、このようなデータは、例えばＩＳＰ、銀行、オークション・サービスなどの最大手企業から信頼も重視もされていない。その結果、これら企業は有意義な形で参加しないか、または全く参加しない。さらに、これら企業は、その運用および業務から生成される大量の不正行為データおよびセキュリティ・ソース・データを提供しない。

【０００７】

さらに、これらのモデルの“オープンな”性質は、誰でも提供でき、ａ）わずかな料金を支払えば誰でも処理データを受信できるか、またはｂ）データは多くの場合、入力データの主要なソースと競合する、１つの特定の製品を後押しするために使用されることを意味する。その結果、大部分の生データを有する企業、すなわちＩＳＰ、銀行などは、自らが不正行為検出データの主要ソースになる一方、他の企業、特にほとんど貢献しない小企業が、共有データの主要な、または不均衡な、さらに最大のプレーヤーから見ると不当で思いがけない大きな利益を得ると考えるため、データを提出したがらない。

【発明の開示】

【課題を解決するための手段】

【０００８】

本発明の実施形態は、改良された不正行為検出および／または防止のシステムならびに方法を提供する。一実施形態によれば、改良された不正行為監視を実現する方法は、不正オンライン活動に関する直接情報を第１エンティティから受信することを含むとよい。直接情報は解析されるとよく、不正オンライン活動に関する一組の正規化データが作成されるとよい。直接情報の解析は、不正オンライン活動に関する一組の派生情報を生成するこ

とを含むとよい。不正オンライン活動に関する一組の派生情報の生成は、直接情報、および他の不正オンライン活動に関する以前保存された情報に基づくとよい。こういった保存データは、直接情報および派生情報を含むとよい。一組の正規化データは、複数のエンティティにより読み取り可能な形式であるとよく、直接情報および派生情報を含むとよい。一組の正規化データは格納されるとよい。

【０００９】

本方法は、複数のエンティティのうちの第２エンティティから、格納された正規化データにアクセスするためのリクエストを受信することをさらに含むとよい。格納された正規化データへの第２エンティティによるアクセスは、制御されるとよい。例えば、格納された正規化データへの第２エンティティによるアクセスを制御することは、第１エンティティと第２エンティティとの間の取り決めに基づくとよい。許可されていれば、格納された正規化データの少なくとも一部が、第２エンティティに提供されるとよい。

【００１０】

一実施形態によれば、第１エンティティからの直接情報の受信は、アプリケーション・プログラム・インターフェイス（ＡＰＩ：Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｒａｍ　Ｉｎｔｅｒｆａｃｅ）を介して直接情報を受信することを含むとよい。それに加えて、またはその代わりに、格納された正規化データにアクセスするためのリクエストの受信は、ＡＰＩを介してリクエストを受信することを含むとよい。場合によっては、格納された正規化データは、第１エンティティにより保持されていてもよい。このような場合、ＡＰＩは、第１エンティティの格納された正規化データを第２エンティティがリクエストするための機能を提供するとよい。それに加えて、またはその代わりに、格納された正規化データは、セキュリティ・サービスにより保持されてもよい。このような場合、ＡＰＩは、直接情報をセキュリティ・サービスに提供するための機能を第１エンティティに、セキュリティ・サービスの格納された正規化データをリクエストするための機能を第２エンティティに提供するとよい。

【００１１】

場合によっては、ＡＰＩは、直接情報の受信、直接情報の解析、一組の正規化データの作成、格納された正規化データへの複数のデータ属性を介したアクセスを提供するとよい。それに加えて、またはその代わりに、データ属性は、第１エンティティもしくは第２エンティティのいずれかに固有のエンティティ固有属性、ならびに／または第１エンティティおよび第２エンティティにより規定された許可に基づき第１エンティティと第２エンティティとの間で共有可能な、共有属性を含むとよい。ＡＰＩは、データ属性を定義するスキーマをさらに含むとよい。スキーマは、例えば、拡張可能なマーク付け言語（ＸＭＬ：ｅＸｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）スキーマを含むとよい。スキーマは場合によって、データ属性にタグ付けされたメタデータをさらに含んでもよい。このような場合メタデータは、タグ付けされているデータ属性を追跡できる。

【００１２】

さらに別の実施形態によれば、機械可読媒体上に、一組の命令が格納されているとよく、これらの命令はプロセッサにより実行されると、プロセッサに、第１エンティティから不正オンライン活動に関する直接情報を受信することで改良された不正行為監視を実現させる。直接情報は解析されるとよく、不正オンライン活動に関する一組の正規化データが作成されるとよい。直接情報の解析は、不正オンライン活動に関する一組の派生情報を生成することを含むとよい。不正オンライン活動に関する一組の派生情報の生成は、直接情報、および他の不正オンライン活動に関する以前保存された情報に基づくとよい。こういった保存情報は、直接情報および派生情報を含むとよい。一組の正規化データは、複数のエンティティにより読み取り可能な形式であるとよく、直接情報および派生情報を含むとよい。一組の正規化データは格納されるとよい。

【００１３】

さらに別の実施形態によれば、改良された不正行為監視を実現するシステムは、通信ネットワーク、および通信ネットワークに通信可能に繋がれた第１クライアントを含むとよ

い。第１クライアントは、不正オンライン活動に関する直接情報を提供するようになっているとよい。さらにシステムは、通信ネットワークに通信可能に繋がれたサーバを含むとよい。サーバは、不正オンライン活動に関する直接情報を第１クライアントから受信し、直接情報を解析し、不正オンライン活動に関連し、複数のクライアントにより読み取り可能な形式である一組の正規化データを作成し、一組の正規化データを格納するようになっているとよい。

【００１４】

さらにサーバは、不正オンライン活動に関する一組の派生情報を生成するようになっているとよい。例えばサーバは、直接情報、および他の不正オンライン活動に関する以前保存された情報に基づき、不正オンライン活動に関する一組の派生情報を生成するようになっているとよい。こういった保存情報は、直接情報および派生情報を含むとよい。サーバにより作成される一組の正規化データは、直接情報および派生情報を含むとよい。

【００１５】

さらにシステムは、第２クライアントを含むとよい。このような場合、サーバはさらに、格納された正規化データへアクセスするためのリクエストを第２クライアントから受信し、格納された正規化データへの第２クライアントによるアクセスを制御するようになっているとよい。例えばサーバは、第１クライアントと第２クライアントとの間の取り決めに基づき、格納された正規化データへの第２クライアントによるアクセスを制御するようになっていてもよい。許可されていれば、サーバは、格納された正規化データの少なくとも一部を第２クライアントへ提供するとよい。

【００１６】

一実施形態によれば、サーバは、第１クライアントからアプリケーション・プログラム・インターフェイス（ＡＰＩ）を介して直接情報を受信するようになっているとよい。それに加えて、またはその代わりに、サーバはＡＰＩを介して、格納された正規化データにアクセスするためのリクエストを受信するとよい。ＡＰＩは、直接情報の受信、直接情報の解析、一組の正規化データの作成、格納された正規化データへの複数のデータ属性を介したアクセスを実現するとよい。データ属性は、第１クライアントもしくは第２クライアントのいずれかに固有のエンティティ固有属性、ならびに／または第１クライアントおよび第２クライアントにより規定された許可に基づき第１クライアントと第２クライアントとの間で共有可能な、共有属性を含むとよい。

【００１７】

さらに別の実施形態によれば、改良された不正行為監視を実現するシステムは、通信ネットワーク、および通信ネットワークに通信可能に繋がれた第１クライアントを含むとよい。第１クライアントは、不正オンライン活動に関する直接情報を生成し、直接情報を解析し、不正オンライン活動に関連し、複数のクライアントにより読み取り可能な形式である一組の正規化データを作成し、一組の正規化データを格納するようになっているとよい。システムは、通信ネットワークに通信可能につながれた第２クライアントを含むとよい。第２クライアントは、格納された格納された正規化データへのアクセスをリクエストするようになっているとよい。サーバは、通信ネットワークに通信可能に接続可能であり、格納された正規化データにアクセスするためのリクエストを第２から受信し、第２クライアントによる格納された正規化データへのアクセスを制御するようになっているとよい。サーバは、第１クライアントと第２クライアントとの間の取り決めに基づき、第２クライアントによる格納された正規化データへのアクセスを制御するようになっているとよい。許可されていれば、第１クライアントは、格納された正規化データの少なくとも一部を第２クライアントへ提供するとよい。

【００１８】

一実施形態によれば、サーバは、アプリケーション・プログラム・インターフェイス（ＡＰＩ）を介してリクエストを受信することにより、格納された正規化データにアクセスするためのリクエストを第２クライアントから受信するようになっているとよい。ＡＰＩは、格納された正規化データへの複数のデータ属性を介したアクセスを実現するとよい。

データ属性は、第１クライアントもしくは第２クライアントのいずれかに固有のクライアント固有属性、ならびに／または第１クライアントおよび第２クライアントにより規定された許可に基づき第１クライアントと第２クライアントとの間で共有可能な、共有属性を含むとよい。

【発明を実施するための最良の形態】

【００１９】

本発明を十分に理解できるよう、以下の説明では、多数の具体的な詳細が説明のために記載される。しかし、本発明はこれらの具体的な詳細事項の一部を伴わずに実践されてもよいということが、当業者にはすぐに分かるであろう。他の場合には、よく知られた構造およびデバイスがブロック図の形式で示される。

【００２０】

本発明の種々の実施形態は、改良された不正行為検出および／または防止のシステムならびに方法を提供する。一組の実施形態は、例えば、企業（オンライン会社、銀行、ＩＳＰなど）が不正行為のフィード（一例の名前を挙げると、これら会社の顧客に宛てられた第三者からの電子メール・メッセージのフィード）をセキュリティ・プロバイダに容易に提供できるようにし、さらに、そういった容易さを実現するシステムおよび方法を提供する。一部の実施形態では、フィード（メッセージなど）が解析されて正規化された直接データおよび／または派生データが作成され、このデータは当該企業が利用できるようになるとよい（おそらく有料で）。直接データおよび派生データへのアクセスを定義および制御することで、セキュリティ・プロバイダは、当該企業が企業間で、どことデータを交換するか、どのデータを交換するか、ならびにどのような商業上の条件およびその他の条件の下で当該データを交換するかについて、二者間の取り決めまたはその他の取り決めについて交渉できるようにする。

