

明 細 書

発明の名称：

情報処理装置、情報処理方法、及び情報処理プログラム

技術分野

[0001] 本発明の実施形態は、情報処理装置、情報処理方法、及び情報処理プログラムに関する。

背景技術

[0002] 近年、送信元のメールアドレスなどを偽装した電子メールを特定の相手に送り、添付したファイルやリンク先にアクセスさせることでユーザの端末をウィルスに感染させる等の標的型メール攻撃が増加している。

[0003] 従来では、電子メールの送信元を偽装する、いわゆる「なりすまし」の電子メールに対応するための技術として、SPF (Sender Policy Framework) 認証やDKIM (DomainKeys Identified Mail)、DMARC (Domain-based Message Authentication, Reporting & Conformance) といった送信元ドメインの認証技術が広く利用されている。

[0004] SPF認証では、認証用のサーバに送信元のメールアドレスのドメインと送信元IPアドレスとの組み合わせを適切な電子メールの送信元として予め登録しておき、メールサーバが電子メールを受信した際、当該電子メールの送信元に対応するドメインと送信元IPアドレスを認証用のサーバに問い合わせ、適切な電子メールの送信元であるか否かの認証を実行する。

先行技術文献

特許文献

[0005] 特許文献1：特開2012-78922号公報

発明の概要

発明が解決しようとする課題

[0006] 上述の送信元ドメインの認証技術のような、送信元のドメインとIPアドレスの組み合わせの登録が予め必要なメール認証システムでは、登録してい

る法人や団体は限定的なものとなるため、認証可能な範囲には限界がある。加えて、送信元のドメイン及び送信元ＩＰアドレスのいずれかがメールシステムの入れ替えなどにより変更された場合、認証を整合させるためには送信元のドメイン及び送信元ＩＰアドレスとの組み合わせを改めて登録する必要がある。このため、送信元のドメイン及び送信元ＩＰアドレスの変更に追従できない場合があった。

[0007] 加えて、従来の送信元ドメインの認証技術では、悪意の第三者自身が、送信元のドメインとＩＰアドレスの組み合わせを認証用のサーバに登録した場合、悪意の第三者からの電子メールを受信した場合であっても認証結果が整合してしまうという問題もあった。

[0008] 本発明はこのような事情を考慮してなされたもので、電子メールの適切な送信元を迅速かつ広範囲に収集でき、電子メールのなりすまし等の不正行為を防止することができる情報処理装置、情報処理方法、及び情報処理プログラムを提供することを目的とする。

課題を解決するための手段

[0009] 本発明の実施形態に係る情報処理装置は、複数のメールサーバのそれぞれで受信された電子メールから抽出される、前記電子メールの送信情報を受け付けるデータ受信部と、前記送信情報に基づいて前記電子メールの送信元が適切か否かを判定する送信情報判定部と、前記適切と判定された前記送信元を複数の前記メールサーバのそれぞれに配信するホワイトリスト配信部と、を備えることを特徴とする。

発明の効果

[0010] 本発明の実施形態により、電子メールの適切な送信元を迅速かつ広範囲に収集でき、電子メールのなりすまし等の不正行為を防止することができる情報処理装置、情報処理方法、及び情報処理プログラムが提供される。

図面の簡単な説明

[0011] [図1]第1実施形態に係る情報処理装置が適用される電子メールシステムの構成の一例を示す構成図。

[図2]電子メールから抽出された送信情報の一例を示す説明図。

[図3]電子メールから抽出された送信情報について、送信情報判定部において適切な送信元か否かを判定した結果の一例を示す説明図。

[図4]ホワイトとなる送信元のリストの一例を示す説明図。

[図5]第1実施形態に係る情報処理方法の一例を示すフローチャート。

[図6]第2実施形態に係る情報処理装置が適用される電子メールシステムの構成の一例を示す構成図。

[図7]第2実施形態に係る情報処理方法の一例を示すフローチャート。

発明を実施するための形態

[0012] 以下、本発明の実施形態を添付図面に基づいて説明する。

図1は、第1実施形態に係る情報処理装置10が適用される電子メールシステムの構成の一例を示す構成図である。

[0013] メールサーバ12は、外部メールサーバを介して、外部端末（図示省略）から電子メールを受信して、受信した電子メールを内部端末11に送信するサーバである。メールサーバ12は、例えばインターネットからの接続が制限される内部ネットワークとインターネットと任意に接続可能な外部ネットワークとの境界（DMZ:DeMilitarized Zone）に設けられる。

