

【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11月10日 (2016.11.10)

【公表番号】特表2016-526226(P2016-526226A)

【公表日】平成28年9月1日 (2016.9.1)

【年通号数】公開・登録公報2016-052

【出願番号】特願2016-516500(P2016-516500)

【国際特許分類】

G 0 6 F 21/53 (2013.01)

H 0 4 M 3/42 (2006.01)

G 0 6 F 21/62 (2013.01)

G 0 6 F 21/12 (2013.01)

【F I】

G 0 6 F 21/53

H 0 4 M 3/42 Z

G 0 6 F 21/62

G 0 6 F 21/12 3 1 0

【手続補正書】

【提出日】平成28年9月20日 (2016.9.20)

【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】

コンピューティングデバイスが実施する方法であって、

ドライバークセキュリティプラットフォームに関連する指定されたフォーマットを有するドライバークパッケージに含まれるトランスモグリファイイング・ドライバークを取得するステップと、

インストールの際に、前記ドライバークパッケージの前記指定されたフォーマットを、前記ドライバークパッケージとともに含まれる識別データに少なくとも部分的に基づいて認識するステップと、

前記認識に回答して、前記トランスモグリファイイング・ドライバークを、前記コンピューティングデバイスによって実施される前記ドライバークセキュリティプラットフォームに登録するステップと、

前記ドライバークセキュリティプラットフォームを介して前記トランスモグリファイイング・ドライバークのための制限された実行環境をインスタンス化するステップと、

前記ドライバークセキュリティプラットフォームの指示で 1 つまたは複数のタスクを実行するように前記制限された実行環境内で前記トランスモグリファイイング・ドライバークを実行するステップと

を含む方法。

【請求項 2】

請求項 1 に記載の方法であって、前記トランスモグリファイイング・ドライバークは、ユーザーモードで実行される、方法。

【請求項 3】

請求項 1 に記載の方法であって、前記トランスモグリファイイング・ドライバークは、ユーザーごとに実行される、方法。

**【請求項 4】**

請求項 1 に記載の方法であって、前記制限された実行環境はアプリケーションコンテナを確立し、前記アプリケーションコンテナは、前記トランスモグリファイイング・ドライバーを隔離して、システムリソースに対する前記トランスモグリファイイング・ドライバーによるアクセスを制限するように構成された、方法。

**【請求項 5】**

請求項 4 に記載の方法であって、前記アプリケーションコンテナは、コンポーネントによる前記トランスモグリファイイング・ドライバーに対するアクセスを拒否するようにさらに構成され、前記コンポーネントは、前記ドライバーセキュリティプラットフォームに関連付けられていないものである、方法。

**【請求項 6】**

請求項 1 に記載の方法であって、前記制限された実行環境は、前記ドライバーセキュリティプラットフォームによってタスクのスケジューリングが扱われる前記トランスモグリファイイング・ドライバーのための背景プロセスを含む、方法。

**【請求項 7】**

請求項 1 に記載の方法であって、前記制限された実行環境は、前記ドライバーセキュリティプラットフォームによる、タスクを実行するための前記トランスモグリファイイング・ドライバーの明示的な呼び出しがない場合に、前記トランスモグリファイイング・ドライバーを一時停止するように構成された、方法。

**【請求項 8】**

請求項 1 に記載の方法であって、前記制限された実行環境は、ユーザー同意に依存して前記トランスモグリファイイング・ドライバーの動作を選択的に可能にするように構成された、方法。

**【請求項 9】**

請求項 1 に記載の方法であって、前記トランスモグリファイイング・ドライバーは、ネットワークを介してサービスプロバイダーのアプリケーションストアから取得される、方法。

**【請求項 10】**

請求項 1 に記載の方法であって、前記トランスモグリファイイング・ドライバーは、ある形態から別の形態へデータを変換するように構成された、方法。

**【請求項 11】**

請求項 1 に記載の方法であって、前記ドライバーセキュリティプラットフォームは、前記コンピューティングデバイスのためのオペレーティングシステムのコンポーネントとして実施される、方法。

**【請求項 12】**

請求項 1 に記載の方法であって、前記トランスモグリファイイング・ドライバーは仮想プライベートネットワーク（VPN）ドライバーを含み、前記仮想プライベートネットワーク（VPN）ドライバーは、ネットワークを介した VPN 通信のためにパケットのカプセル化およびカプセル化解除を行うように構成された、方法。

**【請求項 13】**

コンピューティングデバイスをドライバーセキュリティプラットフォームとして機能させるプログラムであって、前記ドライバーセキュリティプラットフォームは動作を実行するように構成され、該動作は、

ドライバーセキュリティプラットフォームに関連する指定されたフォーマットを有するドライバーパッケージに含まれるトランスモグリファイイング・ドライバーを取得する動作と、

前記トランスモグリファイイング・ドライバーと前記ドライバーセキュリティプラットフォームとの関連付けを、前記ドライバーパッケージとともに含まれる識別データに少なくとも部分的に基づいて認識する動作と、