【００２１】

したがって、本発明の一部の実施形態は、ＩＳＰ（およびその他）が、プライベート・ネットワーク・ピアリング（ｐｒｉｖａｔｅ　ｎｅｔｗｏｒｋ　ｐｅｅｒｉｎｇ）によく似た形の不正行為検出データの交換に関する二者間の具体的なルールを設定できるようにするモデルを提供する。一組の実施形態において、セキュリティ・プロバイダは、容易かつ経済的にデータ交換できるように、主要ネットワークの“ミートミー（ｍｅｅｔ－ｍｅ）”センターにおいて検出システム（いくつかの例として、関連出願で説明されているものなど）を提供してもよい。

【００２２】

種々の実施形態に従い、オンライン不正行為、特に“フィッシング”動作に対抗する、システム、方法およびソフトウェアが提供される。“成りすまし”詐欺として知られる例示的なフィッシング動作は、“成りすまし”電子メール・メッセージを使用して、疑いを持たない顧客が、違法ウェブ・サイトにアクセスして信頼できる関連会社（例えば銀行、オンライン小売業者など）が運用していると思われるサーバに個人情報を提供するよう仕向けるが、このとき実際には、顧客の個人情報にアクセスするために信頼できる関連会社に成りすましている別のパーティによって、このサーバは運用されている。本願明細書で使用される“個人情報”という用語は、当然のことながら、個人を特定するために使用される可能性がある情報、および／または通常は比較的信頼できるエンティティのみに当該の個人により明かされる情報全てを含む。単なる一例として、個人情報は、金融機関の口座番号、クレジット・カードの番号、有効期限および／または暗証番号（当該技術分野では、“カード確認番号”、“カード確認値”、“カード確認コード”または“ＣＶＶ”と呼ばれることもある）、および／またはその他の金融情報；ユーザＩＤ、パスワード、母親の旧姓および／またはその他セキュリティ情報；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／またはその他識別情報が含まれ得るが、これらに限定はされない。

【００２３】

本発明の特定の実施形態は、このような成りすまし電子メール・メッセージを引き付け

、メッセージを解析し、そのメッセージが不正行為に関与している（さらに／または成りすましメッセージを含んでいる）可能性を見積もり、特定されたあらゆる不正行為に応答する、システム、方法および／またはソフトウェアを特徴とする。図１Ａは、これらの実施形態の一部に従ったオンライン不正行為への対処に使用できる、例示的なシステム１００の機能要素を図示しており、特定の実施形態がどのように動作するのかを全体的に概観できる。（種々の実施形態については以下でさらに詳しく論じる）。なお、図１Ａにより表される機能アーキテクチャ、および各機能要素に関して説明される手順は、説明のみを目的として提供されており、本発明の実施形態は必ずしも個々の機能または構造的アーキテクチャに限定されず；本願明細書で論じられる種々の手順は、任意の適切な構成で実行されればよい。

【００２４】

多くの場合、図１Ａのシステム１００は、不正行為防止サービス、セキュリティ・サービスなど（本願明細書では“不正行為防止プロバイダ”と呼ばれる）により、１件または複数件の顧客向けに運用されるよとよい。多くの場合顧客は、模倣、偽造、および／もしくは成りすましされる危険のある製品、ブランドならびに／またはウェブ・サイトを有するエンティティであり、例えばオンライン承認、金融機関、会社などとなる。なお、他の場合では、不正行為防止プロバイダは、例えば、顧客のセキュリティ部門、情報サービス部門など、顧客の従業員および／または顧客と提携しているエンティティ、および／または顧客に合併されたエンティティであってもよい。

【００２５】

本発明の一部の実施形態によれば、システム１００は、様々なデータ・ソース１０５を含むこと（および／またはそれにアクセス）ができる。説明を容易にするために、データ・ソース１０５はシステム１００の一部として描かれているが、多くの場合データ・ソース１０５は、第三者によって独立して保持されること、および／またはシステム１００によりアクセスされてもよいことが、本願明細書の開示に基づき、当業者には分かるであろう。場合によっては、例えばシステム１００がさらに容易にアクセスできるように、データ・ソース１０５の一部がローカルにミラーおよび／またはコピー（必要に応じて）されてもよい。

【００２６】

データ・ソース１０５は、起こり得るオンライン不正行為についてのデータが取得される可能性のある任意のソースを含むとよく、１つまたは複数のチャット・ルーム１０５ａ、ニュースグループ・フィード１０５ｂ、ドメイン登録ファイル１０５ｃ、および／または電子メール・フィード１０５ｄが含まれるが、これらに限定はされない。システム１００は、任意のデータ・ソース１０５から取得した情報を、オンライン不正行為のインスタンスの検出、ならびに／または、本願明細書で論じる不正行為防止方法の能率および／もしくは効果の向上のために使用するとよい。場合によってシステム１００（および／またはその構成要素）は、適切な情報を発見するために、おそらく定期的に（例えば、１０分に１回、１日１回、週１回など）、種々のデータ・ソース１０５を“クロール”する（例えば、自動的にアクセスし、さらに／またはそこから情報をダウンロードする）よう構成されるとよい。

【００２７】

単なる例として、新たなスパミング／成りすましスキームについて論じるため、ならびに収穫された電子メール・アドレスのリストを交換するために一般に使用されているニュースグループがいくつかある。さらに、このようなスキームを追跡する反不正ニュースグループもある。システム１００は、新たな成りすまし詐欺、収穫されたアドレスの新たなリスト、収穫されたアドレスの新たなソースなどについての情報を発見するために、あらゆる適切なニュースグループ（単数または複数）１０５ｂをクロールするよう構成されるとよい。場合によっては、システム１００は、こういったクロール中に、指定のキーワード（例えば“フィッシュ（ｐｈｉｓｈ）”、“成りすまし”など）を検索するよう構成されてもよい。他の場合では、ニュースグループ内のＵＲＬがスキャンされてＵＲＬがダウ

ンロード（またはコピー）され、例えば以下で詳しく説明するように、さらなる解析を受けてもよい。さらに、上述のように、監視が可能な１つまたは複数の反不正グループがあってもよい。このような反不正ニュースグループは、発見された新たな詐欺を記載すること、および／またはそういった詐欺に関するＵＲＬを提供することが多い。そのため、関連情報を発見するためにこのような反不正グループが、例えば上述の方法で監視／クロールされ、続いてその情報がさらなる解析を受けるとよい。その他あらゆるデータ・ソース（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）が同じようにクロールおよび／または検索されてもよい。

【００２８】

別の例として、オンライン・チャット・ルーム（インターネット・リレー・チャット（“ＩＲＣ：Ｉｎｔｅｒｎｅｔ　Ｒｅｌａｙ　Ｃｈａｔ”）・チャネル、ヤフー（Ｙａｈｏｏ）、アメリカ・オンライン（Ａｍｉｒｉｃａ　Ｏｎｌｉｎｅ）などの種々のＩＳＰにより保守／ホストされているチャット・ルームなど、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）が、関連情報について監視（および／またはこのようなチャット・ルームからのログがクロール）されてもよい。場合によっては、自動化プロセス（当該技術分野では“ボット”として知られている）がこの目的で使用されてもよい。なお、他の場合では、人間の参加者がこういったチャット・ルームを自ら監視してもよい。当業者であれば、このようなチャット・ルームでは、アクセス権を維持するために参加が必要なことが多いということが分かるであろう。したがって、場合によっては、投稿者であると思われるように、ボットまたは人間の参加者がこういったチャット・ルームにエントリを投稿してもよい。

【００２９】

さらに、ドメイン登録ゾーン・ファイル１０５ｃ（および／またはＡＲＩＮなどのインターネット・レジストリなど、ドメインおよび／またはネットワーク情報のその他のソース）がデータ・ソースとして使用されてもよい。当業者には分かるとおり、ゾーン・ファイルは新たなドメイン登録を反映するように定期的に（例えば、１時間に１回または毎日）更新される。これらのファイルが、新たなドメイン登録を探すために定期的にクロール／スキャンされるとよい。特定の実施形態では、ゾーン・ファイル１０５ｃの顧客の名前および／またはドメインに類似した登録がスキャンされてもよい。単なる一例として、システム１００は、異なるトップ・レベル・ドメイン（“ＴＬＤ：ｔｏｐ　ｌｅｖｅｌ　ｄｏｍａｉｎ”）またはグローバル・トップ・レベル・ドメイン（“ｇＴＬＤ：ｇｌｏｂａｌ　ｔｏｐ　ｌｅｖｅｌ　ｄｏｍａｉｎ”）を有する、類似したドメイン登録、ならびに／または類似した綴りのドメインを探すように構成されてもよい。そのため、顧客が＜ａｃｍｅｐｒｏｄｕｃｔｓ．ｃｏｍ＞ドメインを使用している場合、＜ａｃｍｅｐｒｏｄｕｃｔｓ．ｂｉｚ＞、＜ａｃｍｅｐｒｏｄｕｃｔｓ．ｃｏ．ｕｋ＞、および／または＜ａｃｍｅｐｒｏｄｕｃｔ．ｃｏｍ＞という登録は、成りすましサイトのホストの可能性があるものとして重要と思われ、このようなドメインのドメイン登録は、その登録が対応するドメインをさらに解析するために、ダウンロードおよび／または記録されるとよい。一部の実施形態では、怪しいドメインが発見されると、当該ドメインは監視リストに置かれるとよい。監視リスト上のドメインは、そのドメインが“有効”になったかどうか（例えば、そのドメインに関連付けられたアクセス可能なウェブ・ページがあるかどうか）を判断するために、以下でさらに詳しく説明されるように定期的に監視されるとよい。

【００３０】

１つまたは複数の電子メール・フィード１０５ｄは、システム１００にさらなるデータ・ソースを提供してもよい。上述のとおり、電子メール・フィードは、スパム・メッセージなど電子メール・メッセージの任意のソースであればよい。（実際には、一部の実施形態に従い、単一の着信電子メール・メッセージが電子メール・フィードと見なされてもよい。）場合によっては、例として以下でさらに詳しく説明されるように、本発明の実施形態によっておとり電子メール・アドレスが“シード”されても、または仕掛けられてもよく、さらに／またはこれらの仕掛けられたアドレスが、電子メールのソース（すなわち電

子メール・フィード）を提供してもよい。したがってシステム１００は、図１Ｂに関して詳しく説明されるアドレス・プランタ１７０を含むとよい。

【００３１】

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を含むとよい。アドレス・ジェネレータ１７５は、ユーザ・インターフェイス１８０および／または１つまたは複数のデータベース１８５（このそれぞれは、リレーショナル・データベースおよび／またはその他任意の適切なストレージ・メカニズムを含むとよい）と通信しているとよい。このようなデータ・ストアの１つは、ユーザＩＤ情報１８５ａのデータベースを含むとよい。ユーザＩＤ情報１８５ａは、本発明の実施形態に従った、ユーザＩＤの生成に使用できる名前、数字および／またはその他識別子のリストを含むとよい。場合によっては、ユーザＩＤ情報１８５ａは分類されてもよい（例えば、名、姓、数字またはその他の文字などの修飾子に）。別のデータ・ストアはドメイン情報１８０を含むとよい。ドメイン情報１８０のデータベースは、アドレスに利用可能であるドメインのリストを含むとよい。多くの場合、これらのドメインは、アドレス・プランタ１７０のオペレータにより所有／管理されているドメインとなる。しかし、他の場合には、ドメインが商用および／または消費者ＩＳＰなど他のものにより管理されることも考えられる。

