(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7111990号
(P7111990)

(45)発行日　令和4年8月3日(2022.8.3)

(24)登録日　令和4年7月26日(2022.7.26)

(51)国際特許分類

Ｈ０４Ｌ　51/00　(2022.01)		Ｈ０４Ｌ	51/00
Ｈ０４Ｌ　12/22　(2006.01)		Ｈ０４Ｌ	12/22

ＦＩ

請求項の数　9　（全13頁）

(21)出願番号　特願2019-97054(P2019-97054)
(22)出願日　令和1年5月23日(2019.5.23)
(62)分割の表示　特願2017-189558(P2017-189558)の分割
原出願日　平成29年9月29日(2017.9.29)
(65)公開番号　特開2019-135680(P2019-135680A)
(43)公開日　令和1年8月15日(2019.8.15)
審査請求日　令和2年9月25日(2020.9.25)

(73)特許権者　390002761
キヤノンマーケティングジャパン株式会社
東京都港区港南２丁目１６番６号
(73)特許権者　592135203
キヤノンＩＴソリューションズ株式会社
東京都港区港南２丁目１６番６号
(74)代理人　100189751
弁理士　木村 友輔
(72)発明者　大和 大輝
東京都品川区東品川２丁目４番１１号
キヤノンＩＴソリューションズ株式会社内
(72)発明者　山内 覚
東京都品川区東品川２丁目４番１１号

最終頁に続く

(54)【発明の名称】　情報処理装置、情報処理システム、制御方法、及びプログラム

(57)【特許請求の範囲】

【請求項１】

コンピュータを、

電子メールを受け付ける受付手段と、

前記電子メールのタイプを特定する特定手段と、

前記特定手段にて所定のタイプとして特定され、当該特定された電子メールの宛先が所定の条件を満たす特定の宛先か否かに応じて設定された時間範囲および数を満たす場合に、当該電子メールに対して、当該電子メールの宛先が前記特定の宛先か否かに応じて決定されるアクションを実行する実行手段

として機能させるためのプログラム。

【請求項２】

前記所定のタイプは、標的型攻撃メールに係る区分であることを特徴とする請求項１に記載のプログラム。

【請求項３】

前記実行手段を、前記電子メールの中継を保留するアクションを実行する手段として機能させるための請求項１または２に記載のプログラム。

【請求項４】

前記コンピュータを、さらに、

前記所定の条件を満たす宛先を記憶する記憶手段として機能させるための請求項１～３の何れか１項に記載のプログラム。

【請求項５】
前記所定の条件を満たす宛先とは、公開された電子メールアドレスであることを特徴とする請求項１～４の何れか１項に記載のプログラム。
【請求項６】
前記実行手段を、所定の除外ルールを満たさない電子メールに対して、前記所定のアクションを実行する手段として機能させるための請求項１～５の何れか１項に記載のプログラム。
【請求項７】
前記所定の除外ルールは、前記電子メールの送信者、受信者、件名の少なくとも１つに係る情報が条件として設定されることを特徴とする請求項６に記載のプログラム。
【請求項８】
電子メールを受け付ける受付手段と、
前記電子メールのタイプを特定する特定手段と、
前記特定手段にて所定のタイプとして特定され、当該特定された電子メールの宛先が所定の条件を満たす特定の宛先か否かに応じて設定された時間範囲および数を満たす場合に、当該電子メールに対して、当該電子メールの宛先が前記特定の宛先か否かに応じて決定されるアクションを実行する実行手段と、
を備えることを特徴とする情報処理装置。
【請求項９】
情報処理装置の受付手段が、電子メールを受け付ける受付ステップと、
前記情報処理装置の特定手段が、前記電子メールのタイプを特定する特定ステップと、
前記情報処理装置の実行手段が、前記特定ステップにて所定のタイプとして特定され、当該特定された電子メールの宛先が所定の条件を満たす特定の宛先か否かに応じて設定された時間範囲および数を満たす場合に、当該電子メールに対して、当該電子メールの宛先が前記特定の宛先か否かに応じて決定されるアクションを実行する実行ステップと、
を備えることを特徴とする情報処理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、標的型攻撃メールを特定する方法に関する。
【背景技術】
【０００２】
ネットワーク技術の発展に伴い、多様な情報が流通するようになり、このような情報を多くのユーザに提供する非常に利便性の高いツールが存在する。
【０００３】
例えば、インターネット上のＨＴＭＬや画像などといったリソースの場所を特定するためのＵＲＬをクリックすることで、ユーザが所望するリソースを入手することが可能である。
【０００４】
しかしながら、最近では、このようなツールの利便性を悪用し、不正にリソースへアクセスさせることで、ウイルスへの感染や多額の支払いを求められるなどの被害が発生している。
【０００５】
このようなツールを悪用した被害例として、不正なリソースの場所を特定するＵＲＬが付与された電子メールを企業のユーザへ一方的に送り付け、当該ユーザがこの電子メールを開いて、誤って電子メールのＵＲＬをクリックするといった被害が発生している。
【０００６】
そこで、このような問題を解消する方法として、受信した電子メールの特徴を保存しておき、新たに受信する電子メールの特徴と過去に受信した電子メールの特徴との類似度が基準値より低い場合、標的型攻撃メールとして特定する技術が開示されている（例えば、

