【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成21年6月25日(2009.6.25)

【公表番号】特表2008-545177(P2008-545177A)
【公表日】平成20年12月11日(2008.12.11)
【年通号数】公開・登録公報2008-049
【出願番号】特願2008-510321(P2008-510321)
【国際特許分類】
Ｇ０６Ｆ　13/00　　(2006.01)
Ｇ０６Ｆ　21/22　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　13/00　　６１０Ｑ
Ｇ０６Ｆ　 9/06　　６６０Ｎ

【手続補正書】
【提出日】平成21年4月28日(2009.4.28)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ネットワークインターフェース、
該ネットワークインターフェースに接続された一つ以上の処理装置、および、
該一つ以上の処理装置に接続され、該一つ以上の処理装置によって実行される際に、該一つ以上の処理装置に実行させるロジックを備え、
前記ロジックは、
受信者アカウントの宛先アドレスを有する電子メールメッセージを受信する手段；
コンピューターウィルスを含むことがわかっているメッセージの属性を規定する一つ以上のルールに基づいて、前記メッセージに対するウィルススコア値を決定する手段であって、該属性は、前記メッセージへの添付ファイルの種類と、添付ファイルのサイズと、前記メッセージの送信者、件名または本文、および添付ファイル以外のシグネチャに基づく一つ以上の経験則と、を含むものである手段；および
ウィルスコア値が規定の閾値と同じかそれを上回る場合に、メッセージを受信者アカウントに即座に配信せずに、メッセージを隔離キューに記憶する手段；
として前記一つ以上の処理装置を機能させるものであることを特徴とする装置。
【請求項２】
受信者アカウントの宛先アドレスを有する電子メールメッセージを受信する手段、
コンピューターウィルスを含むことがわかっているメッセージの属性を規定する一つ以上のルールに基づいて、前記メッセージに対するウィルススコア値を決定する手段であって、該属性は、前記メッセージへの添付ファイルの種類と、添付ファイルのサイズと、前記メッセージの送信者、件名または本文、および添付ファイル以外のシグネチャに基づく一つ以上の経験則と、を含むものである手段、および
ウィルスコア値が規定の閾値と同じかそれを上回る場合に、メッセージを受信者アカウントに即座に配信せずに、メッセージを隔離キューに記憶する手段
を備えた装置。
【請求項３】
前記属性が添付ファイルのコンテンツの種類を含むことを特徴とする請求項１または２

に記載の装置。
【請求項４】
前記経験則は、
送信者識別子を前記メッセージから抽出し、
前記送信者識別子と関連付けられた信用スコア値を読み出し、
前記信用スコア値に少なくとも部分的に基づいて前記ウィルスコア値を決定するものであることを特徴とする請求項１または２に記載の装置。
【請求項５】
前記経験則は、前記メッセージの添付ファイルのバイトをＭｉｃｒｏｓｏｆｔ（登録商標）の実行ファイルの初期バイトを固有に識別するルールと照合するものであることを特徴とする請求項１または２に記載の装置。
【請求項６】
ネットワークインターフェース、
該ネットワークインターフェースに接続された一つ以上の処理装置、および、
該一つ以上の処理装置に接続され、該一つ以上の処理装置によって実行される際に、該一つ以上の処理装置に実行させるロジックを備え、
前記ロジックは、
受信者アカウントの宛先アドレスを有する電子メールメッセージを受信する手段；
前記メッセージに対する脅威スコア値を決定する手段；
前記脅威スコア値が規定の脅威閾値と同じかそれを上回る場合に、前記メッセージを受信者アカウントに即座に配信せずに、前記メッセージを隔離キューに記憶する手段；
先入れ先出しの以外の順序で複数の隔離終了基準のうち任意の基準に基づいて前記隔離キューから前記メッセージを解放する手段であって、それぞれの隔離終了基準は一つ以上の終了アクションと関連付けられているものである手段；および
特定の終了基準に基づいて、前記関連付けられた一つ以上の終了アクションを選択しおよび実行する手段；
として前記一つ以上の処理装置を機能させるものであることを特徴とする装置。
【請求項７】
受信者アカウントの宛先アドレスを有する電子メールメッセージを受信する手段、
前記メッセージに対する脅威スコア値を決定する手段、
前記脅威スコア値が規定の脅威閾値と同じかそれを上回る場合に、前記メッセージを受信者アカウントに即座に配信せずに、前記メッセージを隔離キューに記憶する手段、
先入れ先出しの以外の順序で複数の隔離終了基準のうち任意の基準に基づいて前記隔離キューから前記メッセージを解放する手段であって、それぞれの隔離終了基準は一つ以上の終了アクションと関連付けられている手段、および
特定の終了基準に基づいて、前記関連付けられた一つ以上の終了アクションを選択しおよび実行する手段
を備えた装置。
【請求項８】
前記隔離終了基準は、メッセージ隔離時間制限の満了、前記隔離キューのオーバーフロー、前記隔離キューからの手動解放、および前記脅威スコア値を決定するために一つ以上のルールの更新を受信することを含むことを特徴とする請求項６または７に記載の装置。
【請求項９】
（ａ）前記メッセージ隔離から前記メッセージを手動解放するようにとのユーザー要求に対応して、前記メッセージを修正なしに前記受信者アカウントに配信する手段、および、（ｂ）隔離が満杯に成りつつあるというメッセージに対応して、前記メッセージから添付ファイルを取り除きおよび前記添付ファイルのないメッセージを前記受信者アカウントに配信する手段をさらに含むことを特徴とする請求項６または７に記載の装置。
【請求項１０】
満了時間値をメッセージに割り当てる手段をさらに含み、

