【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】令和1年8月15日(2019.8.15)

【公表番号】特表2018-538633(P2018-538633A)
【公表日】平成30年12月27日(2018.12.27)
【年通号数】公開・登録公報2018-050
【出願番号】特願2018-532300(P2018-532300)
【国際特許分類】
Ｇ０６Ｆ　21/56　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/56

【手続補正書】
【提出日】令和1年7月3日(2019.7.3)
【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】
ハイパーバイザと、ライブイントロスペクションエンジンと、オンデマンドイントロスペクションエンジンとを実行するように構成されたハードウェアプロセッサを含むクライアントコンピュータシステムであって、
前記ハイパーバイザは、ゲスト仮想マシン（ＶＭ）と、前記ゲストＶＭとは別個のセキュリティＶＭとを公開するように構成され、前記オンデマンドイントロスペクションエンジンは前記セキュリティＶＭ内で実行され、前記ライブイントロスペクションエンジンは前記ゲストＶＭと前記セキュリティＶＭとの外部で実行され、
前記ライブイントロスペクションエンジンは、前記ゲストＶＭ内でのイベントの発生を検出するのに応答して、前記イベントのインジケータをリモートサーバコンピュータシステムに通信ネットワークを介して送信するように構成され、
前記オンデマンドイントロスペクションエンジンは、
前記ライブイントロスペクションエンジンが前記イベントの前記インジケータを前記リモートサーバコンピュータシステムに送信するのに応答して、分析要求を前記リモートサーバコンピュータシステムから受信することであって、前記分析要求は、前記クライアントコンピュータシステムを含む複数のクライアントにセキュリティツールを配信するように構成されたリモートツールリポジトリにあるセキュリティツールを示し、前記セキュリティツールは、前記イベントの前記発生を分析するように構成されたソフトウェアを含み、前記セキュリティツールは、前記リモートサーバコンピュータシステムによって前記イベントのイベントタイプに従って選択される、受信することと、
前記分析要求を受信するのに応答して、前記セキュリティツールを前記分析要求に従って識別することと、
前記セキュリティツールを識別するのに応答して、前記セキュリティツールを前記リモートツールリポジトリから選択的に取り出すことであって、前記セキュリティツールを取り出すことは、前記リモートツールリポジトリに前記通信ネットワークを介して接続することを含む、取り出すことと、
前記セキュリティツールを選択的に取り出すのに応答して、前記セキュリティツールを実行することと、
前記セキュリティツールを実行するのに応答して、前記セキュリティツールの実行の