特許文献１参照）。
【先行技術文献】
【特許文献】
【０００７】
【文献】特開２０１３－２３６３０８号公報
【発明の概要】
【発明が解決しようとする課題】
【０００８】
近年、標的型攻撃メールとして、企業等の組織体に対して、同じあるいは類似した電子メールを多くの従業員のメールアドレスに対して送り付ける、いわゆるばらまき型攻撃メールが存在する。
【０００９】
しかしながら、特許文献１に記載された技術では、新たに受信した電子メールが過去に受信した電子メールとの類似度を求めることで、当該新たに受信した電子メールの正当性を判断しており、ばらまき型攻撃メールのように、組織内で拡散された電子メールをまとめて特定することについてまでは、記載や示唆はされていない。
【００１０】
従って、ばらまき型攻撃メールを受信した際に、システムの管理者等は、ばらまき型攻撃メールを受信した従業員等を特定することで、その影響範囲をいち早くつかみ、対処しなければならないが、特許文献１に記載の技術では、このような課題を解決するには至らない。
【００１１】
そこで、本発明では、悪意ある電子メールの可能性がある電子メールに対して、行うべき処理を円滑に実行することが可能な情報処理装置、情報処理システム、制御方法、及び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】
【００１２】
上記課題を解決するための本発明は、コンピュータを、電子メールを受け付ける受付手段と、前記電子メールのタイプを特定する特定手段と、前記特定手段にて所定のタイプとして特定され、当該特定された電子メールの宛先が所定の条件を満たす特定の宛先か否かに応じて設定された時間範囲および数を満たす場合に、当該電子メールに対して、当該電子メールの宛先が前記特定の宛先か否かに応じて決定されるアクションを実行する実行手段として機能させるためのプログラムである。
【発明の効果】
【００１３】
本発明によれば、悪意ある電子メールの可能性がある電子メールに対して、行うべき処理を円滑に実行することができる、という効果を奏する。
【図面の簡単な説明】
【００１４】
【図１】情報処理システムの概略構成を示す構成図である。
【図２】アクセス中継装置、メール中継装置、メールサーバ、外部サーバ、及びクライアント端末のハードウェアの概略構成を示す構成図である。
【図３】メール中継装置の機能構成を示す構成図である。
【図４】標的型攻撃メールの特定処理を示すフローチャートである。
【図５】各テーブルの構成を示す構成図である。
【発明を実施するための形態】
【００１５】
以下、図面を参照して、本発明の実施形態を詳細に説明する
図１には、本発明の実施形態に係る情報処理システムの概略の構成図が示されている。
【００１６】

図１に示すように、本実施形態に係る情報処理システム１００は、アクセス中継装置１０２、メールサーバ１０４、メール中継装置１０６、クライアント端末１０８（少なくとも１台以上備える）、及びＬＡＮ１１０を含む構成を備えており、広域ネットワーク１１２を介して外部サーバ１１４と接続されている。

【００１７】

アクセス中継装置１０２は、情報処理装置として機能する装置であり、クライアント端末１０８と広域ネットワーク１１２を介してデータの通信を行う外部サーバ１１４との中継を行う。

【００１８】

また、アクセス中継装置１０２は、クライアント端末１０８と外部サーバ１１４との間で送受信されるデータを中継するか、あるいは、中継しないかを決定するための中継制御ルールに従って、当該データの通信を制御している。

【００１９】

メールサーバ１０４は、電子メールの送受信を行うために用いられる情報処理装置であって、電子メールのメールアドレス管理や、当該メールアドレスに送信されてきた電子メールを保存する等の機能を有している。