前記満了時間値は、経験則によるテストをメッセージコンテンツに適用する結果に基づいて異なることを特徴とする請求項６または７に記載の装置。
【請求項１１】
前記隔離終了基準は、前記脅威スコア値を決定するために一つ以上のルールの更新を受信し、前記終了アクションは更新されたルールに基づいてメッセージに対する脅威スコア値を再び決定するものであることを特徴とする請求項６または７に記載の装置。
【請求項１２】
前記一つ以上の異なる終了アクション群が、異なる隔離終了基準と関連付けられていることを特徴とする請求項６または７に記載の装置。
【請求項１３】
ネットワークインターフェース、
該ネットワークインターフェースに接続された一つ以上の処理装置、および
該一つ以上の処理装置に接続され、該一つ以上の処理装置によって実行される際に、該一つ以上の処理装置に実行させるロジックを備え、
前記ロジックは、
電子メッセージの特性を規定するルールであって該メッセージと関連付けられた脅威を示す複数のルールを受信しおよび記憶する手段であって、それぞれのルールが優先順位の値を持ち、それぞれのルールがメッセージ要素型と関連付けられている手段；
受信者アカウントの宛先アドレスを有する、複数のメッセージ要素を含む電子メールメッセージを受信する手段；
第一のメッセージ要素を抽出する手段；
前記第一のメッセージ要素のみを、選択されたルールであって前記第一のメッセージ要素に対応するメッセージ要素型を有するルールのみと照合し、かつ、前記選択されたルールの優先順位の順序にしたがって照合することによって、前記メッセージに対する脅威スコア値を決定する手段；
前記脅威スコア値が規定の閾値よりも大きい場合に、前記脅威スコア値を出力する手段；
として前記一つ以上の処理装置を機能させるものであることを特徴とする装置。
【請求項１４】
電子メッセージの特性を規定するルールであって該メッセージと関連付けられた脅威を示す複数のルールを受信しおよび記憶する手段であって、それぞれのルールが優先順位の値を持ち、それぞれのルールがメッセージ要素型と関連付けられている手段、
受信者アカウントの宛先アドレスを有する、複数のメッセージ要素を含む電子メールメッセージを受信する手段、
第一のメッセージ要素を抽出する手段、
前記第一のメッセージ要素のみを、選択されたルールであって前記第一のメッセージ要素に対応するメッセージ要素型を有するルールのみと照合し、かつ、前記選択されたルールの優先順位の順序にしたがって照合することによって、前記メッセージに対する脅威スコア値を決定する手段、および
前記脅威スコア値が規定の閾値よりも大きい場合に、前記脅威スコア値を出力する手段を備えた装置。
【請求項１５】
前記脅威スコア値が規定の閾値未満である場合にのみ、他のメッセージ要素を他のルールと照合することによって、前記メッセージに対する更新された脅威スコア値を決定する手段をさらに含むことを特徴とする請求項１３または１４に記載の装置。
【請求項１６】
前記メッセージの本文を解読することによって前記メッセージに対する更新された脅威スコア値を決定する手段、および、前記脅威スコア値が規定の閾値未満である場合にのみ本文を一つ以上のメール本文ルールと照合する手段をさらに含むことを特徴とする請求項１３または１４に記載の装置。