[0014] 内部端末11は、メールサーバ12から電子メールを受信するクライアント端末である。

[0015] なお、ここでは、メールサーバ12（12a、12b）を2つで構成して、メールサーバ12a及び12bのそれぞれについて電子メールを受信する端末を内部端末11a、11bのそれぞれ1つで構成しているが、さらに複数のメールサーバ12及び内部端末11で構成してもよく、メールサーバ12及び内部端末11の数量、配置は図1に限定されるものは無い。

[0016] メールサーバ12は、電子メール解析部18と、送信情報保存部19と、ホワイトリストデータベース20と、送受信処理部22と、を備えている。

[0017] 電子メール解析部18は、外部メールサーバを介して、外部端末から受信した電子メールから送信情報を抽出して、送信情報に基づいて電子メールの

解析を実行する。送信情報とは、電子メールから抽出されるメール送信に関する各種の情報であり、送信元メールアドレス（エンベロープ From）、メールヘッダ内に記載の送信元 IP アドレス、送信時間、メール件名、メール本文内に記載のリンク先、添付されたファイル名、添付ファイル名及びそのファイル拡張子などである。送信元 IP アドレスは、メールヘッダ内に記載されている IP アドレス（Received From）のうち、インターネットからの接続が制限される内部のネットワークで管理されるメールサーバ 12 の前段にある外部のメールサーバの送信元 IP アドレスにより特定してもよいし、メールサーバ 12 の前段のサーバから送信された接続コマンドの IP アドレスを利用して特定してもよい。

[0018] 電子メール解析部 18 は、抽出した送信情報に基づいて、悪意の第三者により電子メールの送信元が偽装された有害なメールか否かの解析を実行する。具体的には、例えば電子メール解析部 18 は、送信元メールアドレス（エンベロープ From）とメールヘッダ内の送信元アドレスとが一致するか否かを判定して、一致しない場合には送信元の偽装と判定する。また、予め偽装と想定されるメール文章を保存しておき、このメール文章と電子メールの本文とを照合することで送信元の偽装と判定してもよい。

[0019] 送信情報保存部 19 は、電子メール解析部 18 で抽出された送信情報を、電子メールを受信する内部端末 11 のそれぞれを識別する情報（例えば、内部端末 11 の IP アドレス、電子メールアドレスなど）と関連付けて保存する。送信情報は、送信情報保存部 19 に保存されるごとに情報処理装置 10 に送信される。あるいは、送信情報は、定期的（例えば 2 時間ごと）に情報処理装置 10 に送信されてもよい。

[0020] 図 2 は、電子メールから抽出された送信情報の一例を示す説明図である。

図 2 に示すように、送信情報保存部 19 は、送信元メールアドレス、送信元 IP アドレス、送信時間、メール件名、メール本文内に記載のリンク先、添付されたファイルのファイル名などが送信情報として保存される。また、電子メール解析部 18 において実行された、電子メールが偽装か否かの判定

結果を送信情報として付加してもよい。

[0021] ホワイトリストデータベース20は、電子メールの送信元として適切となる（偽装メールのおそれが無い）、送信元メールアドレスのドメインと送信元IPアドレスの組み合わせをリストとして予め保存するデータベースである。ホワイトリストデータベース20は、情報処理装置10から配信された、送信元メールアドレスのドメインと送信元IPアドレスの組み合わせを保存する配信データ保存部21を有している。なお、情報処理装置10から配信されて、配信データ保存部21で保存されるホワイトな送信元（送信元として適切な）に対応するドメインと送信元IPアドレスの詳細については後述する。

[0022] 送受信処理部22は、受信した電子メールについて、内部端末11へのメールの送信制御などを実行する。具体的には、電子メールの送信元メールアドレスのドメイン及び送信元IPアドレスがホワイトリストデータベース20に記載の送信元リストと合致する場合には、適切な送信元と判断して内部端末11に電子メールを送信する。一方、ホワイトリストデータベース20に記載の送信元リストと合致しない場合には、電子メール解析部18における偽装メールか否かの解析結果に基づいて電子メールの送信を制御する。例えば、電子メールが偽装と判定された場合には内部端末11に電子メールを送信せずに、メールサーバ12の内部にメールを隔離する。これにより、電子メールを受信する内部端末11がウィルスに感染するなどのリスクが回避されて、端末の安全性が担保される。