【００２０】

メール中継装置１０６は、メールサーバ１０４やクライアント端末１０８から送信される電子メールに対する送信制御処理を、送信制御ルールを用いて行うとともに、外部サーバ１１４から送信される電子メールに対する受信制御処理を、後述する受信制御ルールを用いて行う。

【００２１】

また、メール中継装置１０６は、クライアント端末１０８を操作するユーザからの要求に応じて、電子メールの送信制御処理（受信制御処理）に用いる送信制御ルール（受信制御ルール）の入力を受け付けたり、送信制御処理（受信制御処理）の結果、送信（受信）が保留された電子メールに対する送信（受信）、送信禁止（受信禁止）の入力（監査入力）を受け付けたりする。

【００２２】

さらに、メール中継装置１０６は、クライアント端末１０８を操作するユーザからの要求に応じて、既に受信した電子メールのなかから、不正な電子メールを特定し、管理者や受信者へ警告通知などを行う。

【００２３】

クライアント端末１０８は、メールサーバ１０４で管理されているメールアドレスを使用して電子メールのやり取りを行うユーザが操作する端末装置である。

【００２４】

また、クライアント端末１０８は、外部サーバ１１４から提供される様々なコンテンツ等をユーザへ提供する端末装置でもある。

【００２５】

さらに、クライアント端末１０８は、ＬＡＮ１１０を介してアクセス中継装置１０２及びメール中継装置１０６に記憶した中継制御ルール、送信制御ルール、及び受信制御ルールの参照や登録等を行うことが可能である。

【００２６】

外部サーバ１１４は、様々なコンテンツ等をユーザへ提供する装置であり、サービス事業者や個人ユーザ等によって設置されたものであったり、外部のユーザが所有するメールサーバとして設置されたものであったりする。

【００２７】

次に、図２では、アクセス中継装置１０２、メールサーバ１０４、メール中継装置１０６、及びクライアント端末１０８に適用可能な情報処理装置のハードウェア構成の一例について説明する。

【００２８】

図２において、２０１はＣＰＵで、システムバス２０４に接続される各デバイスやコントローラを統括的に制御する。また、ＲＯＭ２０２あるいは外部メモリ２１１には、ＣＰＵ２０１の制御プログラムであるＢＩＯＳ（Ｂａｓｉｃ Ｉｎｐｕｔ ／ Ｏｕｔｐｕｔ Ｓｙｓｔｅｍ）やオペレーティングシステムプログラム（以下、ＯＳ）や、各サーバ或いは各ＰＣの実行する機能を実現するために必要な後述する各種プログラム等が記憶されている。

【００２９】

２０３はＲＡＭで、ＣＰＵ２０１の主メモリ、ワークエリア等として機能する。ＣＰＵ２０１は、処理の実行に際して必要なプログラム等をＲＯＭ２０２あるいは外部メモリ２１１からＲＡＭ２０３にロードして、該ロードしたプログラムを実行することで各種動作を実現するものである。

【００３０】

また、２０５は入力コントローラで、キーボード（ＫＢ）２０９や不図示のマウス等のポインティングデバイス等からの入力を制御する。２０６はビデオコントローラで、ＣＲＴディスプレイ（ＣＲＴ）２１０等の表示器への表示を制御する。

【００３１】

なお、図２では、ＣＲＴ２１０と記載しているが、表示器はＣＲＴだけでなく、液晶ディスプレイ等の他の表示器であってもよい。これらは必要に応じて管理者が使用するものである。

【００３２】

２０７はメモリコントローラで、ブートプログラム、各種のアプリケーション、フォントデータ、ユーザファイル、編集ファイル、各種データ等を記憶するハードディスク（ＨＤ）や、フレキシブルディスク（ＦＤ）、或いはＰＣＭＣＩＡカードスロットにアダプタを介して接続されるコンパクトフラッシュ（登録商標）メモリ等の外部メモリ２１１へのアクセスを制御する。

【００３３】

２０８は通信Ｉ／Ｆコントローラで、ネットワーク（例えば、図１に示したＬＡＮ１１０）を介して外部機器と接続・通信するものであり、ネットワークでの通信制御処理を実行する。例えば、ＴＣＰ／ＩＰを用いた通信等が可能である。

【００３４】

なお、ＣＰＵ２０１は、例えばＲＡＭ２０３内の表示情報用領域へアウトラインフォントの展開（ラスタライズ）処理を実行することにより、ＣＲＴ２１０上での表示を可能としている。また、ＣＰＵ２０１は、ＣＲＴ２１０上の不図示のマウスカーソル等でのユーザ指示を可能とする。

