【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28年9月1日(2016.9.1)

【公表番号】特表2016-514295(P2016-514295A)
【公表日】平成28年5月19日(2016.5.19)
【年通号数】公開・登録公報2016-030
【出願番号】特願2015-557980(P2015-557980)
【国際特許分類】
Ｇ０６Ｆ　21/55　(2013.01)
Ｈ０４Ｌ　12/70　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/55　３４０
Ｈ０４Ｌ　12/70　１００Ｚ

【手続補正書】
【提出日】平成28年7月13日(2016.7.13)
【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】
コンピュータデバイス上で第１のコンテキスト内で実行中のアプリケーションに対してネットワークポリシーを実施する方法であって、
前記第１のコンテキストのネットワークソケットを通じたデータフローについての統計を収集すること、
前記収集した統計に基づいて前記ネットワークポリシーを変更すること、
前記第１のコンテキスト内で実行中のエージェントにより、前記アプリケーションからのネットワークソケットイベント要求を、前記ネットワークソケットイベント要求が前記第１のコンテキストのネットワークスタック内のトランスポート層に到達する前にインターセプトすること、
前記エージェントにより、第２のコンテキスト内で実行中のセキュリティサーバに、前記インターセプトされたネットワークソケットイベント要求を許可するか拒絶するかについての判断についての要求を送信することであって、前記判断についての要求はアプリケーション識別子と前記アプリケーションのドメインとを含む、前記判断についての要求を送信すること、
前記エージェントにより、前記セキュリティサーバから前記ネットワークソケットイベント要求の許可又は拒絶を示す判断を受信することであって、前記アプリケーション識別子の指示、前記アプリケーションのドメイン、及び前記変更されたネットワークポリシーに少なくとも部分的に基づく当該判断を受信すること、
前記判断が前記ネットワークソケットイベント要求の拒絶である場合、前記エージェントにより、前記ネットワークソケットイベント要求が前記第１のコンテキスト内の前記トランスポート層に到達することを阻止すること、
を備える方法。
【請求項２】
前記アプリケーション識別子は、前記第１のコンテキストの前記トランスポート層のインタフェースから受信されたデータに基づく、請求項１に記載の方法。
【請求項３】

前記判断が前記ネットワークソケットイベント要求の許可である場合、前記ネットワークソケットイベント要求を前記第１のコンテキスト内の前記アプリケーションから前記第１のコンテキスト内の前記トランスポート層に送信することを更に備える請求項１に記載の方法。
【請求項４】
前記セキュリティサーバは、複数のコンテキスト内のネットワークソケットイベント要求を許可するか拒絶するかについての判断を行う、請求項１に記載の方法。
【請求項５】
前記第１のコンテキストからの前記ネットワークソケットを通じたデータフローについての前記統計を、複数のコンテキストの複数のネットワークソケットを通じたデータフローについての統計を受信するデータ収集モジュールに送信すること、
前記複数のコンテキストの前記複数のネットワークソケットを通じた前記データフローについての前記統計のリポートを生成すること、
を更に備える請求項１に記載の方法。
【請求項６】
前記ネットワークソケットイベント要求は、前記ネットワークソケットをオープンすること、クローズすること、及びリッスンすることのうちの何れかである、請求項１に記載の方法。
【請求項７】
前記アプリケーション識別子は、（ｉ）オペレーティングシステムが前記アプリケーションの実行可能ファイルをロードし実行する場合に作成されるプロセスを識別するとともに（ｉｉ）前記アプリケーションの実行可能ファイルを識別するプロセス識別子に少なくとも基づく、請求項１に記載の方法。
【請求項８】
前記アプリケーション識別子の指示は、前記アプリケーションの実行可能ファイルのファイル名に少なくとも基づく、請求項１に記載の方法。
【請求項９】
前記アプリケーション識別子の指示は、前記アプリケーションの実行可能ファイルのハッシュに少なくとも基づく、請求項１に記載の方法。
【請求項１０】
前記トランスポート層のインタフェースは前記ネットワークソケットイベント要求をインターセプトし、前記インタフェースはトランスポートドライバインタフェースである、請求項１に記載の方法。
【請求項１１】
前記トランスポート層のインタフェースが前記ネットワークソケットイベント要求をインターセプトする、請求項１に記載の方法。
【請求項１２】
コンテキストによって実行可能なコンピュータ可読命令を備えた非一時的コンピュータ可読媒体であって、
第１のコンテキストのネットワークソケットを通じたデータフローについての統計を収集することを実行する命令であって、アプリケーション当たり、ユーザ当たり、仮想マシン当たりのバイト数／パケット数として、ネットワークフロー情報を示す当該統計を収集することを実行する命令と、
前記収集した統計に基づいてネットワークポリシーを変更することを実行する命令と、
第１のコンテキスト内で実行中のエージェントにより、アプリケーションからのネットワークソケットイベント要求を、前記ネットワークソケットイベント要求が前記第１のコンテキストのネットワークスタック内のトランスポート層に到達する前にインターセプトすることを実行する命令と、
前記エージェントにより、第２のコンテキスト内で実行中のセキュリティサーバに、前記インターセプトされたネットワークソケットイベント要求を許可するか拒絶するかにつ

