【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2008-547067(P2008-547067A)
【公表日】平成20年12月25日(2008.12.25)
【年通号数】公開・登録公報2008-051
【出願番号】特願2008-510320(P2008-510320)
【国際特許分類】
Ｇ０６Ｆ　13/00　　(2006.01)
Ｇ０６Ｆ　21/20　　(2006.01)
Ｈ０４Ｌ　12/66　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　13/00　　６１０Ｑ
Ｇ０６Ｆ　15/00　　３３０Ａ
Ｈ０４Ｌ　12/66　　Ｂ

【手続補正書】
【提出日】平成21年5月1日(2009.5.1)
【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】
過去の電子メールメッセージに含まれていた複数の第１のネットワークリソース識別子を備えるホワイトリストを検索するステップと、
前記ホワイトリストから特定の第１のネットワークリソース識別子を検索するステップと、
前記特定の第１のネットワークリソース識別子に対するプロパティの第１のリストを生成するステップと、
前記プロパティを用いて確率フィルタをトレーニングするステップと、
前記ホワイトリスト内の前記第１のネットワークリソース識別子のすべてに対して前記検索、生成およびトレーニングするステップを繰り返すステップと、
スパムまたは脅威に関連する過去の電子メールメッセージに含まれていた複数の第２のネットワークリソース識別子を備えるブロックリストを検索するステップと、
前記ブロックリストから特定の第２のネットワークリソース識別子を検索するステップと、
前記特定の第２のネットワークリソース識別子に対するプロパティの第２のリストを生成するステップと、
前記プロパティを用いて前記確率フィルタをトレーニングするステップと、
前記ブロックリスト内の前記第２のネットワークリソース識別子のすべてに対して前記検索、生成およびトレーニングするステップを繰り返すステップと、
を含むことを特徴とする方法。
【請求項２】
前記プロパティの第２のリストを生成するステップが、
前記第２のネットワークリソース識別子のドメイン部分を抽出するステップと、
ドメインネームシステムから前記抽出されたドメイン部分に関連する１つまたは複数のメール交換記録を検索するステップと、

前記ドメインネームシステムから前記メール交換記録で識別される各メールサーバに対する各アドレス記録を検索するステップと、
前記アドレス記録の各々のネットワークアドレスに関連する評価スコア値を検索するステップと、
平均評価スコア値が規定閾値未満である場合、前記ネットワークリソース識別子をブラックリストに追加するステップと、
を含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記プロパティの第２のリストを生成するステップが、
前記第２のネットワークリソース識別子のドメイン部分を抽出するステップと、
ドメインネームシステムから前記抽出されたドメイン部分に関連する１つまたは複数のネームサーバ記録を検索するステップと、
前記ドメインネームシステムから前記ネームサーバ記録で識別される各メールサーバに対する各アドレス記録を検索するステップと、
前記アドレス記録の各々のネットワークアドレスに関連する評価スコア値を検索するステップと、
平均評価スコア値が規定閾値未満である場合、前記ネットワークリソース識別子をブラックリストに追加するステップと、
を含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記ブラックリストのコピーをメッセージングゲートウェイで受信するステップと、
前記メッセージングゲートウェイで、ユニフォーム・リソース・ロケータ（ＵＲＬ）を含む電子メールメッセージを受信するステップと、
前記ＵＲＬを抽出するとともに、前記ＵＲＬが前記ブラックリストのコピー内にあるかを判断するステップと、
前記ＵＲＬが前記ブラックリストのコピー内にある場合、前記電子メールメッセージに関連する脅威スコア値を変更するステップと、
をさらに含むことを特徴とする請求項２または３に記載の方法。
【請求項５】
前記脅威がウイルス、フィッシング攻撃、およびファーミング攻撃のいずれかを含むことを特徴とする請求項１に記載の方法。
【請求項６】
過去の電子メールメッセージに含まれていた複数の第１のネットワークリソース識別子を備えるホワイトリストを検索する手段と、
前記ホワイトリストから特定の第１のネットワークリソース識別子を検索する手段と、
前記特定の第１のネットワークリソース識別子に対するプロパティの第１のリストを生成する手段と、
前記プロパティを用いて確率フィルタをトレーニングする手段と、
前記ホワイトリスト内の前記第１のネットワークリソース識別子のすべてに対して前記検索、生成およびトレーニング手段の実行を繰り返す手段と、
スパムまたは脅威に関連する過去の電子メールメッセージに含まれていた複数の第２のネットワークリソース識別子を備えるブロックリストを検索する手段と、
前記ブロックリストから特定の第２のネットワークリソース識別子を検索する手段と、
前記特定の第２のネットワークリソース識別子に対するプロパティの第２のリストを生成する手段と、
前記プロパティを用いて前記確率フィルタをトレーニングする手段と、
前記ブロックリスト内の前記第２のネットワークリソース識別子のすべてに対して前記検索、生成およびトレーニングを繰り返す手段と、
を備えることを特徴とする装置。
【請求項７】