【００３２】

アドレス・ジェネレータ１７５は、インターネット上（または他の場所）の適切な位置に仕掛けられるとよい電子メール・アドレスを生成する（個別および／またはバッチで）よう構成されるとよいアドレス生成エンジンを含む。単なる一例として、アドレス・ジェネレータ１７５は、ユーザＩＤデータ・ストア１８５ａからユーザＩＤ情報の１つまたは複数の要素を選択し（さらに／または複数の当該要素を結合し）、それらの要素にドメイン・データ・ストア１８５ｂから選択されたドメインを追加し、それによって電子メール・アドレスを作成するよう構成されるとよい。これらの構成要素を結合する手順は任意に決定できる。単なる一例として、一部の実施形態では、アドレス・ジェネレータ１７５は、特定のドメイン名を優先してそれらのドメインに比較的多くのアドレスが生成されるようにするよう構成されてもよい。その他の実施形態では、１つまたは複数のアドレス構成要素を無作為に選択することがプロセスに含まれることも考えられる。

【００３３】

アドレス・プランタ１７０の一部の実施形態は、仕掛け動作の追跡に使用できる追跡データベース１９０を含み、追跡データベース１９０は、特定のアドレスが仕掛けられる場所（例えばウェブ・サイトなど）、仕掛けた日付／時間、ならびにその他任意の、仕掛けに関する適切な詳細を含むがこれらに限定はされない。単なる一例として、所定のアドレスを用いてメーリング・リストに登録することによりアドレスが仕掛けられると、メーリング・リスト（おそらくウェブ・サイト、リストの維持管理者の電子メール・アドレスなども）が、追跡データベースに記録されるとよい。場合によっては、この情報の追跡は自動化されてもよい（例えば、アドレス・プランタ１７０のユーザ・インターフェイス１８０がウェブ・ブラウザおよび／または電子メール・クライアントを含み、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仕掛けるために使用される場合、仕掛け情報に関する情報はアドレス・プランタ１７０によって自動的に登録されてもよい）。あるいは、ユーザが、手動で（例えば自身のウェブ・ブラウザ、電子メール・クライアントなどを使用して）アドレスを仕掛けてもよく、そのため、専用入力ウィンドウ、ウェブ・ブラウザなどによって追跡データベースに適切な情報を追加してもよい。

【００３４】

したがって、ある一組の実施形態では、電子メール・アドレスの生成、指定位置への電子メール・アドレスの仕掛け（アドレス・プランタ１７０により生成されたかどうかに関わらず）、および／または仕掛け動作についての情報追跡に、アドレス・プランタ１７０が使用されてもよい。特定の実施形態では、アドレス・プランタ１７０は、１つまたは複数のアプリケーション・プログラミング・インターフェイス（“ＡＰＩ”）１９５も含むとよく、これは、図１のシステム１００（またはその他任意の適切なシステム）の他の構

成要素が、プログラムでアドレス・プランタと対話できるようにするとよい。単なる一例として、一部の実施形態においてＡＰＩ１９５は、仕掛け動作を実行するためにアドレス・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連動できるようにするとよい。（その他の実施形態では、上述のように、こういった機能がアドレス・プランタ１７０自体に含まれてもよい）。

【００３５】

一部の実施形態におけるＡＰＩ１９５の特定の用途は、他のシステム構成要素（具体的にはイベント・マネージャ１３５など）がアドレス仕掛け動作（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／または更新できるようにすることである。（場合によっては、プログラムでのアドレス・プランタ１７０へのアクセスは不要なこともある－システム１００の必要な構成要素が、単にデータ・ストア１８５の１つまたは複数に必要に応じてアクセス－ＳＱＬなどを介する－してもよい。）単なる一例として、電子メール・アドレスがシステム１００により解析される（例えば以下で詳しく説明されるように）場合、システム１００は、アドレス・プランタ１７０および／またはデータ・ストア１８５のうちの１つまたは複数に問い合せて、電子メール・メッセージがアドレス・プランタ１７０により仕掛けられたアドレス宛てになっているかどうかを判断するとよい。そうであれば、アドレス・プランタ１７０（または、イベント・マネージャ１３５など、システム１００の他の何らかの構成要素）は、フィッシング・メッセージを招く見込みのある場所として仕掛け場所を記録し、希望に応じて追加のアドレスをこのような場所に仕掛けられるようにするとよい。このようにして、システム１００は、仕掛け動作の効率を高めるべくフィードバック・ループを実装できる。（なお、このフィードバック・プロセスは、フィッシング・メッセージ、一般的なスパム・メッセージ、商標の悪用を明示するメッセージなどを含むがこれらに限定はされない、あらゆる所望の種類の“未承諾”メッセージに関して実装できる。）

その他の電子メール・フィードについては、本願明細書の他の場所で説明されており、それらは、スパマー／フィッシャー（ｐｈｉｓｈｅｒ）から直接受信されたメッセージ；ユーザ、ＩＳＰおよび／またはその他任意のソースから転送された電子メール（おそらく、電子メールがスパムおよび／またはフィッシュではないかという疑念に基づく）；メーリング・リストから転送された電子メール（反不正メーリング・リストを含むが、これに限定はされない）などを含むとよい（ただしこれらに限定はされない）。電子メール・メッセージ（スパム・メッセージの可能性がある）がシステム１００により受信されると、それがフィッシング／成りすましスキームの一部であるかどうかを判断するために、そのメッセージが解析されるとよい。これらデータ・フィードのいずれかから受信された情報の解析については、以下でさらに詳しく説明されており、これには、ウェブ・サイト（多くの場合、データ・ソース１０５から受信／ダウンロードされたＵＲＬまたはその他の情報により参照される）がフィッシングおよび／または成りすまし詐欺に関与しそうかどうかを評価することが含まれることが多い。

【００３６】

システムに着信してくるあらゆる電子メール・メッセージは、本発明の種々の方法によって解析されるとよい。当業者には分かるように、インターネット上には膨大な量の未承諾電子メールのトラフィックがあり、これらメッセージの多くが、オンライン不正行為という文脈において重要と思われる。単なる一例として、本願明細書でさらに詳しく説明される、フィッシング詐欺の一環として、一部の電子メール・メッセージが送信されることも考えられる。他のメッセージは、海賊版ソフトウェア、偽造のデザイナー・アイテム（腕時計、ハンドバッグなどを含むが、これらに限定はされない）などの闇および／または灰色市場の商品に顧客を誘う。さらに他のメッセージは、合法的な商品の宣伝であることもあるが、不適切な商標の使用および／または侵害、意図的な安値での商品販売など、違法かまたは他の形で禁止されている（例えば契約によって）行為を含むこともある。本発明の種々の実施形態は、以下で詳述するように、１つまたは複数のこれらの行為の探索、特定、および／またはそれに対する応答を行うよう構成されるとよい。（特定の実施形態

は、同様の行為のために、電子メール・フィード以外にデータ・ソース－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－に対するアクセス、監視、クロールなどを行うよう構成されてもよいことにも留意されたい）。単なる一例として、システム１００は、１つまたは複数のデータ・ソースの言葉ＲＯＬＥＸをスキャンするよう、さらに／またはＲＯＬＥＸの腕時計のあらゆる不適切な宣伝を特定するよう構成されてもよい。

【００３７】

普通の電子メール・アドレスは多数の未承諾電子メール・メッセージを受信すると考えられること、ならびにシステム１００は下記のように、そういったメッセージを受信および／または解析するよう構成されているとよいということが、当業者にはさらに分かるであろう。着信メッセージは多くの方法で受信されると思われる。単なる一例として、一部のメッセージは、メッセージを促す行動が何もとられていという点において、“無作為に”受信されると思われる。あるいは、１人または複数のユーザが、このようなメッセージをシステムに転送することも考えられる。単なる一例として、ＩＳＰが全ての未承諾メッセージを、下記のようにシステム１００により監視されるとよい特定のアドレスに転送するようユーザに指示することも考えられるし、または、ユーザの着信メッセージのコピーをそのようなアドレスに自動転送することも考えられる。特定の実施形態において、ＩＳＰは、そのユーザに送信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ているあらゆるＵＲＬなど、こういった疑わしいメッセージの一部）を、定期的にシステム１００（および／またはその任意の適切な構成要素）へ転送することも考えられる。場合によっては、このプロセスを容易にするよう設計されたフィルタリング・システムをＩＳＰが有することも考えられるし、さらに／または、システム１００の特定の機能がＩＳＰのシステム内に実装（および／または複製）されることも考えられる。

【００３８】

上述のように、システム１００はさらに、おとり電子メール・アドレス（および／または他のおとり情報）を、例えばスパマー／フィッシャーにより収穫されるように、データ・ソースの一部に仕掛けるかまたは“シード”するとよい。一般に、これらのおとり電子メール・アドレスの目的は、電子メールの収穫者に魅力的な標的を提供することであり、おとり電子メール・アドレスは通常（ただし必ずではない）、フィッシャーを引き付けるために特別に生成されるため、通常の電子メールの通信には使用されない。

【００３９】

その結果、図１Ａに戻り、システム１００は“ハニー・ポット”１１０をさらに含むとよい。ハニー・ポット１１０は、各データ・ソース１０５から情報を受信し、さらに／または必要に応じてさらなる解析用にその情報を相互に関連付けるために使用されるとよい。ハニー・ポット１１０は、本発明の種々の実施形態に従って、様々な方法でこういった情報を受信でき、ハニー・ポット１１０が情報を受信する方法は任意に決定できる。

【００４０】

単なる一例として、ハニー・ポット１００は、上述のようにデータ・ソースの実際のクローリング／監視を行うために使用されてもよいが、そうでなくてもよい。（場合によっては、１つまたは複数の他のコンピュータ／プログラムが実際のクローリング／監視動作の実行に使用され、さらに／またはこのような動作を通して取得されたあらゆる関連情報をハニー・ポット１１０へ送信してもよい。例えば、ゾーン・ファイルを監視し、新たなドメイン登録、無効になったドメイン登録および／または他の形で変更されたドメイン登録の全てを解析用にハニー・ポット１１０へ送信するよう、プロセスが構成されることも考えられる。あるいは、ゾーン・ファイルがハニー・ポット１１０への入力として送られともよく、さらに／またはハニー・ポット１１０が変更されたあらゆるドメイン登録を探すために使用されてもよい。）さらにハニー・ポット１１０は、電子メール・メッセージ（別の受信者から転送されることも考えられる）の受信、および／または１つまたは複数のおとり電子メール・アドレスの着信電子メールの監視を行うよう構成されてもよい。特