[0023] 無料メールドメインやプロバイダ管轄のドメインなど法人や団体だけではなく個人も利用できるドメインについては、標的型のメールとして利用されるおそれが高いため、ホワイトリストデータベース20で保存されるホワイトな送信元としては除外することが望ましい。なお、プライベートドメインをホワイトリストデータベース20とは別に保存してもよい。

[0024] 第1実施形態に係る情報処理装置10は、複数のメールサーバ12で受信された電子メールから抽出された送信情報を受け付けて、送信情報に基づい

て送信元が適切か否かを判定して、適切と判定された送信元をメールサーバ 12 のそれぞれに配信する装置である。

[0025] 情報処理装置 10 は、複数のメールサーバ 12 から送信される送信情報を取得する。情報処理装置 10 は、複数のメールサーバ 12 から送信情報を直接取得してもよいし、送信情報を収集する別個のサーバを経由して送信情報を取得してもよい。

[0026] なお、情報処理装置 10 は一台の装置から構成されてもよいが、複数の装置から構成されてもよい。情報処理装置 10 が複数の装置から構成される場合には、情報処理装置 10 を構成する装置は異なる部屋又は異なる場所に設置されてもよく、情報処理装置 10 の一部と情報処理装置 10 の残部が遠隔地に配置されてもよい。

[0027] 情報処理装置 10 は、データ受信部 13 と、送信情報判定部 14 と、照合データ保存部 15 と、ホワイトリスト配信部 16 と、を備えている。

[0028] なお、情報処理装置 10 を構成する各ユニットの機能は、所定のプログラムコードを、プロセッサを用いて実行することによって実現しても良く、このようなソフトウェア処理に限らず、例えば、ASIC 等を用いたハードウェア処理で実現してもよいし、ソフトウェア処理とハードウェア処理とを組み合わせ実現してもよい。

[0029] データ受信部 13 は、複数のメールサーバ 12 のそれぞれで受信された電子メールから抽出される、電子メールの送信情報をメールサーバ 12 から受け付ける。

[0030] 照合データ保存部 15 は、電子メールの送信情報のそれぞれについて、内部端末 11 に有害となる悪性情報を予め保存するデータベースである。例えば、悪意のあるファイルのダウンロードや Web サイトへの接続に内部端末 11 を誘導する有害な IP アドレスやリンク先 URL、偽装メールのおそれがある送信元メールアドレスのドメイン、IP アドレス、件名、添付ファイル名、添付ファイル名及びそのファイル拡張子等を保存する。

[0031] 送信情報判定部 14 は、電子メールの送信情報に基づいて電子メールの送

信元が適切か否かを判定する。送信情報判定部 14 は、受け付けた送信情報と、照合データ保存部 15 に保存されている悪性情報とを照合して、受け付けた送信情報が悪性情報に合致しない場合には、当該送信情報における送信元メールアドレスのドメイン及び送信元 IP アドレスを適切な送信元と判定する。一方、受け付けた送信情報が悪性情報に合致する場合には、適切な送信元と判定しない。

[0032] また、送信情報判定部 14 は、複数のメールサーバ 12 から受け付けた送信情報において、送信情報に含まれる送信元メールアドレスのドメイン及び送信元 IP アドレスが一致する場合には、当該送信元メールアドレスのドメイン及び送信元 IP アドレスを適切と判定してもよい。例えば、送信情報を受け付けたメールサーバ 12 に対して基準値（例えば、3 つ以上のメールサーバ 12）を設けておき、基準値を超えるメールサーバ 12 から受信した送信情報において、送信元メールアドレスのドメイン及び送信元 IP アドレスが一致する場合には、当該送信元メールアドレスのドメイン及び送信元 IP アドレスを適切と判定する。また、送信情報判定部 14 は、複数のメールサーバ 12 から受け付けた送信情報において、電子メールの偽装判定の結果が良（偽装されていないとの判定結果が出た送信情報）となり、かつ送信元メールアドレスのドメイン及び送信元 IP アドレスが一致する場合に、当該送信元メールアドレスのドメイン及び送信元 IP アドレスを適切と判定してもよい。