【００３５】

本発明を実現するための後述する各種プログラムは、外部メモリ２１１に記録されており、必要に応じてＲＡＭ２０３にロードされることによりＣＰＵ２０１によって実行されるものである。

【００３６】

さらに、上記プログラムの実行時に用いられる定義ファイル及び各種情報テーブル等も、外部メモリ２１１に格納されており、これらについての詳細な説明も後述する。

【００３７】

次に、図３を用いてメール中継装置１０６の機能構成について説明する。尚、各機能の詳細については、後述するフローチャートなどで説明を行う。

【００３８】

メール中継装置１０６は、記憶部３００、ルール情報取得部３０２、メール取得部３０４、及び動作部３０６を備えている。

【００３９】

記憶部３００は、電子メールの受信を制御するためのルールや、標的型攻撃メールを特定するためのルール、公開アドレスの情報、受信した電子メールに関する情報等を記憶管

理する。
【００４０】
ルール情報取得部３０２は、記憶部３００によって記憶管理される標的型攻撃メールを特定するためのルールに関する情報を取得し、メール取得部３０４は、記憶部３００によって記憶管理される電子メールに関する情報を取得する。
【００４１】
動作部３０６は、標的型攻撃メールとして特定された電子メールに対して、この特定に至り該当したルールに対して定義されたアクションを実行する。
【００４２】
次に、図４に示すフローチャートを用いて標的型攻撃メールの特定処理について説明を行う。
【００４３】
ステップＳ１００では、ルール情報取得部３０２は、記憶部３００における判定ルールＤＢ（図５参照）より、電子メールが標的型攻撃メールか否かを判定する際に用いる判定ルール情報を取得する。
【００４４】
図５の最上段には、判定ルールＤＢの構成が示されており、電子メールが標的型攻撃メールか否かを判定するための判定ルールを一意に識別すためのＩＤ、所定時間内に受信した電子メールを特定するために、当該所定時間を定めた時間範囲、所定時間内に受信した電子メールの数を特定するために、当該電子メールの数を示す電子メール数、公開アドレスのＩＤを示す公開アドレスＩＤ、標的型攻撃メールの特徴を識別するための攻撃区分、判定ルールに該当した場合、電子メールに対する動作を示すアクションを含んで構成されている。
【００４５】
図５では、判定ルールの一例が示されており、例えば、最上段のレコードのように、ＩＤが１、時間範囲が１０分、電子メール数が１００、公開アドレスＩＤがＮＵＬＬ（詳細後述）、攻撃区分が２ｏｒ３、アクションが自動でフィルタリングルールに反映が判定ルールＤＢへ記憶されているとする。
【００４６】
この判定ルールは、１０分以内に１００件以上の電子メールを受信した場合であって、それらの電子メールが標的型攻撃の特徴として、偽装されたＵＲＬが電子メールに付与されている、あるいは、二重拡張子とみなされたファイルが添付されているといった電子メールである場合（詳細後述）、その電子メールに関する動作として、今後受信する電子メールをフィルタリングするために、自動でフィルタリングの条件を設定することが示されている。
【００４７】
フィルタリングの条件の例としては、標的型攻撃メールとして特定された電子メールの送信者のアドレスを条件として設定しておくことで、設定後、当該送信者が電子メールを送信してきた場合、その電子メールを一意時的に保留する、あるいは削除する等の対応をとることが可能である。
【００４８】
尚、公開アドレスＩＤについては、図５の最上段から３段目の左に示される公開アドレスリストＤＢに記憶されているＩＤに対応する。
【００４９】
公開アドレスリストＤＢは、公開アドレスを一意に識別するためのＩＤと公開されたアドレスを示す公開アドレスを含む構成を備えている。
【００５０】
この公開アドレスとは、例えば、自社の広報や人事等への問い合わせや、お客様窓口等に関して、外部へ公開しているアドレスを示している。
【００５１】

また、攻撃区分については、図５の最上段から３段目に示される標的型攻撃区分ＤＢに記憶されているＩＤに対応する。

【００５２】

標的型攻撃区分ＤＢは、受信した電子メールに関して、標的型攻撃メールであるか否かを判定するためのルールによって、標的型攻撃メールであると判定した理由に関する情報を記憶しており、その理由を一意に識別するためのＩＤ、その理由に対応する攻撃内容を含む構成を備えている。