定の実施形態では、ハニー・ポット１１０が１つまたは複数の電子メール・アドレス（おとりアドレスであるとよい）のメール・サーバとなるようシステム１００が構成され、当該アドレス宛ての全メールが直接ハニー・ポット１１０へ送信されるようにしてもよい。そのため、ハニー・ポット１１０は、デバイスおよび／またはソフトウェアを含むとよく、これは、おとり電子メール・アドレス宛ての電子メール・メッセージを受信するよう機能するもの（例えばＳＭＴＰサーバなど）、および／または電子メール・メッセージを取り出すよう機能するもの（例えばＰＯＰ３および／またはＩＭＡＰクライアントなど）であるとよい。当該技術分野では、このようなデバイスおよびソフトウェアはよく知られており、本願明細書で詳しく論じる必要はない。種々の実施形態に従い、ハニー・ポット１１０は、ＳＭＴＰ、ＭＩＭＥ、ＨＴＭＬ、ＲＴＦ、ＳＭＳおよび／または同様のものなどを含む、種々の有名なメッセージ・フォーマットのいずれか（または全て）を受信するよう構成されるとよい。さらにハニー・ポット１１０は、１つまたは複数のデータベース（および／またはその他のデータ構造）を含んでもよく、これは、電子メール・メッセージおよびその他のデータ（例えばゾーン・ファイルなど）、ならびにクローリング／監視動作から取得された情報を保持／分類するために使用されるとよい。

【００４１】

一部の態様では、受信データ（受信電子メール・メッセージを含むがこれに限定はされない）の何らかの仮の分類および／またはフィルタリングを行うようハニー・ポット１１０が構成されることも考えられる。例えば、特定の実施形態では、ハニー・ポット１１０は受信データの“ブラックリスト上の”ワードまたはフレーズを検索するよう構成されてもよい。（“ブラックリスト”の概念は、以下でさらに詳しく説明される）。ハニー・ポット１１０は、このようなブラックリスト上の用語を含むデータ／メッセージを、優先的な処理などを目的として分離すること、および／またはこれらの基準もしくは他の基準に基づくデータ／メッセージのフィルタを行うとよい。

【００４２】

さらにハニー・ポット１１０は、顧客ポリシー１１５に従って動作するよう構成されてもよい。例示的な顧客ポリシーは、例えば特定のキーワードを検索するためなどに特定の種類および／またはフォーマットの電子メールを見張るようハニー・ポットに指示することも考えられ、これは顧客別のカスタマイズを可能にする。さらにハニー・ポット１１０は、例えば顧客のウェブ・サイトの侵害（ｃｏｍｐｒｏｍｉｓｅ）の監視など、他の状況に関する監視を含む、拡張された監視オプション１２０を利用してもよい。任意選択で、ハニー・ポット１１０は、メッセージを受信すると電子メール・メッセージをデータ・ファイルに変換してもよい。

【００４３】

一部の実施形態では、ハニー・ポット１１０は、１つまたは複数の相関エンジン（ｃｏｒｒｅｌａｔｉｏｎ　ｅｎｇｉｎｅ）１２５と通信しており、この相関エンジン１２５は、ハニー・ポット１１０により受信された電子メール・メッセージ（および／または、クローリング／監視動作から受信された情報などの他の情報／データ）のさらに詳しい解析を実行できる。（なお、本願明細書でのハニー・ポット１１０、相関エンジン１２５などの様々な構成要素への機能割り当ては無原則なものであり、一部の実施形態に従って、特定の構成要素が他の構成要素に割り当てられた機能を具現化してもよい。）

定期的に、および／またはハニー・ポット１１０により着信メッセージ／情報が受信／取り出しされるにつれ、ハニー・ポット１１０は、受信／取り出しされた電子メール・メッセージ（および／または対応するデータ・ファイル）を利用可能な相関エンジン１２５へ解析用に送信する。あるいは、ハニー・ポット１１０から定期的にメッセージ／データ・ファイルを取り出すよう各相関エンジン１２５が構成されてもよい（例えばスケジュールされたＦＴＰプロセスなどを使用）。例えば特定の実装では、ハニー・ポット１１０が、上述のように電子メール・メッセージおよび／またはその他のデータ（分類／フィルタリング済みでも、そうでなくてもよい）を格納し、各相関エンジンが、データおよび／またはメッセージを定期的に、および／または状況に応じて取り出してもよい。例えば、相

関エンジン１２５が、利用可能な処理能力を有する（例えば、キュー内のあらゆるデータ／メッセージの処理を終了した）ときに次の１００通のメッセージ、データ・ファイルなどを処理用にハニー・ポット１１０からダウンロードすることが考えられる。特定の実施形態に従い、種々の相関エンジン（例えば１２５ａ、１２５ｂ、１２５ｃ、１２５ｄ）が、特定の種類のデータ（例えばドメイン登録、電子メールなど）を処理するよう特別に構成されてもよい。その他の実施形態では、全ての相関エンジン１２５があらゆる利用可能なデータを処理するよう構成されてもよく、さらに／または複数の相関エンジン（例えば１２５ａ、１２５ｂ、１２５ｃ、１２５ｄ）が実装されて並列処理のより高い能率が生かされてもよい。

【００４４】

相関エンジン（単数または複数）１２５は、データ（単なる一例として電子メール・メッセージなど）を解析し、ハニー・ポット１１０により受信されたメッセージのいずれかがフィッシュ・メッセージであるかどうか、および／または個人情報を収集しようとする不正な試みの証明となりそうであるかどうかを判断するとよい。この解析の実行手順については以下で詳しく説明する。

【００４５】

相関エンジン１２５は、イベント・マネージャ１３５と通信しているとよく、さらにイベント・マネージャ１３５は監視センター１３０と通信しているとよい。（あるいは、相関エンジン１２５は監視センター１３０と直接通信していてもよい。）特定の実施形態では、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ってもよく、これは監視センター１３０の技術者によりアクセス可能であるとよい。相関エンジン１２５が、特定の着信電子メール・メッセージについて不正な活動を行いそうなものであると判断するか、またはクローリング／監視動作を通して取得された情報が不正な活動を示す可能性があると判断すると、相関エンジン１２５は、イベント・マネージャ１３５にその電子メール・メッセージについてイベント作成の必要があることを信号で伝える。特定の実施形態では、相関エンジン１２５および／またはイベント・マネージャ１３５は、当該技術分野でよく知られているシンプル・ネットワーク管理（“ＳＮＭＰ：Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ”）プロトコルを使用して通信するよう構成されるとよく、相関エンジンの信号はＳＮＭＰ“トラップ”を含み、解析されたメッセージ（単数または複数）および／またはデータが、さらなる調査が必要な、起こり得る不正イベントを示したことを知らせるとよい。この信号（ＳＮＭＰトラップなど）に応答して、イベント・マネージャ１３５がイベント（ＳＮＭＰイベントを含んでもよく、または独自仕様のフォーマットであってもよい）を作成するとよい。

【００４６】

イベントが作成されると、イベント・マネージャ１３５は、メッセージ／情報、および／またはメッセージ／情報に含まれ、さらに／もしくはそれに関連付けられた、任意のＵＲＬの情報収集動作（調査）１４０を開始するとよい。以下で詳しく説明するように、調査は、このＵＲＬに関連付けられたドメインおよび／またはＩＰアドレスについての情報を収集すること、ならびにそのＵＲＬにより参照されているリソース（例えばウェブ・ページなど）をホストするサーバ（単数または複数）に問い合わせることを含むとよい。（本願明細書で使用される“サーバ”という用語は、文脈によって示されるとおり、ＩＰベースのサービスの提供、または個人情報が交換されることもあるオンライン取引を実施できるあらゆるコンピュータ・システムについて使用されること、および特に、個人情報を要求するウェブ・ページを提供することなどにより個人情報の不正な収集に関与する可能性のあるコンピュータ・システムについて使用されることがある。そのため、このようなサーバの最も一般的な例は、ハイパーテキスト転送プロトコル（“ＨＴＴＰ：ｈｙｐｅｒ　ｔｅｘｔ　ｔｒａｎｓｆｅｒ　ｐｒｏｔｏｃｏｌ”）および／または幾つかの関連サービスのいずれかを使用して動作するウェブ・サーバであるが、場合によっては、サーバは、データベース・サービスなど他のサービスを提供することもある）。特定の実施形態では、単一の電子メール・メッセージ（または情報ファイル）が複数のＵＲＬを含む場合、各

ＵＲＬに別々のイベントが作成されてもよい；他の場合では、単一のイベントが、特定のメッセージ内のＵＲＬ全てを対象としてもよい。メッセージおよび／または調査によって、イベントが特定の顧客に関係することが示されると、そのイベントが当該の顧客に関連付けられるとよい。

【００４７】

さらに、イベント・マネージャは、このイベントについて自動レポート１４５を準備し（さらに／またはレポーティング・モジュール（図示せず）などの別のプロセスにレポートを生成させ）、このレポートが、監視センター１３０（または、さらに言えば他の任意の場所）のさらなる技術者により解析されるとよい；レポートは、調査および／または調査により得られた任意の情報の、概要を含むとよい。一部の実施形態では、このプロセスは完全に自動化されて、人間による解析が必要ないようにしてもよい。必要に応じて（さらにおそらくは顧客ポリシー１１５による指示に従い）、イベント・マネージャ１３５は顧客通知１５０を自動的に作成し、そのイベントに影響を受けた顧客に通知するとよい。顧客通知１５０は、レポート１４５からの情報の一部（または全部）を含むとよい。あるいは、顧客通知１５０は単に顧客にイベントを知らせ（例えば、電子メール、電話、文書などによって）、顧客がレポートのコピーにアクセス（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介して）できるようにしてもよい。顧客はさらに、その顧客に影響を及ぼすイベント（例えば、イベントが、顧客の商標、製品、会社の識別情報などを使用した不正行為を伴う場合）を表示する専用ウェブ・サイトなどのポータルを使用して、興味のあるイベントを見てもよい。

