【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10月24日(2019.10.24)

【公表番号】特表2019-526123(P2019-526123A)
【公表日】令和1年9月12日(2019.9.12)
【年通号数】公開・登録公報2019-037
【出願番号】特願2019-503726(P2019-503726)
【国際特許分類】
Ｇ０６Ｆ　21/53　　(2013.01)
Ｇ０６Ｆ　21/56　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/53
Ｇ０６Ｆ　21/56

【手続補正書】
【提出日】令和1年8月28日(2019.8.28)
【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上で実行されるアプリケーションのハイレベル機能を検出するための方法であって、
コンピューティングデバイス上のセキュアなメモリに、アプリケーションのためのアプリケーション固有仮想アドレスマッピングテーブルを記憶するステップであって、前記アプリケーション固有仮想アドレスマッピングテーブルは、前記アプリケーションのソースコードにおける対応するターゲットアプリケーション機能にマッピングされたアプリケーションバイナリコードにおける複数の仮想アドレスオフセットを含む、ステップと、
前記アプリケーションを起動したことに応答して、実行されるアプリケーションプロセスのインスタンスのためにプロセス固有仮想アドレスマッピングテーブルを生成するステップであって、前記プロセス固有仮想アドレスマッピングテーブルは、前記アプリケーション固有仮想アドレスマッピングテーブルにおける前記仮想アドレスオフセットを使用して、前記ターゲットアプリケーション機能に対応する実際の仮想アドレスを定義する、ステップと、
前記アプリケーションプロセスの前記インスタンスのための前記アプリケーションバイナリコードの実行中に、前記プロセス固有仮想アドレスマッピングテーブルに基づいて、前記ターゲットアプリケーション機能に対応する前記実際の仮想アドレスのうちの1つまたは複数が実行されることを検出するステップと、
前記アプリケーションプロセスの前記インスタンスのための前記アプリケーションバイナリコードの実行に関連付けられた1つまたは複数の例外または挙動を検出するように構成された例外処理モジュールに、前記プロセス固有仮想アドレスマッピングテーブルにおける前記実際の仮想アドレスから検出された、前記実行されたターゲットアプリケーション機能を提供するステップであって、前記例外処理モジュールは、悪意のあるコード検出アルゴリズムを含む、ステップと
を含む方法。
【請求項２】
前記アプリケーションプロセスの他のインスタンスと同時に実行される前記アプリケー

ションプロセスの別のインスタンスのために別のプロセス固有仮想アドレスマッピングテーブルを生成するステップと、
前記アプリケーションプロセスの前記別のインスタンスのための前記アプリケーションバイナリコードの実行中に、前記別のプロセス固有仮想アドレスマッピングテーブルに基づいて、前記ターゲットアプリケーション機能に対応する前記実際の仮想アドレスのうちの1つまたは複数がいつ実行されるかを検出するステップと
をさらに含む、請求項1に記載の方法。
【請求項３】
前記実際の仮想アドレスは、前記アプリケーションプロセスの前記インスタンスのベース仮想アドレスおよび前記アプリケーション固有仮想アドレスマッピングテーブルにおける前記仮想アドレスオフセットを使用して決定される、請求項1に記載の方法。
【請求項４】
前記セキュアなメモリは、ハイレベルオペレーティングシステム(HLOS)における信頼できるゾーンに存在する、請求項1に記載の方法。
【請求項５】
前記アプリケーションは、セキュアなウェブアプリケーションおよびウェブブラウザのうちの1つを含む、請求項1に記載の方法。
【請求項６】
前記アプリケーションバイナリコードは、ネイティブバイナリコードとして実行される、請求項1に記載の方法。
【請求項７】
コンピューティングデバイス上で実行されるアプリケーションのハイレベル機能を検出するためのシステムであって、
コンピューティングデバイス上に、アプリケーションのためのアプリケーション固有仮想アドレスマッピングテーブルを記憶するための手段であって、前記アプリケーション固有仮想アドレスマッピングテーブルは、前記アプリケーションのソースコードにおける対応するターゲットアプリケーション機能にマッピングされたアプリケーションバイナリコードにおける複数の仮想アドレスオフセットを含む、手段と、
前記アプリケーションを起動したことに応答して、実行されるアプリケーションプロセスのインスタンスのためにプロセス固有仮想アドレスマッピングテーブルを生成するための手段であって、前記プロセス固有仮想アドレスマッピングテーブルは、前記アプリケーション固有仮想アドレスマッピングテーブルにおける前記仮想アドレスオフセットを使用して、前記ターゲットアプリケーション機能に対応する実際の仮想アドレスを定義する、手段と、
前記アプリケーションプロセスの前記インスタンスのための前記アプリケーションバイナリコードの実行中に、前記プロセス固有仮想アドレスマッピングテーブルに基づいて、前記ターゲットアプリケーション機能に対応する前記実際の仮想アドレスのうちの1つまたは複数が実行されることを検出するための手段と、
前記アプリケーションプロセスの前記インスタンスのための前記アプリケーションバイナリコードの実行に関連付けられた1つまたは複数の例外または挙動を検出するように構成された例外処理モジュールに、前記プロセス固有仮想アドレスマッピングテーブルにおける前記実際の仮想アドレスから検出された、前記実行されたターゲットアプリケーション機能を提供するための手段であって、前記例外処理モジュールは、悪意のあるコード検出アルゴリズムを含む、手段と
を含むシステム。
【請求項８】
前記アプリケーションプロセスの他のインスタンスと同時に実行される前記アプリケーションプロセスの別のインスタンスのために別のプロセス固有仮想アドレスマッピングテーブルを生成するための手段と、
前記アプリケーションプロセスの前記別のインスタンスのための前記アプリケーション