【００５３】

このような判定ルールによって、標的型攻撃メールのうち、特にばらまき型の攻撃メールを特定することが可能となる。

【００５４】

また、最上段から２段目のレコードのように、時間範囲が３分、電子メール数が３、公開アドレスＩＤが３、攻撃区分がＮＵＬＬ、アクションが管理者に通知、受信者に通知、ホームページ表示が判定ルールＤＢへ記憶されているとする。

【００５５】

このレコードは、３分以内に３件以上の電子メールを受信した場合であって、受信者のメールアドレスに公開アドレスＩＤから特定される公開アドレスが含まれている場合、その電子メールに関して、管理者、受信者に標的型攻撃メールが送信されてきている旨を示す通知を行う、自社が開設しているホームページへ標的型攻撃メールが送信されてきている旨を示す情報を表示する。

【００５６】

公開アドレス自体は、標的型攻撃メールのターゲットになり易く、頻繁に公開アドレスを使っての送受信者間でのやり取りが行われることは稀であることから、時間範囲と電子メール数については、最上段からのレコードと比較して、小さい値を設定することが可能である。

【００５７】

尚、公開アドレスＩＤに関しては、複数のＩＤを記憶することが可能であり、例えば、送信者が所定時間内で電子メールを送信する可能性が低い宛先として、相互に関連性の低い製品に係る窓口と就職に係る窓口とに、電子メールが送信された場合、標的型攻撃メールの可能性が高いので、このような電子メールをも特定することが可能となる。

【００５８】

この場合、判定ルールＤＢには、電子メール数を設定せず、公開アドレスＩＤに対して、複数の値を設定することが可能である。

【００５９】

このような判定ルールによって、同様に、標的型攻撃メールのうち、特にばらまき型の攻撃メールを特定することが可能となる。

【００６０】

ステップＳ１０２では、ルール情報取得部３０２は、ステップＳ１００において判定ルール情報を取得した結果、取得できたと判定した場合は、ステップＳ１０４へ処理を進め、取得できたと判定しない場合は、処理を終了する。

【００６１】

ステップＳ１０４では、ルール情報取得部３０２は、記憶部３００における除外ルールＤＢ（図５参照）より、電子メールが判定ルールによって標的型攻撃メールとして特定されても、例外として、標的型攻撃メールと見做さないことを定めるための除外判定ルール情報を取得する。

【００６２】

図５の最上段から２段目には、除外ルールＤＢの構成が示されており、除外ルールＤＢは、例外として、標的型攻撃メールと見做さないことを定めるための除外判定ルールを一意に識別するためのＩＤ、電子メールの送信者のアドレスを示す送信者、電子メールの受信者のアドレスを示す受信者、及び電子メールの件名を含む構成を備えている。