【請求項１７】
受信者アカウントの宛先アドレスを有する電子メールメッセージを受信するステップ、
コンピューターウィルスを含むことがわかっているメッセージの属性を規定する一つ以上のルールに基づいて、メッセージに対するウィルススコア値を決定するステップであって、該属性は、前記メッセージへの添付ファイルの種類と、添付ファイルのサイズと、前記メッセージの送信者、件名または本文、および添付ファイル以外のシグネチャに基づく一つ以上の経験則と、を含むものであるステップ、
ウィルスコア値が規定の閾値と同じかそれを上回る場合に、メッセージを受信者アカウントに即座に配信せずに、メッセージを隔離キューに記憶するステップ
を有してなる方法。
【請求項１８】
前記属性が添付のコンテンツの種類を含むことを特徴とする請求項１７に記載の方法。
【請求項１９】
前記経験則は、
送信者識別子をメッセージから抽出し、
前記送信者識別子と関連付けられた信用スコア値を読み出し、
前記信用スコア値に少なくとも部分的に基づいて前記ウィルスコア値を決定する
ものであることを特徴とする請求項１７に記載の方法
【請求項２０】
前記経験則は、前記メッセージの添付ファイルのバイトを「Ｍｉｃｒｏｓｏｆｔ」の実行ファイルの初期バイトを固有に識別するルールと照合するものであることを特徴とする請求項１７に記載の方法。
【請求項２１】
前記経験則は、
送信者識別子をメッセージから抽出し、
前記送信者識別子がローカルに記憶された送信者のブラックリストの中にあるか否かを決定し、
前記送信者識別子がブラックリストの中にあるか否かに少なくとも部分的に基づいて前記ウィルスコア値を決定する
ものであることを特徴とする請求項１７に記載の方法
【請求項２２】
前記経験則は、
送信者識別子をメッセージから抽出し、
ネットワーク上で、前記送信者識別子が記憶された送信者のブラックリストの中にあるか否かを決定するよう外部サービスを要求し、および前記外部サービスからの応答を受信し、
前記応答に少なくとも部分的に基づいて前記ウィルスコア値を決定する
ものであることを特徴とする請求項１７に記載の方法。
【請求項２３】
受信者アカウントの宛先アドレスを有する電子メールメッセージを受信するステップ、
前記メッセージに対する脅威スコア値を決定するステップ、
前記脅威スコア値が規定の脅威閾値と同じかそれを上回る場合に、前記メッセージを受信者アカウントに即座に配信せずに、前記メッセージを隔離キューに記憶するステップ、
先入れ先出しの以外の順序で複数の隔離終了基準のうち任意の基準に基づいて前記隔離キューから前記メッセージを解放するステップであって、それぞれの隔離終了基準は一つ以上の終了アクションと関連付けられているステップ、および
特定の終了基準に基づいて、前記関連付けられた一つ以上の終了アクションを選択しおよび実行するステップ
を有してなる方法。
【請求項２４】

（ａ）前記メッセージ隔離から前記メッセージを手動解放するようにとのユーザー要求に対応して、前記メッセージを修正なしに前記受信者アカウントに配信するステップ、および（ｂ）隔離が満杯に成りつつあるというメッセージに対応して、前記メッセージから添付ファイルを取り除きおよび前記添付ファイルのないメッセージを前記受信者アカウントに配信するステップをさらに含むことを特徴とする請求項２３に記載の方法。

【請求項２５】

満了時間値をメッセージに割り当てるステップをさらに含み、

前記満了時間値が、経験則によるテストをメッセージコンテンツに適用する結果に基づいて異なることを特徴とする請求項２３に記載の方法。

【請求項２６】

前記隔離終了基準は、前記脅威スコア値を決定するために一つ以上のルールの更新を受信し、前記終了アクションは更新されたルールに基づいて前記メッセージに対する脅威スコア値を再び決定するものであることを特徴とする請求項２３に記載の方法。

【請求項２７】

前記一つ以上の異なる終了アクション群が、異なる隔離終了基準と関連付けられていることを特徴とする請求項２３に記載の方法。

【請求項２８】

ネットワークインターフェース、

該ネットワークインターフェースに接続された一つ以上の処理装置を備えた装置において、

該一つ以上の処理装置に接続されたロジックが、該一つ以上の処理装置によって実行される際に、該一つ以上の処理装置により実行される方法であって、

電子メッセージの特性を規定するルールであって該メッセージと関連付けられた脅威を示す複数のルールを受信しおよび記憶するステップであって、それぞれのルールが優先順位の値を持ち、それぞれのルールがメッセージ要素型と関連付けられているステップ、

受信者アカウントの宛先アドレスを有する、複数のメッセージ要素を含む電子メールメッセージを受信するステップ、

第一のメッセージ要素を抽出するステップ、

前記第一のメッセージ要素のみを、選択されたルールであって前記第一のメッセージ要素に対応するメッセージ要素型を有するルールのみと照合し、かつ、前記選択されたルールの優先順位の順序にしたがって照合することによって、前記メッセージに対する脅威スコア値を決定するステップ、および、

前記脅威スコア値が規定の閾値よりも大きい場合に、前記脅威スコア値を出力するステップ

を有してなる方法。

【請求項２９】

前記脅威スコア値が規定の閾値未満である場合にのみ、他のメッセージ要素を他のルールと照合することによって、前記メッセージに対する更新された脅威スコア値を決定するステップをさらに含むことを特徴とする請求項２８に記載の方法。

【請求項３０】

前記メッセージの本文を解読することによって前記メッセージに対する更新された脅威スコア値を決定するステップ、および、前記脅威スコア値が規定の閾値未満である場合にのみ本文を一つ以上のメール本文ルールと照合するステップをさらに含むことを特徴とする請求項２８に記載の方法。