バイナリコードの実行中に、前記別のプロセス固有仮想アドレスマッピングテーブルに基づいて、前記ターゲットアプリケーション機能に対応する前記実際の仮想アドレスのうちの1つまたは複数がいつ実行されるかを検出するための手段と
をさらに含む、請求項7に記載のシステム。
【請求項９】
前記実際の仮想アドレスは、前記アプリケーションプロセスの前記インスタンスのベース仮想アドレスおよび前記アプリケーション固有仮想アドレスマッピングテーブルにおける前記仮想アドレスオフセットを使用して決定される、請求項7に記載のシステム。
【請求項１０】
記憶するための前記手段は、ハイレベルオペレーティングシステム(HLOS)における信頼できるゾーンに存在する、請求項7に記載のシステム。
【請求項１１】
前記アプリケーションは、セキュアなウェブアプリケーションおよびウェブブラウザのうちの1つを含む、請求項7に記載のシステム。
【請求項１２】
前記アプリケーションバイナリコードは、ネイティブバイナリコードとして実行される、請求項7に記載のシステム。
【請求項１３】
メモリ内で具現化され、コンピューティングデバイス上で実行されるアプリケーションのハイレベル機能を検出するためにプロセッサによって実行可能であるコンピュータ可読プログラムコードを有するコンピュータプログラムであって、
コンピューティングデバイス上のセキュアなメモリに、アプリケーションのためのアプリケーション固有仮想アドレスマッピングテーブルを記憶することであって、前記アプリケーション固有仮想アドレスマッピングテーブルは、前記アプリケーションのソースコードにおける対応するターゲットアプリケーション機能にマッピングされたアプリケーションバイナリコードにおける複数の仮想アドレスオフセットを含む、記憶することと、
前記アプリケーションを起動したことに応答して、実行されるアプリケーションプロセスのインスタンスのためにプロセス固有仮想アドレスマッピングテーブルを生成することであって、前記プロセス固有仮想アドレスマッピングテーブルは、前記アプリケーション固有仮想アドレスマッピングテーブルにおける前記仮想アドレスオフセットを使用して、前記ターゲットアプリケーション機能に対応する実際の仮想アドレスを定義する、生成することと、
前記アプリケーションプロセスの前記インスタンスのための前記アプリケーションバイナリコードの実行中に、前記プロセス固有仮想アドレスマッピングテーブルに基づいて、前記ターゲットアプリケーション機能に対応する前記実際の仮想アドレスのうちの1つまたは複数が実行されることを検出することと、
前記アプリケーションプロセスの前記インスタンスのための前記アプリケーションバイナリコードの実行に関連付けられた1つまたは複数の例外または挙動を検出するように構成された例外処理モジュールに、前記プロセス固有仮想アドレスマッピングテーブルにおける前記実際の仮想アドレスから検出された、前記実行されたターゲットアプリケーション機能を提供することであって、前記例外処理モジュールは、悪意のあるコード検出アルゴリズムを含む、ことと
を行うように構成された論理を含むコンピュータプログラム。
【請求項１４】
前記アプリケーションプロセスの他のインスタンスと同時に実行される前記アプリケーションプロセスの別のインスタンスのために別のプロセス固有仮想アドレスマッピングテーブルを生成することと、
前記アプリケーションプロセスの両方のインスタンスのための前記アプリケーションバイナリコードの同時実行中に、前記別のプロセス固有仮想アドレスマッピングテーブルに基づいて、前記ターゲットアプリケーション機能に対応する前記実際の仮想アドレスのう