【００６３】
図５では、除外判定ルールの一例が示されており、例えば、最上段のレコードのように、送信者のアドレスがｎｅｗｓ－ｗｅｅｋ　ｅｘａｍｐｌｅ．ｎｅｔであり、件名がｗｅｅｋｌｙ　ｍａｇａｚｉｎｅの場合、判定ルールによって標的型攻撃メールとして特定された電子メールであっても、標的型攻撃メールとして見做さない。
【００６４】
また、最上段から２段目のレコードのように、送信者のアドレスがｎｅｗｓ－ｄａｉｌｙ　ｅｘａｍｐｌｅ．ｎｅｔであり、受信者のアドレスがｓａｌｅｓ　ｃａｎｏｎ－ｉｔｓ．ｃｏ．ｊｐ、件名が先頭にｄａｉｌｙを含む語の場合、判定ルールによって標的型攻撃メールとして特定された電子メールであっても、標的型攻撃メールとして見做さない。
【００６５】
これらの除外判定ルールはメールマガジンやニュースなどの特定の安全な送信者から大量に同一あるいは類似の電子メールが所定時間内に送信されてくるため、こういった電子メールを標的型攻撃メールと見做さないことで、標的型攻撃メールを特定するための手間を軽減することが可能である。
【００６６】
ステップＳ１０６では、ルール情報取得部３０２は、ステップＳ１０４において除外判定ルール情報を取得できたか否かを判定し、取得できたと判定しない場合は、ステップＳ１０８へ処理を進め、取得できたと判定した場合は、ステップＳ１１０へ処理を進める。
【００６７】
ステップＳ１０８では、メール取得部３０４は、ステップＳ１００においてルール情報取得部３０２によって取得した判定ルール情報に基づいて記憶部３００におけるメールログＤＢ（図５参照）から電子メールに関する情報を取得する。
【００６８】
図５の最下段には、既に受信した電子メールの情報を記憶するメールログＤＢの構成が示されており、電子メールを一意に識別するためのＩＤ、電子メールを受信した時刻を示す受信日時、電子メールの送信者、電子メールの受信者、電子メールの件名、及び標的型攻撃の特徴を識別する攻撃区分を含んで構成されている。
【００６９】
尚、攻撃区分については、前述したように、電子メールを受信した際に、標的型攻撃メールであるか否かを判定するためのルールによって、標的型攻撃メールであると判定した理由に関する情報を記憶している。
【００７０】
本ステップでは、まず、メールログＤＢに記憶された電子メールのうち、送信者のアドレスが同一、あるいは、件名が同一または類似、あるいは、本文が同一または類似、あるいは、これらの全ての条件、あるいは、任意の組み合わせた条件を満たし、さらに受信者のアドレスが異なる、あるいは受信者のアドレスは同じものでも良い等の条件を満たす電子メールを特定する。
【００７１】
そして、このような条件で特定された電子メールであって、さらに判定ルール情報を満たす電子メールであれば、標的型攻撃メールであるとして、その電子メールに関する情報を取得する。
【００７２】
例えば、判定ルール情報として、図５の最上段のレコードを適用すると、１０分間に１００件以上の受信がなされ、攻撃区分が２ｏｒ３であることから、図５に示すように、メールログＤＢの送信者が、ａｔｔａｃｋｅｒ　ｅｘａｍｐｌｅ．ｃｏｍであり、受信者が異なる電子メールとして、ＩＤが１から７・・・が特定され、この特定された電子メールの受信日時が１０分以内で１００件以上受信しており、攻撃区分が２ｏｒ３の電子メールに関する情報を取得する。
【００７３】

一方、判定ルール情報として、図５の最上段から２段目のレコードを適用すると、３分以内に３件以上の公開アドレスＩＤが３であることから、メールログＤＢの送信者が、ａｔｔａｃｋｅｒ　ｅｘａｍｐｌｅ．ｃｏｍであり、受信者が異なる電子メールとして、ＩＤが１から７・・・が特定され、この特定された電子メールの受信日時が３分以内で３件以上受信しており、送信者がｓｕｐｐｏｒｔ　ｃａｎｏｎ－ｉｔｓ．ｃｏ．ｊｐの電子メールに関する情報を取得する。

【００７４】

ステップS１１０では、メール取得部３０４は、ステップＳ１００においてルール情報取得部３０２によって取得した判定ルール情報、及びステップＳ１０４においてルール情報取得部３０２によって取得した除外判定ルール情報に基づいて記憶部３００におけるメールログＤＢから電子メールに関する情報を取得する。

【００７５】

本ステップでは、まず、判定ルール情報に基づいて記憶部３００におけるメールログＤＢから電子メールを特定するが、ステップＳ１０８と同様な処理を行うため説明を省略する。

【００７６】

続いて、判定ルール情報に従って特定された電子メールに対して、除外判定ルール情報を満たす電子メールを標的型攻撃メールと見做さず、除外判定ルール情報を満たさない電子メールを標的型攻撃メールと見做して、当該電子メールに関する情報をメールログＤＢから取得する。

【００７７】

例えば、除外判定ルール情報として、図５の最上段のレコードを適用すると、判定ルール情報に従って特定された電子メールの送信者がｎｅｗｓ－ｗｅｅｋ　ｅｘａｍｐｌｅ．ｎｅｔであり、件名がｗｅｅｋｌｙ　ｍａｇａｚｉｎｅの場合、当該電子メールは標的型攻撃メールと見做さないが、判定ルール情報に従って特定された電子メールの送信者がｎｅｗｓ－ｗｅｅｋ　ｅｘａｍｐｌｅ．ｎｅｔでない、あるいは、件名がｗｅｅｋｌｙ　ｍａｇａｚｉｎｅでない場合、当該電子メールを標的型攻撃メールと見做す。