結果を前記リモートサーバコンピュータシステムに送信することと
を行うように構成された、
クライアントコンピュータシステム。
【請求項２】
請求項１に記載のクライアントコンピュータシステムであって、前記リモートサーバコンピュータシステムは、前記クライアントコンピュータシステムが悪意のあるソフトウェアを含むかどうかを前記結果に従って判断するようにさらに構成された、クライアントコンピュータシステム。
【請求項３】
請求項１に記載のクライアントコンピュータシステムであって、前記リモートサーバコンピュータシステムは、前記クライアントコンピュータシステムの悪意のある侵入を前記結果に従って検出するようにさらに構成された、クライアントコンピュータシステム。
【請求項４】
請求項１に記載のクライアントコンピュータシステムであって、前記オンデマンドイントロスペクションエンジンは、
前記結果を前記リモートサーバコンピュータシステムに送信するのに応答して、前記リモートサーバコンピュータシステムから前記リモートツールリポジトリにある緩和ツールのインジケータを受信することであって、前記緩和ツールは、前記クライアントコンピュータシステム上で実行される悪意のあるソフトウェアを無能力化するように構成されたソフトウェア含む、受信することと、
前記緩和ツールの前記インジケータを受信するのに応答して、前記緩和ツールを取り出し、実行することと
を行うようにさらに構成された、クライアントコンピュータシステム。
【請求項５】
請求項１に記載のクライアントコンピュータシステムであって、前記ライブイントロスペクションエンジンは、
前記イベントの前記発生を検出するのに応答して、前記イベントのイベントタイプに従って、イベント適格性条件が満たされるかどうかを判断することと、
前記イベントの前記インジケータを前記リモートサーバコンピュータシステムに、前記イベント適格性条件が満たされたときのみ送信することと
を行うようにさらに構成された、クライアントコンピュータシステム。
【請求項６】
請求項１に記載のクライアントコンピュータシステムであって、前記セキュリティツールを前記リモートツールリポジトリから取り出すことは、前記リモートツールリポジトリを前記セキュリティＶＭのファイルシステムにマウントすることを含む、クライアントコンピュータシステム。
【請求項７】
請求項１に記載のクライアントコンピュータシステムであって、前記セキュリティＶＭはネットワークフィルタをさらに含み、前記ハイパーバイザは、前記ゲストＶＭとリモートパーティとの間のネットワークトラフィックを、前記ネットワークフィルタを介してルーティングするようにさらに構成された、クライアントコンピュータシステム。
【請求項８】
請求項７に記載のクライアントコンピュータシステムであって、
前記リモートサーバコンピュータシステムは、前記クライアントコンピュータシステムが悪意のあるソフトウェアを含むかどうかを判断するのに応答して、前記クライアントコンピュータシステムが悪意のあるソフトウェアを含むときに、セキュリティアラートを前記クライアントコンピュータシステムに送るようにさらに構成され、
前記ネットワークフィルタは、前記クライアントコンピュータシステムが前記セキュリティアラートを受信するのに応答して、前記ゲストＶＭと前記リモートパーティとの間のネットワークトラフィックを制限するように構成された、

クライアントコンピュータシステム。
【請求項９】
請求項１に記載のクライアントコンピュータシステムであって、前記セキュリティツールの実行の前記結果は、前記ゲストＶＭによって使用されたメモリのセクションのコンテンツのコピーを含む、クライアントコンピュータシステム。
【請求項１０】
請求項１に記載のクライアントコンピュータシステムであって、前記セキュリティツールの実行の前記結果は、前記ゲストＶＭ内で実行されるソフトウェアエンティティのリストを含む、クライアントコンピュータシステム。
【請求項１１】
請求項１に記載のクライアントコンピュータシステムであって、前記セキュリティツールの実行の前記結果は、前記クライアントコンピュータシステムのハードウェア構成のインジケータを含む、クライアントコンピュータシステム。
【請求項１２】
請求項１に記載のクライアントコンピュータシステムであって、
前記ハイパーバイザは、前記リモートサーバコンピュータシステムと前記セキュリティＶＭとの間にセキュアなポイントツーポイント通信チャネルを確立するように構成され、
前記オンデマンドイントロスペクションエンジンは、前記セキュアなポイントツーポイント通信チャネルを介して、前記分析要求を受信し、前記結果を送信するように構成された、
クライアントコンピュータシステム。
【請求項１３】
複数のクライアントシステムとのコンピュータセキュリティトランザクションを実施するように構成されたサーバコンピュータシステムであって、前記サーバコンピュータシステムは、ハードウェアプロセッサを含み、該ハードウェアプロセッサは、
前記複数のクライアントシステムのうちの１つのクライアントシステムから、前記１つのクライアントシステム上で実行されるゲスト仮想マシン（ＶＭ）内でのイベントの発生を示すイベントインジケータを受信するのに応答して、前記複数のクライアントシステムにセキュリティツールを配信するように構成されたリモートツールリポジトリにあるセキュリティツールを選択することであって、前記セキュリティツールは、前記イベントの前記発生を分析するように構成されたソフトウェアを含み、前記セキュリティツールを選択することは、前記イベントのイベントタイプに従って実施される、選択することと、
前記セキュリティツールを選択するのに応答して、分析要求を前記１つのクライアントシステムに通信ネットワークを介して送信することであって、前記分析要求は前記セキュリティツールの識別子を含む、送信することと、
前記セキュリティツールの前記識別子を含む前記分析要求を送信するのに応答して、前記１つのクライアントシステムから、前記セキュリティツールを前記１つのクライアントシステム上で実行した結果を受信することと
を行うように構成され、
前記１つのクライアントシステムは、ハイパーバイザと、ライブイントロスペクションエンジンと、オンデマンドイントロスペクションエンジンとを実行するように構成され、
前記ハイパーバイザは、前記ゲストＶＭと、前記ゲストＶＭとは別個のセキュリティＶＭとを公開するように構成され、前記オンデマンドイントロスペクションエンジンは前記セキュリティＶＭ内で実行され、前記ライブイントロスペクションエンジンは前記ゲストＶＭと前記セキュリティＶＭとの外部で実行され、
前記ライブイントロスペクションエンジンは、前記イベントの前記発生を検出するのに応答して、前記イベントインジケータを前記サーバコンピュータシステムに送信するように構成され、
前記オンデマンドイントロスペクションエンジンは、
前記分析要求を受信するのに応答して、前記セキュリティツールを前記分析要求に