いての判断についての要求を送信することを実行する命令であって、前記判断についての要求はアプリケーション識別子と前記アプリケーションのドメインとを含む、前記判断についての要求を送信することを実行する命令と、
前記エージェントにより、前記セキュリティサーバから前記ネットワークソケットイベント要求の許可又は拒絶を示す判断を受信することを実行する命令であって、前記アプリケーション識別子の指示、前記アプリケーションのドメイン、及び前記変更されたネットワークポリシーに少なくとも部分的に基づく当該判断を受信することを実行する命令と、
前記判断が前記ネットワークソケットイベント要求の拒絶である場合、前記エージェントにより、前記ネットワークソケットイベント要求が前記第１のコンテキスト内の前記トランスポート層に到達することを阻止するように実行する命令と、
を備える非一時的コンピュータ可読媒体。
【請求項１３】
前記アプリケーション識別子は、前記第１のコンテキストの前記トランスポート層のインタフェースから受信されたデータに基づく、請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項１４】
前記ネットワークソケットイベント要求を前記第１のコンテキスト内の前記アプリケーションから前記第１のコンテキスト内の前記トランスポート層に送信する命令を更に備える請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項１５】
前記セキュリティサーバは、複数のコンテキスト内のネットワークソケットイベント要求を許可するか拒絶するかについての判断を行う、請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項１６】
前記第１のコンテキストからの前記統計を、複数のコンテキストの複数のネットワークソケットを通じたデータフローについての統計を受信するデータ収集モジュールに送信する命令と、
前記複数のコンテキストの前記複数のネットワークソケットを通じた前記データフローについての前記統計のリポートを生成する命令と、
を更に備える請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項１７】
前記ネットワークソケットイベント要求は、前記ネットワークソケットをオープンすること、クローズすること、及びリッスンすることのうちの何れかである、請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項１８】
前記アプリケーション識別子は、（ｉ）オペレーティングシステムが前記アプリケーションの実行可能ファイルをロードし実行する場合に作成されるプロセスを識別するとともに（ｉｉ）前記アプリケーションの実行可能ファイルを識別するプロセス識別子に少なくとも基づく、請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項１９】
前記アプリケーション識別子の指示は、前記アプリケーションの実行可能ファイルのファイル名に少なくとも基づく、請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項２０】
前記アプリケーション識別子の指示は、前記アプリケーションの実行可能ファイルのハッシュに少なくとも基づく、請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項２１】
前記トランスポート層のインタフェースは前記ネットワークソケットイベント要求をインターセプトし、前記インタフェースはトランスポートドライバインタフェースである、請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項２２】

前記トランスポート層のインタフェースが前記ネットワークソケットイベント要求をインターセプトする、請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項２３】
プロセッサと、コンテキストを有するメモリとを備えるコンピュータシステムであって、
前記コンテキストは、
第１のコンテキストのネットワークソケットを通じたデータフローについての統計を収集することを実行する命令であって、アプリケーション当たり、ユーザ当たり、仮想マシン当たりのバイト数／パケット数として、ネットワークフロー情報を示す当該統計を収集することを実行する命令と、
前記収集した統計に基づいてネットワークポリシーを変更することを実行する命令と、
第１のコンテキスト内で実行中のエージェントにより、アプリケーションからのネットワークソケットイベント要求を、前記ネットワークソケットイベント要求が前記第１のコンテキストのネットワークスタック内のトランスポート層に到達する前にインターセプトすることを実行する命令と、
前記エージェントにより、第２のコンテキスト内で実行中のセキュリティサーバに、前記インターセプトされたネットワークソケットイベント要求を許可するか拒絶するかについての判断についての要求を送信することを実行する命令であって、前記判断についての要求はアプリケーション識別子と前記アプリケーションのドメインとを含む、前記判断についての要求を送信することを実行する命令と、
前記エージェントにより、前記セキュリティサーバから前記ネットワークソケットイベント要求の許可又は拒絶を示す判断を受信することを実行する命令であって、前記アプリケーション識別子の指示、前記アプリケーションのドメイン、及び前記変更されたネットワークポリシーに少なくとも部分的に基づく当該判断を受信することを実行する命令と、
前記判断が前記ネットワークソケットイベント要求の拒絶である場合、前記エージェントにより、前記ネットワークソケットイベント要求が前記第１のコンテキスト内の前記トランスポート層に到達することを阻止することを実行する命令と、
を実行する、コンピュータシステム。