ちの1つまたは複数がいつ実行されるかを検出することと
を行うように構成された論理をさらに含む、請求項13に記載のコンピュータプログラム。
【請求項１５】
前記実際の仮想アドレスは、前記アプリケーションプロセスの前記インスタンスのベース仮想アドレスおよび前記アプリケーション固有仮想アドレスマッピングテーブルにおける前記仮想アドレスオフセットを使用して決定される、請求項13に記載のコンピュータプログラム。
【請求項１６】
前記セキュアなメモリは、ハイレベルオペレーティングシステム(HLOS)における信頼できるゾーンに存在する、請求項13に記載のコンピュータプログラム。
【請求項１７】
前記アプリケーションは、セキュアなウェブアプリケーションおよびウェブブラウザのうちの1つを含む、請求項13に記載のコンピュータプログラム。
【請求項１８】
前記アプリケーションバイナリコードは、ネイティブバイナリコードとして実行される、請求項13に記載のコンピュータプログラム。
【請求項１９】
実行中のアプリケーションのハイレベル機能を検出するためのシステムであって、
アプリケーションバイナリコードを実行するように構成された処理デバイスと、
ハイレベルオペレーティングシステム(HLOS)と
を含み、前記HLOSは、
前記アプリケーションのソースコードにおける対応するターゲットアプリケーション機能にマッピングされた前記アプリケーションバイナリコードにおける複数の仮想アドレスオフセットを含むアプリケーション固有仮想アドレスマッピングテーブルと、
前記アプリケーションを起動したことに応答して、実行されるアプリケーションプロセスのインスタンスのためにプロセス固有仮想アドレスマッピングテーブルを生成するように構成されたカーネルモジュールであって、前記プロセス固有仮想アドレスマッピングテーブルは、前記アプリケーション固有仮想アドレスマッピングテーブルにおける前記仮想アドレスオフセットを使用して、前記ターゲットアプリケーション機能に対応する実際の仮想アドレスを定義する、カーネルモジュールと
を含み、
前記HLOSは、前記アプリケーションプロセスの前記インスタンスのための前記アプリケーションバイナリコードの実行中に、前記プロセス固有仮想アドレスマッピングテーブルに基づいて、前記ターゲットアプリケーション機能に対応する前記実際の仮想アドレスのうちの1つまたは複数が実行されることを検出するように構成され、
前記HLOSは、前記アプリケーションプロセスの前記インスタンスのための前記アプリケーションバイナリコードの実行に関連付けられた1つまたは複数の例外または挙動を検出するように構成された例外処理モジュールに、前記プロセス固有仮想アドレスマッピングテーブルにおける前記実際の仮想アドレスから検出された、前記実行されたターゲットアプリケーション機能を提供し、前記例外処理モジュールは、悪意のあるコード検出アルゴリズムを含む、システム。
【請求項２０】
前記HLOSは、
前記アプリケーションプロセスの他のインスタンスと同時に実行される前記アプリケーションプロセスの別のインスタンスのために別のプロセス固有仮想アドレスマッピングテーブルを生成することと、
前記アプリケーションプロセスの両方のインスタンスのための前記アプリケーションバイナリコードの同時実行中に、前記別のプロセス固有仮想アドレスマッピングテーブルに基づいて、前記ターゲットアプリケーション機能に対応する前記実際の仮想アドレスのうちの1つまたは複数がいつ実行されるかを検出することと

を行うようにさらに構成される、請求項19に記載のシステム。
【請求項２１】
前記実際の仮想アドレスは、前記アプリケーションプロセスの前記インスタンスのベース仮想アドレスおよび前記アプリケーション固有仮想アドレスマッピングテーブルにおける前記仮想アドレスオフセットを使用して決定される、請求項20に記載のシステム。
【請求項２２】
前記アプリケーション固有仮想アドレスマッピングテーブルは、前記HLOSにおける信頼できるゾーンに記憶される、請求項20に記載のシステム。