[0033] また、送信情報判定部 14 は、複数のメールサーバ 12 から受け付けた送信情報において、送信情報に含まれる添付ファイル名及びその拡張子が送信情報の間で一致する場合には、不審な電子メールから抽出された送信情報の疑いがあるとして、送信情報に含まれる送信元メールアドレスのドメイン及び送信元 IP アドレスを不適切な送信元と判定してもよい。

[0034] また、照合データ保存部 15 は、送信情報判定部 14 において適切な送信元と判定されなかった送信情報の各種情報を悪性情報として保存してもよい。

- [0035] 図3は、電子メールの送信情報に基づいて電子メールの送信元が適切か否かを判定した結果の一例を示す説明図である。送信情報判定部14は、受け付けた送信情報のそれぞれについて、照合データ保存部15に保存されている悪性情報と照合することで送信元が適切か否かを判定する。
- [0036] 図3に示すように、送信元IPアドレスが「178.50.1.x」に対応する電子メールの送信情報にリンク先として「http://・・・/a.html」が存在して、このリンク先が悪性情報と合致する場合、この送信情報に対応する送信元は不適切と判定する。一方、送信元IPアドレスが「178.60.1.y」に対応する電子メールの送信情報について、送信情報のそれぞれが悪性情報と合致しない場合、送信情報に対応する送信元メールアドレスのドメイン及び送信元IPアドレスを適切な送信元、すなわちホワイトな送信元と判定する。
- [0037] ホワイトリスト保存部17は、適切と判定された送信元を保存する。ホワイトリスト保存部17は、適切と判定された送信元を蓄積していく。また、ホワイトリスト保存部17に保存された送信元は、照合データ保存部15の悪性情報と随時照合されて、送信元が適切か否かの判定結果が更新されてもよい。
- [0038] ホワイトリスト配信部16は、送信情報判定部14において適切と判定された送信元を複数のメールサーバ12のそれぞれに配信する。そして、メールサーバ12のそれぞれは、配信された送信元（メールアドレスのドメイン及び送信元IPアドレス）を配信データ保存部21に保存する。ホワイトリスト配信部16は、適切と判断された送信元が収集されるごとに複数のメールサーバ12のそれぞれに配信してもよいし、ホワイトリスト保存部17に保存された送信元の全てのデータを一定時間ごとに配信してもよい。また、情報処理装置10がメールサーバ12からの配信要求を受け付けて、ホワイトリスト保存部17に保存された送信元の全てのデータを配信してもよい。
- [0039] また、ホワイトリスト配信部16は、ホワイトリスト保存部17に保存された送信元とともに照合データ保存部15に保存されている悪性情報をメールサーバ12のそれぞれに配信してもよい。メールサーバ12の電子メール

解析部 18 は、配信された悪性情報を用いて偽装解析を実施してもよい。

[0040] 図 4 は、ホワイトリストデータベース 20 (20a、20b) で保存されるホワイトリストの一例を示す説明図である。ホワイトリストデータベース 20 には、送信元として適切とされた、送信元メールアドレスのドメインと送信元 IP アドレスの組み合わせが保存される。ホワイトリスト配信部 16 から配信されるごとに、適切な送信元として新たに保存される。

[0041] 続いて、第 1 実施形態に係る情報処理装置 10 の動作について説明する。

図 5 は、第 1 実施形態に係る情報処理方法の一例を示すフローチャートである (適宜、図 1 参照)。

[0042] データ受信部 13 は、複数のメールサーバ 12 のそれぞれで受信された電子メールから抽出される、電子メールの送信情報をメールサーバ 12 から受け付ける (S10)。

[0043] 送信情報判定部 14 は、受け付けた電子メールの送信情報と、照合データ保存部 15 に保存されている悪性情報とを照合して、電子メールの送信元が適切か否かを判定する (S11)。

[0044] そして、受け付けた電子メールの送信情報が悪性情報に合致しない場合には、当該送信情報における送信元メールアドレスのドメイン及び送信元 IP アドレスを適切な送信元と判定する (S12: YES)。一方、受け付けた電子メールの送信情報が悪性情報に合致する場合には、適切な送信元と判定しない (S12: NO)。

[0045] ホワイトリスト配信部 16 は、送信情報判定部 14 において適切と判定された送信元を複数のメールサーバ 12 のそれぞれに配信する (S13)。なお、ホワイトリスト配信部 16 は、ホワイトリスト保存部 17 に保存された送信元の全てのデータを一定時間ごとに配信してもよい。