【００４８】

調査１４０により、ＵＲＬにより参照されるサーバが個人情報を収集しようとする不正な試みに関与していることが明らかになると、技術者は禁止応答１５５（本願明細書では“技術応答”とも呼ばれる）を開始するとよい。（あるいは、技術者による介入なしに自動的に応答を開始するようイベント・マネージャ１３５が構成されてもよい）。状況および実施形態に応じて種々の応答が適切となり得る。例えば、場合によってはサーバが侵害される（すなわち“ハッキング”される）可能性もあり、その場合、サーバのオペレータの制御下にないアプリケーションの実行および／またはサービスの提供をサーバが行っているということが、当業者には分かるであろう。（この文脈で使用される“オペレータ”という用語は、サーバを所有、保守する存在、および／または他の形でサーバに関与する存在を意味する。）調査１４０により、サーバのオペレータは単なる無意識の被害者であって不正スキームの関係者でなく、サーバが侵害されているらしいことが明らかになれば、適切な応答は単に、サーバが侵害されていることをサーバのオペレータに通知すること、さらにおそらく、侵害を許したあらゆる脆弱性について修正方法を説明することを含むとよい。

【００４９】

その他の場合では、他の応答の方が適切なこともある。このような応答は概して、以下でさらに詳しく説明するように、事実上、管理１６０または技術１６５のいずれかに分類できる。場合によっては、システム１００は、希釈エンジン（ｄｉｌｕｔｉｏｎ ｅｎｇｉｎｅ）（図示せず）を含んでもよく、これは以下でさらに詳しく説明するように、技術応答を引き受けるために使用できる。一部の実施形態において希釈エンジンは、コンピュータ上で実行されるソフトウェア・アプリケーションであり、本発明の方法に従い特にフィッシング詐欺への応答を作成するよう、さらに／またはそのフォーマットを整えるよう構成されてもよい。希釈エンジンは、相関エンジン１２５、イベント・マネージャ１３５などと同じコンピュータにあっても（さらに／またはそこに組み込まれても）よく、さらに／またはこれら構成要素のいずれかと通信しているとよい別のコンピュータにあってもよい。

【００５０】

上述のように、一部の実施形態においてシステム１００は、どの仕掛け場所／技術がスパムの発生に比較的効果が高いかを容易に判断できるようにするために、フィードバック

・プロセスを取り入れるとよい。単なる一例として、システム１００は上述のように、仕掛けられたアドレスに関する情報を追跡するメカニズムを提供するとよいアドレス・プランタ１７０を含むとよい。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（および特に、イベントをもたらすメッセージ）を解析し、そのメッセージが仕掛け動作に起因するかどうかを判断するよう構成されているとよい。例えば、システム１００により仕掛けられた１つまたは複数のアドレス（単数または複数）に対応するアドレスがあるとすればそれがどれであるのかを判断するために、メッセージのアドレスが評価されるとよい。メッセージが１つまたは複数の仕掛けられたアドレスに対応すると判断されると、仕掛けの状況を判断するために仕掛けられたアドレスのデータベースが調べられ、システム１００がこの情報を技術者に表示することも考えられる。このようにすれば、技術者は、有益な場所に追加のアドレスを仕掛けることを選択できる。あるいは、システム１００は、アドレス・プランタ１７０に自動フィードバックを提供するよう構成されてもよく、アドレス・プランタ１７０もまた、追加のアドレスをそういった場所に自動的に仕掛けるよう構成されてもよい。

【００５１】

したがって、本発明の種々の実施形態に従い、不正行為の存在を判断するために、起こり得るオンライン不正行為についての一組のデータ（電子メール・メッセージ、ドメイン登録、ＵＲＬおよび／またはオンライン不正行為についてのその他関連データであればよい）が受信および解析されるとよく、不正行為の一例はフィッシング・スキームでもあり得る。本願明細書で使用される“フィッシング”という用語は、例えば、自分の個人情報の提供、違法製品の購入など、ユーザが別の状況ではとらないような行動をユーザに取らせる不正スキームを意味し、これは多くの場合、ユーザに合法的に見えることもあるウェブ・サーバなどのサーバにアクセスするよう要求する未承諾電子メール・メッセージの送信（または、例えば電話、ウェブ・ページ、ＳＭＳメッセージなど、他の何らかの通信）によるものである。そうであれば、あらゆる関連の電子メール・メッセージ、ＵＲＬ、ウェブ・サイトなどが調査され、さらに／または応答行動がとられるとよい。さらなる特徴およびその他の実施形態について、以下でさらに詳しく論じる。

【００５２】

上記のように、本発明の特定の実施形態は、オンライン不正行為に対処するシステムを提供する。図２のシステム２００は、ある一組の実施形態の具体例と見なされるとよい。システム２００は一般的に、ネットワーク２０５を含み得るネットワーク化環境において実行される。多くの場合、ネットワーク２０５はインターネットであるが、一部の実施形態においてネットワーク２０５は、他の何らかのパブリックおよび／またはプライベート・ネットワークであってもよい。一般的に、コンピュータ間のデータ通信をサポートできるネットワークであればどれでも十分である。システム２００は、本願明細書で論じられている手順または方法のいずれかを実行するのに使用できるマスタ・コンピュータ２１０を含む。特に、マスタ・コンピュータ２１０は、種々のデータ・ソースのクロール／監視、おとり電子メール・アドレスのシード、おとり電子メール・アドレスに送信された電子メール・メッセージの収集および／もしくは解析、イベントの作成および／または追跡、ＵＲＬおよび／もしくはサーバの調査、イベントについてのレポートの準備、イベントについての顧客への通知、ならびに／または、例えば通信リンクを介した監視センター２１５との（および、より具体的には、監視センター内の監視コンピュータ２２０との）通信を行うよう構成されるとよい（例えばソフトウェア・アプリケーションによって）。マスタ・コンピュータ２１０は、複数のコンピュータであってもよく、複数のコンピュータのそれぞれは、種々の実施形態に従い特定のプロセスを実行するよう構成されるとよい。単なる一例として、１台のコンピュータが、ハニー・ポットに関して上述した機能を実行するよう構成され、別のコンピュータが、相関エンジンに関連付けられたソフトウェアを実行するよう構成されて、例えば電子メール・メッセージ／データ・ファイルの解析を実行してもよく；第３のコンピュータが、イベント・マネージャとしての機能を果たすよう構成されて、例えば疑わしい不正行為の出来事の調査および／もしくはそれへの対応などを

してもよく、さらに／または、第４のコンピュータが、希釈エンジンの機能を果たすよう構成されて、例えば技術応答を生成および／もしくは送信してもよく、単なる一例としてこの技術応答は、以下でさらに詳しく説明するように、１つまたは複数のＨＴＴＰリクエストを含んでもよい。同じく、監視コンピュータ２２０も、適切な機能を実行するよう構成されるとよい。

【００５３】

監視センター２１５、監視コンピュータ２２０、および／またはマスタ・コンピュータ２１０は、例えば通信リンクを介して１件または複数件の顧客２２５と通信しているとよく、通信リンクは、電話線、無線接続、広域ネットワーク、ローカル・エリア・ネットワーク、仮想プライベート・ネットワークおよび／または同様のものなど、音声および／またはデータ通信を提供できる任意の媒体を介した接続を含むとよい。上記の通信は、データ通信および／または音声通信（例えば、監視センターの技術者が顧客側の人物と電話通信を行ってもよい）であればよい。顧客（単数または複数）２２５との通信は、イベント・レポートの送信、イベントの通知、および／または不正行為への応答に関する協議を含むとよい。

【００５４】

マスタ・コンピュータ２１０は、上述のデータ・ソース１０５を含むがこれに限定はされない複数のデータ・ソースを含む（および／またはそれと通信する）とよい。その他のデータ・ソースが同様に使用されてもよい。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を含むとよく、これは、以下で詳しく論じられるように用いられるよう、おとり電子メール・アドレスおよび／もしくは１つまたは複数の架空（または本物）の識別情報に関する個人情報を生成ならびに／または格納するために使用できる。（本願明細書で使用される“データベース”という用語は、従来の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／または同様のものなど、データを格納する任意の手段を含むよう、広く解釈される必要がある。）さらにマスタ・コンピュータ２１０は、調査されるインターネットおよび／または任意のサーバに関する情報の、１つまたは複数のソースと通信していてもよい。このような情報ソースは、ドメインＷＨＯＩＳデータベース２４０、ゾーン・データ・ファイル２４５などを含むとよい。多くの場合、ＷＨＯＩＳデータベースは中央登録機関（例えば、アメリカン・レジストリ・フォー・インターネット・ナンバーズ（“ＡＲＩＮ：Ａｍｅｒｉｃａｎ Ｒｅｇｉｓｔｒｙ ｆｏｒ Ｉｎｔｅｒｎｅｔ Ｎｕｍｂｅｒｓ”）、ネットワーク・ソリューションズ社（Ｎｅｔｗｏｒｋ Ｓｏｌｕｔｉｏｎｓ，Ｉｎｃ．など）により保守されており、マスタ・コンピュータ２１０は、これら機関に問合せを行うよう構成されてもよく；あるいは、マスタ・コンピュータ２１０は、非公開で保守されているデータベースなどの他のソースから、当該情報を取得するよう構成されてもよいということが、当業者には分かるであろう。マスタ・コンピュータ２１０（および／またはその他任意の適切なシステム構成要素）は、これらのリソース、ならびに公開されているドメイン名サーバ（ＤＮＳ：ｄｏｍａｉｎ ｎａｍｅ ｓｅｒｖｅｒ）・データ、ルーティング・データおよび／または同様のものなど、その他のものを使用して、不正行為の実行が疑われるサーバ２５０を調査するとよい。上述のとおりサーバ２５０は、オンライン取引の処理、ウェブ・ページの提供、および／または他の方法での個人情報の収集ができる、任意のコンピュータであればよい。

【００５５】

さらにシステムは、１つまたは複数の応答コンピュータ２５５を含むとよく、応答コンピュータ２５５は、以下でさらに詳しく説明するように、不正行為に対して技術応答を提供するために使用されるとよい。特定の実施形態では、１つまたは複数の応答コンピュータ２５５は、フィッシング詐欺への応答を作成するため、および／またはそのフォーマットを整えるために使用できる希釈エンジンを含んでもよく、さらに／または希釈エンジンと通信していてもよい。（なお、応答コンピュータ２５５の機能は、マスタ・コンピュータ２１０、監視コンピュータ２２０などにより実行されてもよい。）特定の実施形態では