【００７８】

一方、除外判定ルール情報として、図５の最上段から２段目のレコードを適用すると、判定ルール情報に従って特定された電子メールの送信者がｎｅｗｓ－ｄａｉｌｙ　ｅｘａｍｐｌｅ．ｎｅｔであり、受信者のアドレスがｓａｌｅｓ　ｃａｎｏｎ－ｉｔｓ．ｃｏ．ｊｐ、件名が先頭にｄａｉｌｙを含む語の場合、当該電子メールを標的型攻撃メールと見做さないが、判定ルール情報に従って特定された電子メールの送信者がｎｅｗｓ－ｄａｉｌｙ　ｅｘａｍｐｌｅ．ｎｅｔでない、あるいは、受信者のアドレスがｓａｌｅｓ　ｃａｎｏｎ－ｉｔｓ．ｃｏ．ｊｐでない、あるいは、件名が先頭にｄａｉｌｙを含む語でない場合、当該電子メールを標的型攻撃メールと見做す。

【００７９】

ステップＳ１１２では、動作部３０６は、ステップＳ１０８あるいはステップＳ１１０においてメール取得部３０４によって標的型攻撃メールとしてメールログＤＢから取得した電子メールに関して、当該電子メールが満たした判定ルールにおけるアクションを実行する。

【００８０】

このアクションを行う際に、標的型攻撃メールとして見做された電子メールに付与されたＵＲＬ等のリソースを特定する情報を抽出し、アクセス中継装置１０２へ送信した後、アクセス中継装置１０２は、このリソースを特定する情報を自身に登録しておくことで、クライアント端末１０８から外部サーバ１１４の当該リソースへアクセスする際に、その通信の中継を制御することが可能である。

【００８１】

以上、本発明によれば、悪意ある電子メールを容易に特定することができる。

【００８２】

なお、上述した各種データの構成及びその内容はこれに限定されるものではなく、用途や目的に応じて、様々な構成や内容で構成されることは言うまでもない。

【００８３】

以上、一実施形態について示したが、本発明は、例えば、方法、プログラムもしくは記録媒体等としての実施態様をとることが可能である。

【００８４】

また、本発明におけるプログラムは、図４に示すフローチャートの処理方法をコンピュータが実行可能なプログラムである。

【００８５】

以上のように、前述した実施形態の機能を実現するプログラムを記録した記録媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記録媒体に格納されたプログラムを読出し実行することによっても、本発明の目的が達成されることは言うまでもない。

【００８６】

この場合、記録媒体から読み出されたプログラム自体が本発明の新規な機能を実現することになり、そのプログラムを記憶した記録媒体は本発明を構成することになる。

【００８７】

プログラムを供給するための記録媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＥＥＰＲＯＭ、シリコンディスク、ソリッドステートドライブ等を用いることができる。

【００８８】

また、コンピュータが読み出したプログラムを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムの指示に基づき、コンピュータ上で稼働しているＯＳ（オペレーティングシステム）等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００８９】

さらに、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００９０】

また、システムあるいは装置にプログラムを供給することによって達成される場合にも適応できることは言うまでもない。この場合、本発明を達成するためのプログラムを格納した記録媒体を該システムあるいは装置に読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【００９１】

さらに、本発明を達成するためのプログラムをネットワーク上のサーバ、データベース等から通信プログラムによりダウンロードして読み出すことによって、そのシステムあるいは装置が、本発明の効果を享受することが可能となる。