[0046] このように、第 1 実施形態に係る情報処理装置 10 は、電子メールの適切な送信元を迅速かつ広範囲に収集できる。短期間で電子メールの適切な送信元を広範囲に収集できることで、電子メールのなりすまし等の不正行為を防止することができる。

[0047] メールシステムの入れ替えやドメイン情報変更などにより送信元のメールアドレスのドメインとIPアドレスとの組み合わせが変化する場合、SPF認証などでは、ドメインと送信元IPアドレスの組み合わせを改めて各メールサーバの管理者が登録する必要がある。

[0048] 一方、本実施形態では、複数のメールサーバ12で実際に受信された電子メールの送信情報に基づいてホワイトとなる送信元を収集、配信することで、送信元のメールアドレスのドメインとIPアドレスとの組み合わせが変化する場合であっても、例えばSPF認証のようにドメインと送信元IPアドレスの組み合わせを各メールサーバの管理者が予めDNSサーバに登録する必要は無く、最新の適切な送信元を迅速に使用することができる。すなわち、実際に受信された電子メールの送信情報に基づいてホワイトとなる送信元を更新することで、ドメインや送信元IPアドレスの変更に追従でき、ホワイトとなる送信元リストを常に最新の状態に保持することができる。また、SPF認証とは異なり、悪意の第三者がメールアドレスのドメインと送信元IPアドレスの組み合わせを送信元として登録することはできないため、メールサーバ12において悪意の第三者から受信した電子メールが適切な送信元と判断されることを防止できる。

[0049] (第2実施形態)

図6は、第2実施形態に係る情報処理装置10の構成の一例を示す図である。なお、図6において第1実施形態(図1)と共通の構成又は機能を有する部分は、同一符号で示し、重複する説明を省略する。

[0050] 第2実施形態に係る情報処理装置10では、内部端末11のユーザまたはメールサーバ12の管理者により登録された送信元メールアドレスのドメイン及び送信元IPアドレスについて情報処理装置10で受信して、この登録された送信元メールアドレスのドメイン及び送信元IPアドレスを適切な送信元としてメールサーバ12のそれぞれに配信する。

[0051] 具体的な構成について説明する。

メールサーバ12のホワイトリストデータベース20は、内部端末11の

ユーザまたはメールサーバ12の管理者により登録される、電子メールの送信元として適切となる送信元メールアドレスのドメインと送信元IPアドレスの組み合わせを保存する登録データ保存部23をさらに有している。

[0052] なお、内部端末11のユーザ（またはメールサーバ12の管理者）は、送信元を登録するための登録画面を端末上に表示して、送信元メールアドレスのドメインと送信元IPアドレスの組み合わせからなる送信元を登録する。登録された送信元は、登録データ保存部23に保存される。

[0053] また、ユーザの端末上に表示された登録画面は、すでにホワイトリストデータベース20の登録データ保存部23に登録されている送信元の登録データを表示可能に構成されてもよい。このとき、登録データ保存部23に保存された送信元の登録データを、情報処理装置10から配信されて配信データ保存部21に保存された送信元の配信データと比較照合して、配信データと一致する登録データについては、配信データとして保存されていることをユーザが認識できるように表示されてもよい（例えば、配信データと一致する登録データは識別用のマークを付して表示される）。

[0054] データ受信部13は、ユーザにより登録される、送信元メールアドレスのドメインと送信元IPアドレスの組み合わせからなる送信元をメールサーバ12から受け付ける。なお、メールサーバ12は、送信元を情報処理装置10に送信する際、メールサーバ12のそれぞれを識別するための識別情報を送信元に付与して送信してもよい。これにより、情報処理装置10では、受け付けた送信元がいずれのメールサーバ12から送信されたものか識別することができる。

[0055] また、データ受信部13は、1つの送信元メールアドレスのドメインと複数の送信元IPアドレスとが対応付けてユーザにより登録された組み合わせを受け付けてもよい。例えば、図4のNo. 3に示すように、CIDR (Classless Inter-Domain Routing) 形式を用いて、1つのドメインに特定のアドレス範囲を指定する送信元IPアドレスを対応付けて受け付ける。