、複数のコンピュータ（例えば２５５ａ－ｃ）を使用して、分散応答（ｄｉｓｔｒｉｂｕｔｅｄ　ｒｅｓｐｏｎｓｅ）を提供してもよい。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／または監視コンピュータ２２０は、ハードウェア、ファームウェアおよび／または必要なタスクを実行するためのソフトウェア命令を有する専用コンピュータであってもよい。あるいは、これらのコンピュータ２１０、２２０、２５５は、例えばマイクロソフト社（Ｍｉｃｒｏｓｏｆｔ　Ｃｏｒｐ．）のウィンドウズ（登録商標）（Ｗｉｎｄｏｗｓ（登録商標））および／またはアップル社（Ａｐｐｌｅ　Ｃｏｒｐ．）のマッキントッシュ（Ｍａｃｉｎｔｏｓｈ）・オペレーティング・システム）の任意の適切な特色を実行するパーソナル・コンピュータおよび／もしくはラップトップ・コンピュータ、ならびに／または様々な商用のＵＮＩＸ（登録商標）またはＵＮＩＸ（登録商標）ライクのオペレーティング・システムのいずれかを実行しているワークステーション・コンピュータなど、オペレーティング・システムを有する汎用コンピュータであってもよい。特定の実施形態では、コンピュータ２１０、２２０、２５５は、例えばＧＮＵ／Ｌｉｎｕｘ、ＦｒｅｅＢＳＤなど、様々なフリーのオペレーティング・システムのいずれかを実行してもよい。

【００５６】

さらに、コンピュータ２１０、２２０、２５５は、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）サーバおよび同様のものなどを含む、種々のサーバ・アプリケーションを実行するとよい。これらのコンピュータは、他のコンピュータからのリクエスト、および／またはそれとの対話に応答して、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プログラムまたはスクリプトを実行できる、１つまたは複数の汎用コンピュータであればよい。このようなアプリケーションは、単なる例として、Ｃ、Ｃ＋＋、Ｊａｖａ（登録商標）、ＣＯＢＯＬ、または、Ｐｅｒｌ、ＰｙｔｈｏｎもしくはＴＣＬなどの任意のスクリプト言語、またはそれらの任意の組み合わせなど、任意のプログラミング言語で書かれた１つまたは複数のスクリプトまたはプログラムとして実装されるとよい。さらにコンピュータ２１０、２２０、２５５は、ローカルおよび／または他のコンピュータで実行されているデータベース・クライアントからのリクエストを処理できる、オラクル（Ｏｒａｃｌｅ）、マイクロソフト、サイベース（Ｓｙｂａｓｅ）、ＩＢＭおよび同様のものから市販されているパッケージを含むがこれらに限定されない、データベース・サーバ・ソフトウェアを含んでもよい。単なる一例として、マスタ・コンピュータ２１０は、本発明の実施形態に従いタスクを実行するための個別アプリケーション・ソフトウェアを実行するよう構成された、ＧＮＵ／Ｌｉｎｕｘオペレーティング・システムおよびＰｏｓｔｇｒｅＳＱＬデータベース・エンジンを動作させるインテル（Ｉｎｔｅｌ）・プロセッサ・マシンであってもよい。

【００５７】

一部の実施形態では、１つまたは複数のコンピュータ１１０は、調査レポートなどの表示用に、必要に応じて動的にウェブ・ページを作成するとよい。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（例えば監視コンピュータ２２０）との間のインターフェイスとしての機能を果たすとよい。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てもよく、その一方で、別の（例えば監視コンピュータ２２０）デバイスが専用クライアント・アプリケーションを実行してもよい。そのため、サーバ・アプリケーションは、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イスとしての機能を果たすとよい。あるいは、コンピュータの中の特定のものが、“シン・クライアント”または他のコンピュータと通信する端末として構成されてもよい。

【００５８】

システム２００は１つまたは複数のデータ・ストアを含むとよく、このデータ・ストアは、１つまたは複数のハード・ドライブなどを含むとよく、例えばデータベース（２３０、２３５など）を格納するために使用されてもよい。データ・ストアの位置は任意に決定できる：単なる一例として、１つまたは複数のコンピュータの、ローカルのストレージ媒

体上にあっても（さらに／またはコンピュータに常駐しても）よい。あるいは、データ・ストアはこれらデバイスのいずれかまたは全てから、これらのうちの１つまたは複数と通信（例えばネットワーク２０５を介して）している限りは離れていてもよい。一部の実施形態では、データ・ストアは、当業者によく知られているストレージ・エリア・ネットワーク（“ＳＡＮ：ｓｔｏｒａｇｅ－ａｒｅａ　ｎｅｔｗｏｒｋ”）にあってもよい。（同じく、コンピュータ２１０、２２０、２５５による機能を実行するのに必要なあらゆるファイルは、必要に応じて、各コンピュータのローカルのコンピュータ可読ストレージ媒体、および／または各コンピュータから離れたコンピュータ可読ストレージ媒体に格納されるとよい。）

図３は、本願明細書で説明されているように、本発明の方法、ならびに／または、マスタ・コンピュータ、監視コンピュータおよび／もしくは応答コンピュータの機能を実行できる、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である。図３では、種々の構成要素に関する一般化された説明図を提供することのみが意図されており、これらのうちのいずれかが必要に応じて利用されるとよい。コンピュータ・システム３００は、バス３０５を介して電気的に繋がれることが可能な１つまたは複数のプロセッサ３１０；１つまたは複数のストレージ・デバイス３１５など、ハードウェア構成要素を含むとよく、ストレージ・デバイス３１５は、ディスク・ドライブ、光学ストレージ・デバイス、例えばランダム・アクセス・メモリ（“ＲＡＭ：ｒａｎｄｏｍ　ａｃｃｅｓｓ　ｍｅｍｏｒｙ”）　および／または読み出し専用メモリ（“ＲＯＭ：ｒｅａｄ－ｏｎｌｙ　ｍｅｍｏｒｙ”）などの固体ストレージ・デバイスを含んでもよいがこれらに限定はされず、プログラム、フラッシュ・アップデート、および／または、同様のことが可能で（さらに、上述のようにデータ・ストアとして機能可能で）あるとよい。マウス、キーボードおよび／もしくは同様のものを含み得るがこれらに限定されない１つまたは複数の入力デバイス３２０；表示デバイス、プリンタおよび／もしくは同様のものを含み得るがこれらに限定されない１つまたは複数の出力デバイス３２５；ならびに、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／もしくは同様のものを含み得るがこれらに限定されない通信サブシステム３３０も、同じくバス３０５と通信するようになっているとよい。

【００５９】

さらに、コンピュータ・システム３００は、上述のようなアプリケーション・プログラム、および／または本発明の方法を実装するよう設計されたアプリケーション・プログラムなど、オペレーティング・システム３４０および／またはその他のコード３４５を含む、ワーキング・メモリ３３５内に現在は位置して示されているソフトウェア構成要素を含むとよい。特定の実施形態および／または要求に従って、多くの変形物がつくられてもよいことが、当業者には分かるであろう。例えば、カスタマイズされたハードウェアがさらに使用されることも考えられ、さらに／または特定の構成要素がハードウェア、ソフトウェア（アプレットなどの高移植性ソフトウェアを含む）、または両方に実装されることが考えられる。

【００６０】

一般的に、図４により示されるように、所定のＩＳＰ（またはその他の会社）４００が、そのソース４０５から不正行為に関するデータを、加えておそらくはセキュリティ・プロバイダから種々のデータ４１０を、受信するとよい。本発明の実施形態に従い、このようなデータを共有すること（および／または、以下でさらに詳しく説明されるように、こういった共有を実行する方法の制御を実施すること）が容易になると思われる。

【００６１】

一例として、図５は、複数の会社５０５がピアリング関係５０４に参加するとよいシステム５００を図示する。場合によっては、セキュリティ・プロバイダ５０９は、プロバイダ５０９と会社５０５との間の対話を可能にするために、アプリケーション・プログラミング・インターフェイス（“ＡＰＩ”）５１０を提供する。さらにシステムは、種々のフィードに関するデータ属性５１５ａの生成、解析および／または提供、ならびにまたは、

種々の会社５０５に固有の情報５１５ｂに対する、権限サービス５１４もしくはその他アクセス制御の提供など、他の拡張サービスを提供してもよい。追加のサービス５２０は、不正行為検出サービス５２０ａ、早期事前警告サービス５２０ｂ、および／または不正行為対応／解決サービス５２０ｃを含むとよい。このようなサービスについては関連出願で詳しく説明されている。

【００６２】

場合によっては、システムは種々のデータ・サービス５２５および／またはソース（一様に数字５２５ａ、５２５ｂ、５２５ｃにより参照される構成要素によって示されている）を利用してもよく、これらの多くについては関連出願で説明されている。

【００６３】

図６により示されているように、システム５００はさらに、プライベート・ピア交換ＡＰＩ６１０（上述のＡＰＩ５１０と同じＡＰＩであってもよい）を実現して、プロバイダと会社５０５との間、ならびに場合によっては１つの会社５０５ａと別の会社５０５ｂとの間のデータ交換を可能にするとよい。このような情報は、次に限定するものでないが、特定の会社５０５ａに固有な場合もある会社固有またはエンティティ固有の配信属性６１５を含むこともあるため、場合によっては他の会社５０５ｂ－ｄと共有されない。このようなエンティティ固有属性の例には、不正行為の種類、通信が検出された元のＵＲＬまたはポート、不正行為の標的エンティティ、データ許可、レポータの識別子、レポータのソース、電子メール・データなどに関する情報が含まれ得るが、これらに限定はされない。さらにデータ属性は、会社またはエンティティの間で、これら会社および／またはプロバイダにより規定される許可におそらく基づき共有可能な共有属性６２０を含んでもよい。このような許可は、１つの会社５０５ａが、別の会社５０５ｂのものであるデータに不正にアクセスするのを防ぐべく、ＡＰＩ６１０により強制されるとよい。共有データ属性６２０の例をいくつか挙げると、ＩＳＰ配信属性、レポータの評判、サイトの状況、不正行為の識別子、ドメイン所有者、ネットワークもしくはＩＳＰのデータ、レポートのタイムスタンプ、確認タイムスタンプなどが含まれるが、これらに限定はされない。なお、場合によって会社５０５ａは、会社固有の配信属性を共有することを選択してもよい。

【００６４】

本発明の実施形態はさらなる追加の特徴を提供することもあり、これには、交渉済みの条件および／またはデータ許可におそらく基づき、任意の二者（またはそれより多い会社）間について、二者間の取り決め（例えばデータ属性の共有）を実現することが含まれるが、これに限定はされない。場合によっては、パーティが、それらがシステムに提供するデータ（フィードなど）の量に比例してシステムから利益を得ることを、システムが可能にしてもよい（例えば、種々のデータ属性へのアクセス制御を通して）。さらに、システムが“匿名の”不正行為検出をサポートして、フィードからの情報が会社に配布される前にセキュリティ・プロバイダによって（および／またはシステムによって）ジェネリック化される（ｇｅｎｅｒｉｃｉｚｅｄ）ようにし、１つの会社（および／またはその顧客）の個人情報は他の会社と共有されないもののその会社のデータ（および／またはその解析）の利点は他者が得られるようにするとよい。