従って識別することと、
前記セキュリティツールを識別するのに応答して、前記セキュリティツールを前記リモートツールリポジトリから選択的に取り出すことであって、前記セキュリティツールを取り出すことは、前記１つのクライアントシステムが前記リモートツールリポジトリに前記通信ネットワークを介して接続することを含む、取り出すことと、
前記セキュリティツールを取り出すのに応答して、前記結果を生成するために前記セキュリティツールを実行することと
を行うように構成された、
サーバコンピュータシステム。
【請求項１４】
請求項１３に記載のサーバコンピュータシステムであって、前記ハードウェアプロセッサは、前記１つのクライアントシステムが悪意のあるソフトウェアを含むかどうかを前記結果に従って判断するようにさらに構成された、サーバコンピュータシステム。
【請求項１５】
請求項１３に記載のサーバコンピュータシステムであって、前記ハードウェアプロセッサは、前記１つのクライアントシステムの悪意のある侵入を前記結果に従って検出するようにさらに構成された、サーバコンピュータシステム。
【請求項１６】
請求項１３に記載のサーバコンピュータシステムであって、前記ハードウェアプロセッサは、
前記１つのクライアントシステムが悪意のあるソフトウェアを含むかどうかを判断するのに応答して、前記１つのクライアントシステムが悪意のあるソフトウェアを含むときに、緩和ツールを前記リモートツールリポジトリから選択することであって、前記緩和ツールは、前記悪意のあるソフトウェアを無能力化するように構成されたソフトウェアを含む、選択することと、
前記緩和ツールを選択するのに応答して、前記緩和ツールのインジケータを前記１つのクライアントシステムに送信することと
を行うようにさらに構成された、サーバコンピュータシステム。
【請求項１７】
請求項１３に記載のサーバコンピュータシステムであって、前記ライブイントロスペクションエンジンは、
前記イベントの前記発生を検出するのに応答して、前記イベントのイベントタイプに従って、イベント適格性条件が満たされるかどうかを判断することと、
前記イベントインジケータを前記サーバコンピュータシステムに前記イベント適格性条件が満たされたときのみ送信することと
を行うようにさらに構成された、サーバコンピュータシステム。
【請求項１８】
請求項１３に記載のサーバコンピュータシステムであって、前記セキュリティツールを前記リモートツールリポジトリから取り出すことは、前記リモートツールリポジトリを前記セキュリティＶＭのファイルシステムにマウントすることを含む、サーバコンピュータシステム。
【請求項１９】
請求項１３に記載のサーバコンピュータシステムであって、前記セキュリティＶＭはネットワークフィルタをさらに含み、前記ハイパーバイザは、前記ゲストＶＭとリモートパーティとの間のネットワークトラフィックを、前記ネットワークフィルタを介してルーティングするようにさらに構成された、サーバコンピュータシステム。
【請求項２０】
請求項１９に記載のサーバコンピュータシステムであって、前記ハードウェアプロセッサは、前記１つのクライアントシステムが悪意のあるソフトウェアを含むかどうかを判断するのに応答して、前記１つのクライアントシステムが悪意のあるソフトウェアを含むとき

