【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24年7月5日(2012.7.5)

【公表番号】特表2011-523482(P2011-523482A)
【公表日】平成23年8月11日(2011.8.11)
【年通号数】公開・登録公報2011-032
【出願番号】特願2011-510688(P2011-510688)
【国際特許分類】
Ｇ０６Ｆ　21/22　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　9/06　　６６０Ｎ

【手続補正書】
【提出日】平成24年5月17日(2012.5.17)
【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】
マルウェアを検知するためのコンピュータ実施方法であって、
一組の既知のマルウェア定義に基づいたフィルタをクライアント装置においてローカルに格納し、前記一組の既知のマルウェア定義から既知のマルウェア定義のサブセットを前記クライアント装置においてローカルに格納する工程であって、前記サブセットは、前記クライアント装置において検知された前記既知のマルウェア定義に対応するマルウェアの所定の可能性に基づいて選択される、工程と、
入力ファイルが前記一組の既知のマルウェア定義内のマルウェア定義のものと一致する特性を有するかどうかを検知するために前記入力ファイルに前記フィルタを適用する工程と、
前記フィルタを適用する工程に基づく前記マルウェア定義のものと一致する特性を有する前記入力ファイルに応答して、前記マルウェア定義が前記既知のマルウェア定義のサブセット内にローカルに格納されているかどうかを決定する工程と、
前記マルウェア定義のものと一致する特性を有する前記入力ファイルとローカルに格納されていない前記マルウェア定義とに応答して、中央サーバから前記マルウェア定義を取得する工程と、
前記取得したマルウェア定義を使用して前記入力ファイルをスキャンする工程と、
前記スキャンする工程に基づき前記入力ファイルがマルウェアを含むかどうかを判断する工程と、
前記スキャンする工程に基づき前記マルウェアを含まない前記入力ファイルに応答して、前記入力ファイルを特定する報告を前記中央サーバに送信する工程と、
前記報告の応答として、前記スキャンする工程に基づき前記入力ファイルが前記マルウェアを含まないと判断された場合に、前記フィルタの将来のアプリケーションにおいて誤陽性発生の可能性を低減する修正されたフィルタを前記中央サーバから受信する工程と
を含む方法。
【請求項２】
前記マルウェア定義は、前記マルウェアに存在することがわかっている特徴的バイトパターンを含み、
前記入力ファイルをスキャンする工程は、前記特徴的バイトパターンが前記入力ファイ

ルに存在するかどうかを判断する工程を含む、請求項１に記載の方法。
【請求項３】
前記一組の既知のマルウェア定義から前記既知のマルウェア定義のサブセットを前記中央サーバから受信する工程と、
前記フィルタを前記中央サーバから受信する工程と
をさらに含む、請求項１に記載の方法。
【請求項４】
更新された一組の既知のマルウェアに基づき生成された更新フィルタを含む更新を前記中央サーバから受信する工程をさらに含む、請求項１に記載の方法。
【請求項５】
前記フィルタは前記入力ファイルに対するハッシュ関数を計算するようにされたＢｌｏｏｍフィルタを含み、
前記ハッシュ関数の出力は前記入力ファイルが前記一組の既知のマルウェア定義のいずれかと一致する特性を有するかどうかを示す、請求項１に記載の方法。
【請求項６】
前記入力ファイルに前記Ｂｌｏｏｍフィルタを適用する工程は、マルウェアの誤陽性検出を生ずる可能性があるが、誤陰性検出を生ずることができない、請求項５に記載の方法。
【請求項７】
前記フィルタは、
各マルウェア定義毎のハッシュ関数を計算する工程と、
前記ハッシュ関数の出力に基づき前記フィルタを定義する工程と、
に従って生成される、請求項１に記載の方法。
【請求項８】
マルウェアを検知するためのコンピュータプログラム製品であって、
一組の既知のマルウェア定義に基づいたフィルタをクライアント装置においてローカルに格納し、前記一組の既知のマルウェア定義から既知のマルウェア定義のサブセットを前記クライアント装置においてローカルに格納し、前記サブセットは、前記クライアント装置において検知された前記既知のマルウェア定義に対応するマルウェアの所定の可能性に基づいて選択され、
入力ファイルが前記一組の既知のマルウェア定義内のマルウェア定義のものと一致する特性を有するかどうかを検知するために前記入力ファイルに前記フィルタを適用し、
前記フィルタを適用する工程に基づく前記マルウェア定義のものと一致する特性を有する前記入力ファイルに応答して、前記マルウェア定義が前記既知のマルウェア定義のサブセット内にローカルに格納されているかどうかを決定し、
前記マルウェア定義のものと一致する特性を有する前記入力ファイルとローカルに格納されていない前記マルウェア定義とに応答して、中央サーバから前記マルウェア定義を取得し、
前記取得したマルウェア定義を使用して前記入力ファイルをスキャンし、
前記スキャンする工程に基づき前記入力ファイルがマルウェアを含むかどうかを判断し、
前記スキャンする工程に基づき前記マルウェアを含まない前記入力ファイルに応答して、前記入力ファイルを特定する報告を前記中央サーバに送信し、そして
前記報告の応答として、前記スキャンする工程に基づき前記入力ファイルが前記マルウェアを含まないと判断された場合に、前記フィルタの将来のアプリケーションにおいて誤陽性発生の可能性を低減する修正されたフィルタを前記中央サーバから受信する
ためのコンピュータプログラムコードを含む非一時的コンピュータ可読記憶媒体を含む、コンピュータプログラム製品。
【請求項９】
前記マルウェア定義は、前記マルウェアに存在することがわかっている特徴的バイトパ