【００９２】

なお、上述した各実施形態およびその変形例を組み合わせた構成も全て本発明に含まれるものである。

【符号の説明】

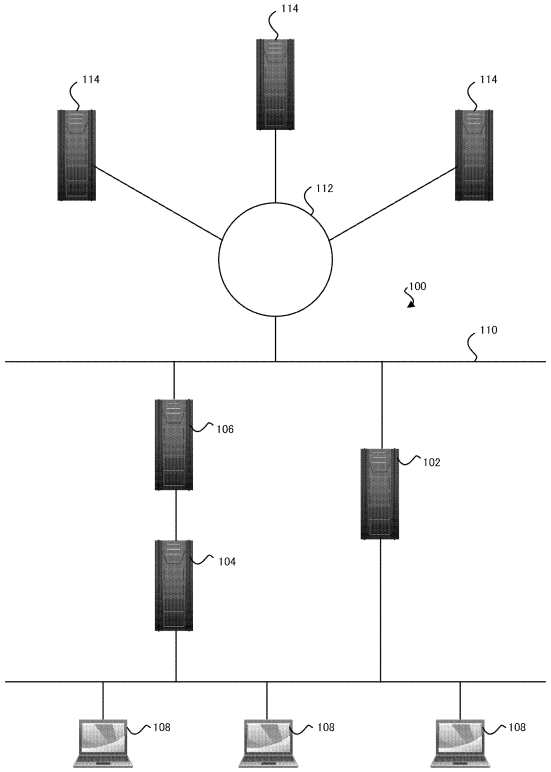
【００９３】

１００　情報処理システム
１０２　アクセス中継装置
１０４　メールサーバ

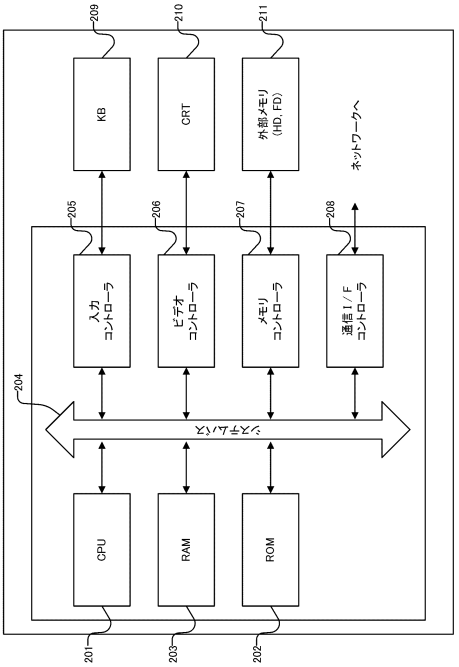
１０６　メール中継装置
１０８　クライアント端末
１１０　ＬＡＮ
１１２　広域ネットワーク
１１４　外部サーバ

【図面】

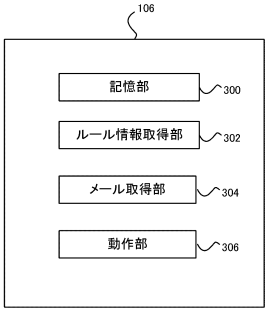
【図１】



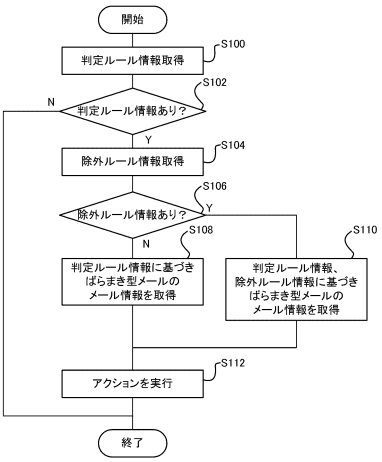
【図２】



【図３】



【図４】



【図５】

【判定ルールDB】

ID	時間範囲	電子メール数	公開アドレスID	攻撃区分	アクション
1	10 min	100	Null	2 or 3	自動でフィルタリングルールに反映
2	3 min	3	3	Null	管理者に通知、受信者に通知、ホームページ表示
…	…	…	…	…	…

【除外ルールDB】

ID	送信者	受信者	件名
1	news-week@example.net	*	weekly magazine
2	news-daily@example.net	sales@canon-its.co.jp	daily*
…	…	…	…

【公開アドレスリストDB】

ID	公開アドレス
1	info@canon-its.co.jp
2	sales@canon-its.co.jp
3	support@canon-its.co.jp
…	…

【標的型攻撃区分DB】

ID	攻撃内容
1	偽装されたURL
2	二重拡張子
3	実行形式(RLO制御文字)
…	…

【メールログDB】

ID	受信日時	送信者	受信者	件名	攻撃区分
1	2017/8/30 12:00:00	attacker@example.com	user01@canon-its.co.jp	請求書	1/3
2	2017/8/30 12:00:00	attacker@example.com	user02@canon-its.co.jp	請求書	1/3
3	2017/8/30 12:00:00	attacker@example.com	user03@canon-its.co.jp	請求書	1/3
4	2017/8/30 12:00:00	attacker@example.com	user04@canon-its.co.jp	請求書	1/3
5	2017/8/30 12:00:01	attacker@example.com	info@canon-its.co.jp	見積書	2
6	2017/8/30 12:00:01	attacker@example.com	sales@canon-its.co.jp	見積書	2
7	2017/8/30 12:00:02	attacker@example.com	support@canon-its.co.jp	見積書	2
…	…	…	…	…	…

フロントページの続き

キヤノンＩＴソリューションズ株式会社内

審査官　岩田 玲彦

(56)参考文献　特開２００６－１２８９１７（ＪＰ，Ａ）
特開２００３－１５０５１３（ＪＰ，Ａ）
特開２０１３－２３６３０８（ＪＰ，Ａ）
特開２００４－１４０７３３（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　５１／００
Ｈ０４Ｌ　１２／２２