前記認識に応答して、前記ドライバーセキュリティプラットフォームを介して前記トラ

ンスモグリファイイング・ドライバーのために可能にされたタスクのセットを確かめる動作と、

前記トランスモグリファイイング・ドライバーの動作を、前記ドライバーセキュリティプラットフォームを介して可能にされたタスクの前記セットに制限する実行環境を確立する動作と、

前記トランスモグリファイイング・ドライバーの動作を可能にされたタスクの前記セットに制限する前記実行環境を介して、前記トランスモグリファイイング・ドライバーの動作を制御する動作と

を含む、プログラム。

【請求項 14】

請求項 13 に記載のプログラムであって、

前記トランスモグリファイイング・ドライバーは仮想プライベートネットワーク（VPN）ドライバーを含み、

前記 VPN ドライバーのために前記ドライバーセキュリティプラットフォームを介して可能にされたタスクの前記セットは、ネットワークを介した VPN サーバーとの VPN 通信に関連する、接続、切断、カプセル化及びカプセル化解除のタスクに制限される、方法。

【請求項 15】

請求項 13 に記載のプログラムであって、前記トランスモグリファイイング・ドライバーの前記動作を制御する動作は、

可能にされたタスクの前記セットの実行のために、前記トランスモグリファイイング・ドライバーを呼び出す動作と、

前記プラットフォームによるタスクを実行する指示がない場合に、前記トランスモグリファイイング・ドライバーを一時停止する動作と

を含む、プログラム。

【請求項 16】

請求項 13 に記載のプログラムであって、前記トランスモグリファイイング・ドライバーの前記動作を制御する動作は、タスクの前記セットを、前記ドライバーセキュリティプラットフォームにより仲介される背景タスクとしてスケジューリングする動作を含む、プログラム。

【請求項 17】

請求項 13 に記載のプログラムであって、前記実行環境は、サンドボックス化されたアプリケーションコンテナを含み、該サンドボックス化されたアプリケーションコンテナは、ユーザーモードにおいてユーザーごとに実行され、可能にされたタスクの前記セットに関するものを除き、システムアクセスを防ぐように構成された低特権トークンを割り当てられた、プログラム。

【請求項 18】

1 以上の処理コンポーネントと、

前記 1 以上の処理コンポーネントをドライバーセキュリティプラットフォームとして機能させる命令を記憶した 1 以上のコンピューター可読記憶媒体と

を備えたコンピューティングシステムであって、前記ドライバーセキュリティプラットフォームは、少なくとも 1 つの VPN ドライバーの動作を制限し、

ドライバーマネージャーモジュールであって、

前記ドライバーマネージャーモジュールは、前記 VPN ドライバーをネットワークを介してサービスプロバイダーのアプリケーションストアから取得し、前記 VPN ドライバーは、前記ドライバーセキュリティプラットフォームに関連する指定されたフォーマットを有するドライバーパッケージに含まれ、

前記ドライバーマネージャーモジュールは、インストールの際に、前記ドライバーパッケージの前記指定されたフォーマットを、前記ドライバーパッケージとともに含まれる識別データに少なくとも部分的に基づいて認識し、前記識別データは識別子、コード又は

ファイル拡張子を含み、

前記認識に応答して、前記ドライバーマネージャモジュールは、前記VPNドライバーを含むようにアプリケーションコンテナを確立し、該アプリケーションコンテナは、ユーザーモードにおいてユーザーごとに実行され、タスクの定められたセットに関するものを除き、システムアクセスを防ぐように構成された低特権トークンを割り当てられ、タスクの前記定められたセットは、前記VPNドライバーのために前記ドライバーセキュリティプラットフォームにより明示的に可能にされた、

前記ドライバーマネージャモジュールと、

背景マネージャであって、

前記VPNドライバーを含む前記アプリケーションコンテナのために背景プロセスをインスタンス化し、

前記背景プロセスを介してタスクの前記定められたセットのスケジューリングを扱い、

タスクの前記定められたセットが前記ドライバーマネージャモジュールの指示で実行されるとき以外、前記背景プロセスを一時停止する

前記背景マネージャと、

前記背景マネージャモジュールを介してスケジュールされたタスクを実行するように、前記VPNドライバーとシステムサービスとの間の対話を仲介するイベントを生成するイベントブローカーと

を含む、コンピューティングシステム。

【請求項 19】

請求項 18 に記載のコンピューティングシステムであって、前記イベントブローカーにより生成される前記イベントは、前記コンピューティングシステムを介してさらされるユーザーインターフェース (UI) コンポーネントとの対話の仲介のための UI イベントを含む、コンピューティングシステム。

【請求項 20】

請求項 18 に記載のコンピューティングシステムであって、前記VPNドライバーのために前記ドライバーセキュリティプラットフォームにより明示的に可能にされたタスクの前記定められたセットは、ネットワークを介したVPNサーバーとのVPN通信に関連する、接続、切断、カプセル化及びカプセル化解除のタスクのうちの 1 以上を含む、コンピューティングシステム。

【請求項 21】

請求項 13 から 17 のうちの何れか一項に記載のプログラムを記憶した 1 以上のコンピューター可読記憶媒体。