【００６５】

こういった不正行為およびセキュリティ関係の情報を交換する理由には以下が含まれ得るが、これらに限定はされない：

・新型または変形したセキュリティ・イベントまたは脅威を、それが最初に起こったときに起こった場所を問わず発見する。

・あらゆるセキュリティ・イベントまたは脅威の大きさ、継続期間および程度を理解する。

・あらゆるセキュリティ・イベントまたは脅威のライフ・サイクル、系統、適応および時間の経過による変形を理解する。

・脅威プロファイル（履歴、起源、順列、型、分類および見本など）イベント・ログ、セキュリティ・データベース、検出モデルおよび予想力を確立する

・異なるセキュリティ・イベントまたは脅威の間の相関関係、相互関係および相違点を判断する。
・自らのセキュリティ・イベントまたは脅威の体験と対比して、同じ業界または他の業界の他のものを、個別または総合的に理解する。
・セキュリティ脅威およびイベントについての傾向、データ解析、統計およびレポートを作成する。

【００６６】

種々の実施形態は、容易さ、システム、プログラム、アルゴリズム、処理、データ・ストレージ、データ送信、プロセス、データ定義、スキーマ、分類法、プロセス、ワークフロー、動作を提供して、ＩＳＰ、銀行、オークション・サービス・プロバイダ、セキュリティ企業などが、生および／または処理済みのセキュリティ・イベントもしくは脅威のデータ（フィードを含むがこれに限定はされない）を配信できるようにする。その結果システムは、このようなデータを一定の方法で処理し、さらに／またはこのような生および／もしくは処理済みのデータを定義済みであり正規化された定義および標準に従って整理および／もしくは格納し、いずれの会社も、それらがまさに交換したいデータの具体的な種類、量、ボリューム、時間、形式およびフォーマット、ならびにそのデータ交換に適用したい商業、運用、配信に関する条件について、他のあらゆる会社と相互に定義および交渉できるようにすることが可能である。

【００６７】

特定の実施形態では、データが多少の価値を有し、参加者が、データ保全性、フォーマット、定義、配信方法および信頼性に関する一定の基準を順守する限り、参加者がそれぞれの入力データを提出（および／または取り出し）することの許可において、かなり寛大であってもよい。場合によっては、システムは、入力データの出所、所有権、ソース、直接および関連のパーティの識別情報、評判、利用特性および制限にタグを付け、さらに／またはそれを追跡する。続いてシステムが、データを処理すること、および／または提出されたデータに関する追加の派生データを作成すること、加えて、我々が有することもある他のデータもしくは他者から提出された他のデータにデータを相関させて、派生データを作成することも考えられる。加えて、データは、時間がたつにつれて格納されてもよく、さらに／または多次元解析が実行されてもよく、さらに特定のデータ・セット内およびデータ・リポジトリ全体にわたって関係が特定されてもよい。このような解析および関係の特定については、関連出願でさらに詳しく説明されている。

【００６８】

さらに本発明の実施形態は、参加者間における二者間または多者間の商業上の取り決めを容易かつ可能にし、どのデータを他者と交換するかについて、ならびに全ての関連した商業上、技術上、運用上の条件について、交渉可能にすることも考えられる。その結果システムは次に、各パーティに、それらが交換に合意し、アクセスするのに十分な法的権利、商権またはその他の権利を有するデータおよび派生データのみを提供することにより、この取り決めを満たすようにサービスを提供することができる。

【００６９】

したがって、一部の実施形態では、データの提供相手、厳密な提供対称データおよび提供する程度、見返りとして得るもの（金銭、データまたはサービスの交換、またはその他の報酬など）、およびどの運用、技術、地理、法律、規制、ポリシー、商業に関する条件および制限の下におくかを、定義、制御でき、そこから利益を享受し、それを強制（二者間、多者間、個別に、および／または状況に応じて）できるということを知った上で、関連した不正行為およびセキュリティのデータ全てを提出するよう参加者に勧める。

【００７０】

図７は、本発明の一実施形態による、改良された不正行為監視を提供する情報収集プロセスを図示する流れ図である。この例では、プロセスは、不正オンライン活動に関する直接情報を第１エンティティから受信することで始まる（７０５）。上述の通り、直接情報を第１エンティティから受信することは、アプリケーション・プログラム・インターフェ

イス（ＡＰＩ）を介して直接情報を受信することを含むとよい。例示的なＡＰＩおよびこのようなＡＰＩのデータ属性についてのさらなる説明は、以下でさらに論じられる。

【００７１】

受信すると（７０５）、直接情報は解析され（７１０）、不正オンライン活動に関する一組の正規化データが作成されるとよい（７１５）。直接データの解析（７１０）は、不正オンライン活動に関する一組の派生データを生成することを含むとよい。不正オンライン活動に関する一組の派生情報の生成は、直接情報、および他の不正オンライン活動に関する以前保存された情報に基づくとよい。このような保存情報は、直接情報および派生情報を含むとよい。一組の正規化データは、複数のエンティティにより読み取り可能な形式であるとよく、直接情報および派生情報を含むとよい。一組の正規化データは格納されるとよい（７２０）。

【００７２】

図８は、本発明の一実施形態に従った、改良された不正監視に関する情報を提供するプロセスを図示する流れ図である。この例では、複数のエンティティのうちの第２エンティティから、格納された正規化データにアクセスするためのリクエストを受信することでプロセスが始まる（８０５）。上述のとおり、格納された正規化データにアクセスするためのリクエストを受信することは、ＡＰＩを介してリクエストを受信することを含むとよい。第２エンティティによる格納された正規化データへのアクセスは、制御されるとよい（８１０）。例えば、上述のとおり、第２エンティティによる格納された正規化データへのアクセスを制御することは、第１エンティティと第２エンティティとの間の取り決めに基づくとよい。許可されている（８１０）場合、格納された正規化データの少なくとも一部が、第２エンティティに提供されるとよい（８１５）。

【００７３】

一組の実施形態では、システムは、上述のものを含むがそれらに限定はされない１つまたは複数のＡＰＩを特色とするとよい。このＡＰＩは、データの提出方法および／またはシステムからの受信方法を定義する、データに関するＸＭＬスキーマと関連して使用されてもよい。システムはさらに、違法アクセス（例えばハッカーによる）からの情報保護、および１つの参加会社による別の会社のデータへの不正アクセスの防止の両方のために、アクセス制御、認証および／または送信セキュリティ（当該技術分野で知られている種々の暗号化および／または認証スキームを含むがこれらに限定はされない）のための種々の手段を含むとよい。例えば、プライバシーまたはポリシーの理由で参加会社が保護する必要がある、あるレベルの個人データまたは識別データを含む受信データに対応するために、システム内に格納されているデータが任意選択で暗号化されてもよい。

【００７４】

実際には、場合によって、プライバシーに関する法律およびポリシーに応じて、データの一部または全部が参加会社の記憶場所にあってもよい。そのような場合には、システムは例えば交換管理の処理および／または指示を提供して２者（またはそれより多くの会社）間の中間物としての機能を果たすが、データは参加会社から参加会社へ直接送信される、ということも考えられる。（例えば、ＩＳＰまたは銀行などの特定の会社は、セキュリティ保護のために、顧客データの使用についてセキュリティ・プロバイダよりも強い権利を持つことも考えられる。

【００７５】

次の表には、システムにより受信、処理、解析および／または提供されるとよい各種データ属性の例がいくつか記載されている。本願明細書の開示に基づき、他の種類のデータも同じく使用可能であることが、当業者には分かるであろう。

【００７６】

【表１－１】

解析される項目	入力ソース	入力ソース・クリエータ
ドメイン名	ゾーン・ファイルdff(ＥＷＳ)	
	ブランド収穫	検索エンジン
テキスト	ISP	スパム・コレクタ
		ハニー・ポット
		ユーザ提出
	顧客	スパム
		ハニー・ポット
		ユーザ提出
	仕掛け	プランタ
		仕掛けアドレス
		仕掛けツール＋バージョン
URL	ISPフィード	スパム
		ハニー・ポット
		ユーザ提出
	IM解析	
	電子メール解析	
	図形解析	
	ポップアップ解析	
	手動入力	
	オークション・サイト解析	
IPアドレス	ISPフィード	
	IM解析	
	電子メール解析	

【００７７】
【表１－２】

	図形解析	
	ポップアップ解析	
	手動入力	
	ウェブ解析	
	オークション・サイト解析	
電子メール・アドレス	フィード	ISP
		顧客
	電子メール解析	
	ウェブ・ページ解析	
	IM解析	
	図形相関	
	ポップアップ	
	手動入力	
ロゴ	電子メール解析	テキスト解析 ロゴ解析 暗号化(stego)解析
	ウェブ解析	
	ポップアップ解析	
	オークション・サイト解析	
	フィード	
	手動入力	
画像／図形		
登録記録	ドメインWhols	
	ネットワークWhols	
取引		

次の表には、システムにより受信、処理、解析および／または提供された一組のデータ

にタグを付け、さらに／またはそれを追跡するために使用されるとよい、メタデータの種類の例が記載されている。本願明細書の開示に基づき、他の種類のメタデータも同じく使用可能であることが、当業者には分かるであろう。

【００７８】

【表２】

識別子	入力ソースの評判	派生データ
タイムスタンプ	高確率	ドメイン・レジストリ
項目ID	怪しい	登録
ソースID	低確率	ネーム・サーバ（単数，複数）
顧客ID	確認済み	ネットワーク・レジストリ
実行日		アクセス・ネットワーク IPブロック所有者
システムID		
		ドメインWhoIs記録 （whoisスキーマが必要）
		ネットワークWhoIS記録 （whoisスキーマが必要）

次の表には、システムによって受信、処理、解析および／または提供されたデータに関連した各種の違法活動を特定するために使用されるとよいタグの種類の例が記載されている。本願明細書の開示に基づき、他の種類のタグも同じく使用可能であることが、当業者には分かるであろう。

【００７９】

【表３】

権利基準	権限
商標	法律 管轄 国 条約 <New>
著作権	法律 管轄 国 条約 <New>
特許	法律 管轄 国 条約 <New>
判例法上の権利	判例／権利 管轄 国 条約 <New>

本願明細書で説明されたプライベート不正行為ピアリング・モデルは、不正行為およびその他のセキュリティに関するデータの収集、処理、交換に関して説明されたが、同じモデルを、他の業界における他の目的のための異なる種類のデータを交換するために適用することも可能である。