前記プロパティの第２のリストを生成する手段が、
前記第２のネットワークリソース識別子のドメイン部分を抽出する手段と、
ドメインネームシステムから前記抽出されたドメイン部分に関連する１つまたは複数のメール交換記録を検索する手段と、
前記ドメインネームシステムから前記メール交換記録で識別される各メールサーバに対する各アドレス記録を検索する手段と、
前記アドレス記録の各々のネットワークアドレスに関連する評価スコア値を検索する手段と、
平均評価スコア値が規定閾値未満である場合、前記ネットワークリソース識別子をブラックリストに追加する手段と、
を備えることを特徴とする請求項６に記載の装置。
【請求項８】
前記プロパティの第２のリストの生成する手段が、
前記第２のネットワークリソース識別子のドメイン部分の抽出する手段と、
ドメインネームシステムからの前記抽出されたドメイン部分に関連する１つまたは複数のネームサーバ記録の検索する手段と、
前記ドメインネームシステムから前記ネームサーバ記録で識別される各メールサーバに対する各アドレス記録の検索する手段と、
前記アドレス記録の各々のネットワークアドレスに関連する評価スコア値の検索する手段と、
平均評価スコア値が規定閾値未満である場合、前記ネットワークリソース識別子のブラックリストへの追加する手段と、
を含むことを特徴とする請求項６に記載の装置。
【請求項９】
前記ブラックリストのコピーをメッセージングゲートウェイで受信する手段と、
前記メッセージングゲートウェイで、ユニフォーム・リソース・ロケータ（ＵＲＬ）を含む電子メールメッセージを受信する手段と、
前記ＵＲＬを抽出するとともに、前記ＵＲＬが前記ブラックリストのコピー内にあるかを判断する手段と、
前記ＵＲＬが前記ブラックリストのコピー内にある場合、前記電子メールメッセージに関連する脅威スコア値を変更する手段と、
をさらに備えることを特徴とする請求項７または８に記載の装置。
【請求項１０】
前記脅威がウイルス、フィッシング攻撃、およびファーミング攻撃のいずれかを含むことを特徴とする請求項６に記載の装置。
【請求項１１】
１つまたは複数のプロセッサと、
実行のために１つまたは複数の媒体に符号化されたロジックと、
を備えた電子メールサーバであって、
前記ロジックは実行された場合、前記１つまたは複数のプロセッサに、
過去の電子メールメッセージに含まれていた複数の第１のネットワークリソース識別子を備えるホワイトリストを検索するステップと、
前記ホワイトリストから特定の第１のネットワークリソース識別子を検索するステップと、
前記特定の第１のネットワークリソース識別子に対するプロパティの第１のリストを生成するステップと、
前記プロパティを用いて確率フィルタをトレーニングするステップと、
前記ホワイトリスト内の前記第１のネットワークリソース識別子のすべてに対して前記検索、生成およびトレーニングするステップを繰り返すステップと、
スパムまたは脅威に関連する過去の電子メールメッセージに含まれていた複数の第２の

ネットワークリソース識別子を備えるブロックリストを検索するステップと、
前記ブロックリストから特定の第２のネットワークリソース識別子を検索するステップと、
前記特定の第２のネットワークリソース識別子に対するプロパティの第２のリストを生成するステップと、
前記プロパティを用いて前記確率フィルタをトレーニングするステップと、
前記ブロックリスト内の前記第２のネットワークリソース識別子のすべてに対して前記検索、生成およびトレーニングするステップを繰り返すステップと、
を行わせるように動作可能であることを特徴とする電子メールサーバ。
【請求項１２】
前記プロパティの第２のリストを生成するロジックがさらなるロジックを備え、前記さらなるロジックは、実行された場合、
前記第２のネットワークリソース識別子のドメイン部分を抽出するステップと、
ドメインネームシステムから前記抽出されたドメイン部分に関連する１つまたは複数のメール交換記録を検索するステップと、
前記ドメインネームシステムから前記メール交換記録で識別される各メールサーバに対する各アドレス記録を検索するステップと、
前記アドレス記録の各々のネットワークアドレスに関連する評価スコア値を検索するステップと、
平均評価スコア値が規定閾値未満である場合、前記ネットワークリソース識別子をブラックリストに追加するステップと、
を行わせるように動作可能であることを特徴とする請求項１１に記載の電子メールサーバ。
【請求項１３】
前記プロパティの第２のリストを生成するロジックがさらなるロジックを備え、前記さらなるロジックは、実行された場合、
前記第２のネットワークリソース識別子のドメイン部分を抽出するステップと、
ドメインネームシステムから前記抽出されたドメイン部分に関連する１つまたは複数のネームサーバ記録を検索するステップと、
前記ドメインネームシステムから前記ネームサーバ記録で識別される各メールサーバに対する各アドレス記録を検索するステップと、
前記アドレス記録の各々のネットワークアドレスに関連する評価スコア値を検索するステップと、
平均評価スコア値が規定閾値未満である場合、前記ネットワークリソース識別子をブラックリストに追加するステップと、
を行わせるように動作可能であることを特徴とする請求項１１に記載の電子メールサーバ。
【請求項１４】
前記ブラックリストのコピーをメッセージングゲートウェイで受信するステップと、
前記メッセージングゲートウェイで、ユニフォーム・リソース・ロケータ（ＵＲＬ）を含む電子メールメッセージを受信するステップと、
前記ＵＲＬを抽出するとともに、前記ＵＲＬが前記ブラックリストのコピー内にあるかを判断するステップと、
前記ＵＲＬが前記ブラックリストのコピー内にある場合、前記電子メールメッセージに関連する脅威スコア値を変更するステップと、
をさらに行われるように動作可能であることを特徴とする請求項１２または１３に記載の電子メールサーバ。
【請求項１５】
前記脅威がウイルス、フィッシング攻撃、およびファーミング攻撃のいずれかを含むことを特徴とする請求項１１に記載の電子メールサーバ。