[0056] 送信情報判定部14は、受け付けた送信元メールアドレスのドメインと送

送信元IPアドレスの組み合わせに基づいてこの送信元が適切か否かを判定する。具体的には、送信情報判定部14は、受け付けた送信元メールアドレスのドメインと送信元IPアドレスと、照合データ保存部15に保存されている悪性情報とを照合することで、適切な送信元か否かを判定する。

[0057] ホワイトリスト保存部17は、適切と判定された送信元を保存する。なお、送信情報判定部14において、メールサーバ12においてユーザ（または管理者）により登録され、データ受信部13で受け付けた送信元メールアドレスのドメインと送信元IPアドレスについて適切か否かの判定を必ず実行する必要は無く、データ受信部13で受け付けた送信元メールアドレスのドメインと送信元IPアドレスをホワイトリスト保存部17に保存してもよい。

[0058] ホワイトリスト配信部16は、ホワイトリスト保存部17に保存された送信元を、送信元の登録に係るメールサーバ12を含むメールサーバ12のそれぞれに配信する。なお、ホワイトリスト配信部16は、ホワイトリスト保存部17に送信元が保存されるごとに複数のメールサーバ12のそれぞれに配信してもよいし、ホワイトリスト保存部17に保存された送信元の全てのデータを一定時間ごとに配信してもよい。また、情報処理装置10がメールサーバ12からの配信要求を受け付けて、ホワイトリスト保存部17に保存された送信元の全てのデータを配信してもよい。

[0059] 第2実施形態における配信の方法について図6を用いて具体的に説明する。メールサーバ12aにおいて、送信元メールアドレスのドメインと送信元IPアドレスの組み合わせからなる送信元が登録データ保存部23aに登録された場合、この送信元は情報処理装置10に送信される。情報処理装置10の送信情報判定部14は、送信されたドメインと送信元IPアドレスが適切か否かを判定する。ホワイトリスト配信部16は、適切な送信元と判定された場合、この送信元はメールサーバ12a、12bに送信する。メールサーバ12a、12bのそれぞれは、送信された送信元を配信データ保存部21a、21bに保存する。

[0060] 続いて、第2実施形態に係る情報処理装置10の動作について説明する。

図7は、第2実施形態に係る情報処理方法の一例を示すフローチャートである（適宜、図6参照）。

[0061] データ受信部13は、ユーザにより登録される、送信元メールアドレスのドメインと送信元IPアドレスの組み合わせからなる送信元を受け付ける（S20）。

[0062] 送信情報判定部14は、受け付けた送信元メールアドレスのドメインと送信元IPアドレスの組み合わせに基づいてこの送信元が適切か否かを判定する（S21）。

[0063] ホワイトリスト配信部16は、適切と判定された送信元（メールのドメイン及び送信元IPアドレス）を、ユーザによる送信元の登録に係るメールサーバ12を含むメールサーバ12a、12bのそれぞれに配信する（S22：YES、S23）。なお、ホワイトリスト配信部16は、ホワイトリスト保存部17に保存された送信元の全てのデータを一定時間ごとに配信してもよい。一方、適切と判定されなかった場合には、メールサーバ12に配信しない（S22：NO）。

[0064] 第2実施形態に係る情報処理装置10は、ユーザにより登録された送信元について、メールサーバ12に配信することで、ホワイトとなる送信元を複数のメールサーバ間で即時に共有することができ、ホワイトとなる送信元リストを広範囲に収集できる。

[0065] なお、第2実施形態に係る情報処理装置10において、第1実施形態で示した情報処理装置10の構成、すなわち複数のメールサーバ12で実際に受信された電子メールの送信情報に基づいてホワイトとなる送信元を収集、配信する構成を組み合わせてもよい。

[0066] 以上述べた実施形態の情報処理装置によれば、メールサーバのそれぞれから抽出された送信情報に基づいて電子メールの適切な送信元を判定し、送信元を各メールサーバに配信することにより、適切な電子メールの送信元を迅速かつ広範囲に収集でき、SPF認証などに比較してタイムリーにより正確

に送信元を把握することにより、電子メールのなりすまし等の不正行為を防止することができる。

[0067] なお、情報処理装置 10 で実行されるプログラムは、ROM 等の記憶回路に予め組み込んで提供される。もしくは、このプログラムは、インストール可能な形式または実行可能な形式のファイルで CD-ROM、CD-R、メモ리카ード、DVD、フレキシブルディスク等のコンピュータで読み取り可能な記憶媒体に記憶されて提供するようにしてもよい。また、情報処理装置 10 で実行されるプログラムは、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせて提供するようにしてもよい。