【００８０】

前述の説明では、説明のために特定の順序で方法が説明された。当然のことながら、代

わりの実施形態では、説明とは異なる順序でこの方法が実行されてもよい。さらにこの方法は、追加のステップを含んでもよく、または上述よりも少ないステップを含んでもよい。さらに、当然のことながら、上述の方法はハードウェア構成要素により実行されても、または、一組の機械実行可能な命令に具現化されてもよく、この命令は、この命令でプログラミングされた汎用または専用プロセッサもしくは論理回路などの機械にこの方法を実行させるために使用されるとよい。これらの機械実行可能な命令は、ＣＤ－ＲＯＭもしくは他の種類の光ディスク、フロッピー（登録商標）・ディスケット、ＲＯＭ、ＲＡＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、磁気もしくは光カード、フラッシュ・メモリ、または電子命令を格納するのに適した他の種類の機械可読媒体など、１つまたは複数の機械可読媒体に格納されるとよい。あるいはこの方法は、ハードウェアおよびソフトウェアの組み合わせにより実行されてもよい。

【００８１】

本発明の説明に役立つ現時点において好適な実施形態が本願明細書で詳しく説明されてきたが、当然のことながら、本発明の概念は、別の方法で多様に具現化および採用されてもよく、添付の特許請求の範囲は、先行技術により制限されている場合を除いて、こういった変形を含むように解釈されることが意図されている。

【図面の簡単な説明】

【００８２】

【図１Ａ】図１Ａは、本発明の種々の実施形態に従った、オンライン不正行為に対処するシステムを図示する機能図である。

【図１Ｂ】図１Ｂは、本発明の種々の実施形態に従った、おとり電子メール・アドレスを仕掛けるシステムを図示する機能図である。

【図２】図２は、本発明の種々の実施形態に従った、オンライン不正行為に対処するシステムを示す概略図である。

【図３】図３は、本発明の種々の実施形態に従った、オンライン不正行為に対処するシステムに実装されるとよいコンピュータの一般化された概略図である。

【図４】図４は、セキュリティ・プロバイダとセキュリティ・プロバイダの複数の顧客との間の典型的な関係を図示する。

【図５】図５は、本発明の実施形態に従った、セキュリティ・プロバイダとセキュリティ・プロバイダの複数の顧客との間のピアリング関係を図示する。

【図６】図６は、本発明の一部の実施形態に従った、プライベート・ピアリング・アプリケーション・プログラミング・インターフェイスを図示する。

【図７】図７は、本発明の一実施形態に従った、改良された不正行為監視を実現するために情報を収集するプロセスを図示する流れ図である。

【図８】図８は、本発明の一実施形態に従った、改良された不正行為監視に関する情報を提供するプロセスを図示する流れ図である。

【図１Ａ】

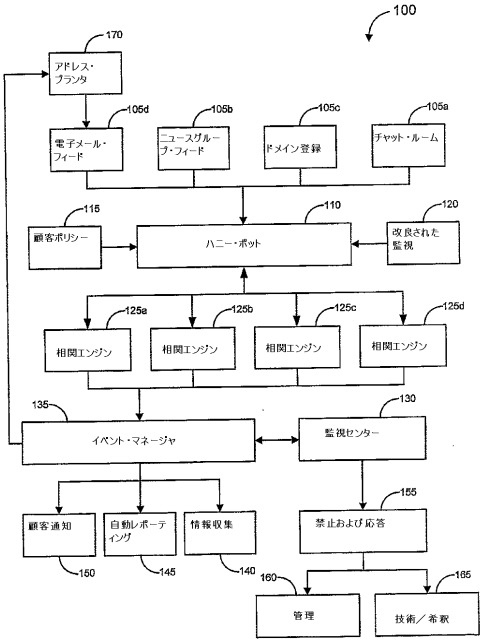


FIG. 1A

【図１Ｂ】

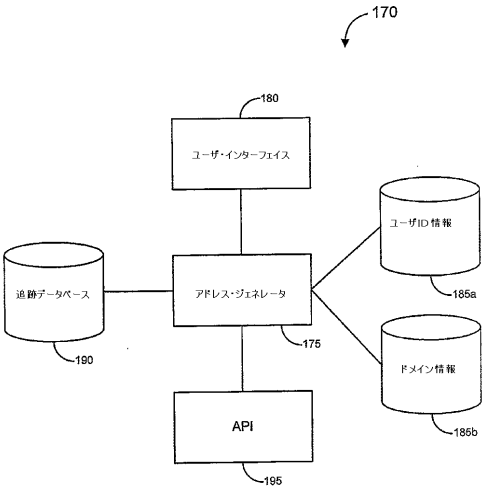


FIG. 1B

【図２】

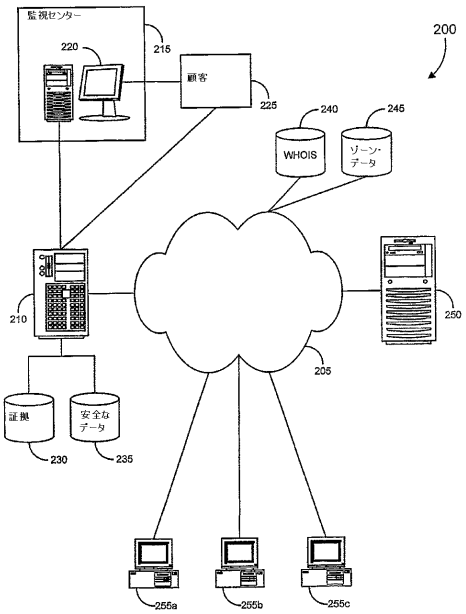


FIG. 2

【図３】

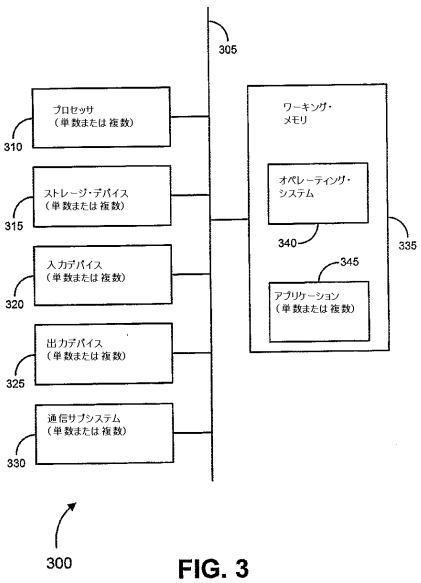


FIG. 3

【図４】

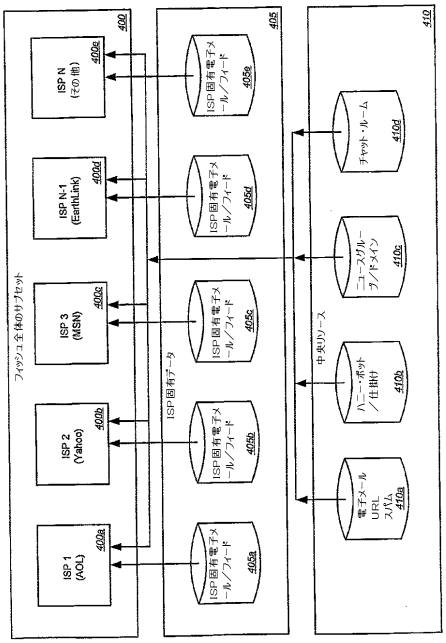


FIG. 4

【図５】

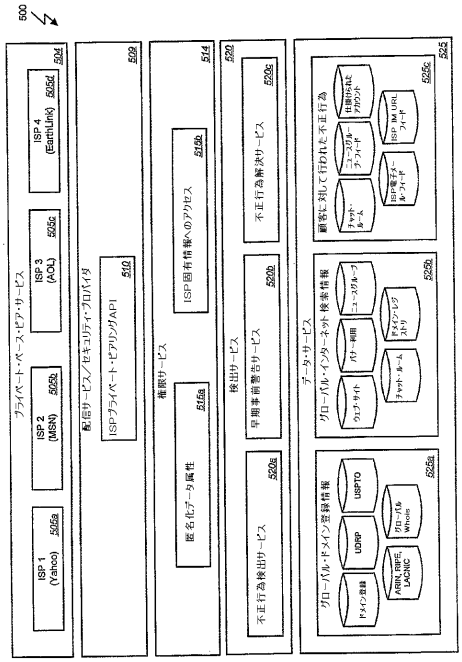


FIG. 5

【図６】

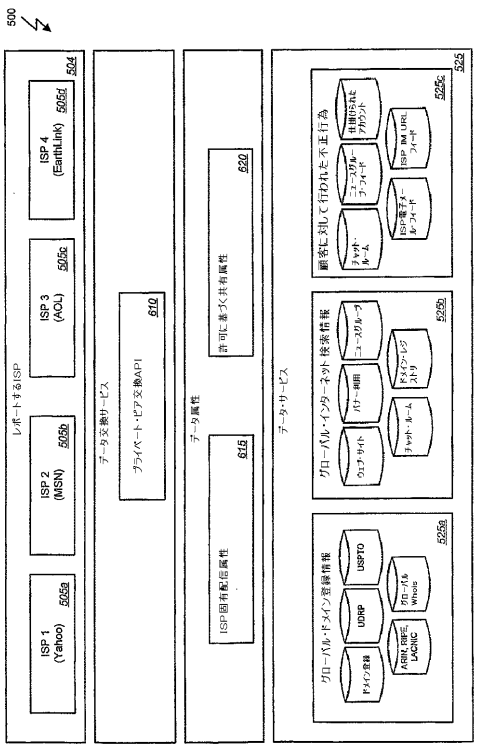


FIG. 6

【図７】

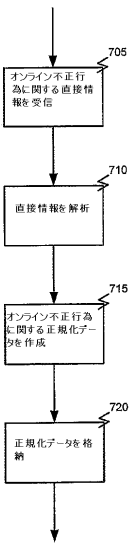


FIG. 7

【図８】

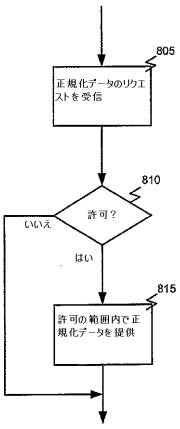


FIG. 8

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,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,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,RS,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,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
(72)発明者 シュライム, 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

Ｆターム(参考) 5B017 AA03 BA06 BA07
5B285 AA01 AA04 AA05 AA06 AA07 BA01 BA07 BA10 CA06 CA32
CA33 CA41 DA02 DA03 DA04 DA09 DA10