ターンを含み、
前記入力ファイルをスキャンする工程は、前記特徴的バイトパターンが前記入力ファイルに存在するかどうかを判断する工程を含む、請求項８に記載のコンピュータプログラム製品。
【請求項１０】
前記コンピュータ可読記憶媒体はさらに、
前記一組の既知のマルウェア定義から前記既知のマルウェア定義のサブセットを前記中央サーバから受信し、そして
前記フィルタを前記中央サーバから受信する
ためのコンピュータプログラムコードを含む、請求項８に記載のコンピュータプログラム製品。
【請求項１１】
前記コンピュータ可読記憶媒体はさらに、
更新された一組の既知のマルウェアに基づき生成された更新フィルタを含む更新を前記中央サーバから受信する
ためのコンピュータプログラムコードを含む、請求項８に記載のコンピュータプログラム製品。
【請求項１２】
前記フィルタは前記入力ファイルに対するハッシュ関数を計算するようにされたＢｌｏｏｍフィルタを含み、
前記ハッシュ関数の出力は前記入力ファイルが前記一組の既知のマルウェア定義のいずれかと一致する特性を有するかどうかを示す、請求項８に記載のコンピュータプログラム製品。
【請求項１３】
前記入力ファイルに前記Ｂｌｏｏｍフィルタを適用する工程は、マルウェアの誤陽性検出を生ずる可能性があるが、誤陰性検出を生ずることができない、請求項１２に記載のコンピュータプログラム製品。
【請求項１４】
前記フィルタは、
各マルウェア定義毎のハッシュ関数を計算する工程と、
前記ハッシュ関数の出力に基づき前記フィルタを定義する工程と
に従って生成される、請求項８に記載のコンピュータプログラム製品。
【請求項１５】
クライアント装置にマルウェア定義を配信する方法であって、
一組の既知のマルウェア定義から、入力ファイルが前記一組の既知のマルウェア定義のものと一致する特性を有するかどうかを検知するフィルタを生成する工程と、
前記クライアント装置に前記フィルタを配信する工程と、
前記クライアント装置に配信された前記フィルタを生成するために使用される前記一組の既知のマルウェア定義からマルウェア定義のサブセットを選択する工程であって、前記マルウェアのサブセットは、前記一組の既知のマルウェア定義の全てよりも少なく含み、前記サブセットは、前記クライアント装置において検知された前記既知のマルウェア定義に対応するマルウェアの所定の可能性に基づいて選択される、工程と、
前記選択されたマルウェア定義のサブセットを前記フィルタと共にサーバが前記クライアント装置に配信する工程と、
前記クライアント装置によって前記フィルタが前記入力ファイルに適用された際に、前記クライアントに配信された前記既知のマルウェア定義のサブセット内に存在しないマルウェア定義についての前記クライアント装置からの照会を受信する工程と、
前記照会に応答して、前記入力ファイルのスキャンに利用される、前記照会されたマルウェア定義を前記クライアント装置に送信する工程と、
前記照会されたマルウェア定義は前記入力ファイルに存在しないことを示す報告を前記

クライアント装置から受信する工程と、
前記報告の受信に応答して、前記フィルタの将来のアプリケーションにおいて誤陽性発生の可能性を低減するために前記フィルタを修正し、前記修正されたフィルタを前記クライアント装置に送信する工程と、
を含む方法。
【請求項１６】
前記クライアント装置からのマルウェア定義の照会の頻度に基づき前記クライアント装置に配信すべき前記既知のマルウェア定義のサブセットを更新する工程、をさらに含む、請求項１５に記載の方法。
【請求項１７】
前記フィルタは、前記入力ファイルに対しハッシュ関数を計算するようにされたＢｌｏｏｍフィルタを含み、
前記ハッシュ関数の出力は、前記入力ファイルが前記一組の既知のマルウェア定義のいずれかと一致する特性を有するかどうかを示す、請求項１５に記載の方法。
【請求項１８】
前記一組の既知のマルウェア定義は、前記クライアント装置において最も検知される可能性が高いマルウェア定義を含む、請求項１に記載の方法。
【請求項１９】
前記一組の既知のマルウェア定義は、前記クライアント装置において最も検知される可能性が高いマルウェア定義を含む、請求項８に記載のコンピュータプログラム製品。
【請求項２０】
前記マルウェア定義のサブセットは、前記クライアント装置において最も検知される可能性が高いマルウェア定義を含む、請求項１５に記載の方法。