に、セキュリティアラートを前記１つのクライアントシステムに送るようにさらに構成され、前記１つのクライアントシステムによる前記セキュリティアラートの受信が、前記ネットワークフィルタに前記ゲストＶＭと前記リモートパーティとの間のネットワークトラフィックを制限させる、サーバコンピュータシステム。
【請求項２１】
請求項１３に記載のサーバコンピュータシステムであって、前記セキュリティツールの実行の前記結果は、前記ゲストＶＭによって使用されたメモリのセクションのコンテンツのコピーを含む、サーバコンピュータシステム。
【請求項２２】
請求項１３に記載のサーバコンピュータシステムであって、前記セキュリティツールの実行の前記結果は、前記ゲストＶＭ内で実行されるソフトウェアエンティティのリストを含む、サーバコンピュータシステム。
【請求項２３】
請求項１３に記載のサーバコンピュータシステムであって、前記セキュリティツールの実行の前記結果は、前記クライアントシステムのハードウェア構成のインジケータを含む、サーバコンピュータシステム。
【請求項２４】
請求項１３に記載のサーバコンピュータシステムであって、
前記ハイパーバイザは、前記サーバコンピュータシステムと前記セキュリティＶＭとの間にセキュアなポイントツーポイント通信チャネルを確立するように構成され、
前記ハードウェアプロセッサは、前記セキュアなポイントツーポイント通信チャネルを介して、前記セキュリティツールの前記識別子を含む前記分析要求を送り、前記セキュリティツールの実行の前記結果を受信するようにさらに構成された、
サーバコンピュータシステム。
【請求項２５】
命令のセットを記憶した非一時的コンピュータ可読媒体であって、命令の前記セットは、クライアントコンピュータシステムのハードウェアプロセッサ上で実行されたときに、前記クライアントコンピュータシステムに、ハイパーバイザと、ライブイントロスペクションエンジンと、オンデマンドイントロスペクションエンジンとを形成させ、
前記ハイパーバイザは、ゲスト仮想マシン（ＶＭ）と、前記ゲストＶＭとは別個のセキュリティＶＭとを公開するように構成され、前記オンデマンドイントロスペクションエンジンは前記セキュリティＶＭ内で実行され、前記ライブイントロスペクションエンジンは前記ゲストＶＭと前記セキュリティＶＭとの外部で実行され、
前記ライブイントロスペクションエンジンは、前記ゲストＶＭ内でのイベントの発生を検出するのに応答して、前記イベントのインジケータをリモートサーバコンピュータシステムに通信ネットワークを介して送信するように構成され、
前記オンデマンドイントロスペクションエンジンは、
前記ライブイントロスペクションエンジンが前記イベントの前記インジケータを前記リモートサーバコンピュータシステムに送信するのに応答して、分析要求を前記リモートサーバコンピュータシステムから受信することであって、前記分析要求は、前記クライアントコンピュータシステムを含む複数のクライアントにセキュリティツールを配信するように構成されたリモートツールリポジトリにあるセキュリティツールを示し、前記セキュリティツールは、前記イベントの前記発生を分析するように構成されたソフトウェアを含み、前記セキュリティツールは、前記リモートサーバコンピュータシステムによって前記イベントのイベントタイプに従って選択される、受信することと、
前記分析要求を受信するのに応答して、前記セキュリティツールを前記分析要求に従って識別することと、
前記セキュリティツールを識別するのに応答して、前記セキュリティツールを前記リモートツールリポジトリから選択的に取り出すことであって、前記セキュリティツールを取り出すことは、前記リモートツールリポジトリに前記通信ネットワークを介して接続す

ることを含む、取り出すことと、
前記セキュリティツールを選択的に取り出すのに応答して、前記セキュリティツールを実行することと、
前記セキュリティツールを実行するのに応答して、前記セキュリティツールの実行の結果を前記リモートサーバコンピュータシステムに送信することと
を行うように構成された、
非一時的コンピュータ可読媒体。