[0068] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

符号の説明

[0069] 10…情報処理装置、11…内部端末、12…メールサーバ、13…データ受信部、14…送信情報判定部、15…照合データ保存部、16…ホワイトリスト配信部、17…ホワイトリスト保存部、18…電子メール解析部、19…送信情報保存部、20…ホワイトリストデータベース、21…配信データ保存部、22…送受信処理部、23…登録データ保存部。

請求の範囲

- [請求項1] 複数のメールサーバのそれぞれで受信された電子メールから抽出される、前記電子メールの送信情報を受け付けるデータ受信部と、
前記送信情報に基づいて前記電子メールの送信元が適切か否かを判定する送信情報判定部と、
前記適切と判定された前記送信元を複数の前記メールサーバのそれぞれに配信するホワイトリスト配信部と、
を備えることを特徴とする情報処理装置。
- [請求項2] 前記送信元は、送信元メールアドレスのドメインと送信元IPアドレスとの組み合わせから構成される、
ことを特徴とする請求項1に記載の情報処理装置。
- [請求項3] 前記送信情報は、受信された前記電子メールにおける送信に係る各種の情報を含み、
前記送信情報のそれぞれについて有害となる悪性情報を予め保存する照合データ保存部を備えて、
前記送信情報判定部は、受け付けた前記送信情報と前記悪性情報とを照合して、前記電子メールの前記送信元が適切か否かを判定する、
ことを特徴とする請求項1に記載の情報処理装置。
- [請求項4] 前記送信情報判定部は、複数の前記メールサーバから受け付けた複数の前記送信情報において、前記送信情報に含まれる前記送信元が一致する場合には、当該前記送信元を適切と判定する、
ことを特徴とする請求項1に記載の情報処理装置。
- [請求項5] 前記送信情報判定部において前記適切と判定された前記送信元を保存するホワイトリスト保存部を備えて、
保存された前記送信元は、前記悪性情報と照合されて、前記送信元が適切か否かの判定結果が更新される、
ことを特徴とする請求項3に記載の情報処理装置。
- [請求項6] 前記データ受信部は、ユーザにより登録される、送信元メールアドレス

レスのドメインと送信元 I P アドレスの組み合わせからなる前記送信元を受け付けて、

前記ホワイトリスト配信部は、前記送信元を前記メールサーバのそれぞれに配信する、

ことを特徴とする請求項 1 に記載の情報処理装置。

[請求項7]

複数のメールサーバのそれぞれにおいてユーザにより登録される、送信元メールアドレスのドメインと送信元 I P アドレスの組み合わせからなる送信元を受け付けるデータ受信部と、

前記送信元を前記メールサーバのそれぞれに配信するホワイトリスト配信部と、

を備えることを特徴とする情報処理装置。

[請求項8]

受け付けた前記送信元メールアドレスのドメインと送信元 I P アドレスとの組み合わせからなる前記送信元が適切か否かを判定する送信情報判定部を備えることを特徴とする請求項 7 に記載の情報処理装置。

[請求項9]

前記データ受信部は、ユーザにより登録される、1つのメールのドメインと複数の送信元 I P アドレスとの組み合わせからなる前記送信元を受け付ける、

ことを特徴とする請求項 7 に記載の情報処理装置。

[請求項10]

複数のメールサーバのそれぞれで受信された電子メールから抽出される、前記電子メールの送信情報を受け付けるステップと、

前記送信情報に基づいて前記電子メールの送信元のドメイン及び送信元 I P アドレスが適切か否かを判定するステップと、

前記適切と判定された前記送信元のドメイン及び送信元 I P アドレスを複数の前記メールサーバのそれぞれに配信するステップと、を含むことを特徴とする情報処理方法。

[請求項11]

コンピュータを、

複数のメールサーバのそれぞれで受信された電子メールから抽出さ

れる、前記電子メールの送信情報を受け付ける機能、

前記送信情報に基づいて前記電子メールの送信元のドメイン及び送信元IPアドレスが適切か否かを判定する機能、

前記適切と判定された前記送信元のドメイン及び送信元IPアドレスを複数の前記メールサーバのそれぞれに配信する機能、
として機能させることを特徴とする情報処理プログラム。