【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11月28日(2019.11.28)

【公表番号】特表2019-527892(P2019-527892A)
【公表日】令和1年10月3日(2019.10.3)
【年通号数】公開・登録公報2019-040
【出願番号】特願2019-503727(P2019-503727)
【国際特許分類】
Ｇ０６Ｆ　21/56　　(2013.01)
Ｇ０６Ｆ　21/74　　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　21/56　　３６０
Ｇ０６Ｆ　21/74

【手続補正書】
【提出日】令和1年10月15日(2019.10.15)
【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、複数の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、各仮想アドレスマッピングテーブルは、複数のアプリケーションのうちの1つに対応し、各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の複数の仮想アドレスを含む、ステップと、
ハイレベルオペレーティングシステム(HLOS)に前記アプリケーションを登録するステップと、
前記アプリケーションバイナリコードの実行中に、前記HLOSが、前記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仮想アドレスのうちの1つまたは複数が実行されるときを検出するステップと
を含む方法。
【請求項２】
前記セキュアなメモリは、前記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３】
前記アプリケーションバイナリコードが更新されたときに、前記ターゲットアプリケーション機能の改訂された仮想アドレスにより前記仮想アドレスマッピングテーブルを更新するステップ
をさらに含む、請求項1に記載の方法。
【請求項４】
前記アプリケーション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
をさらに含む、請求項1に記載の方法。

【請求項５】
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、請求項4に記載の方法。
【請求項６】
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７】
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８】
前記アプリケーションバイナリコードは、関連する仮想機械を含む、請求項1に記載の方法。
【請求項９】
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、複数の仮想アドレスマッピングテーブルをセキュアに記憶するための手段であって、各仮想アドレスマッピングテーブルは、複数のアプリケーションのうちの1つに対応し、各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の複数の仮想アドレスを含む、手段と、
ハイレベルオペレーティングシステム(HLOS)に前記アプリケーションを登録するための手段と、
前記アプリケーションバイナリコードの実行中に、前記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仮想アドレスのうちの1つまたは複数が実行されるときを検出するための手段と
を含むシステム。
【請求項１０】
前記セキュアなメモリは、前記HLOSにおける信頼できるゾーンを含む、請求項9に記載のシステム。
【請求項１１】
前記アプリケーションバイナリコードが更新されたときに、前記ターゲットアプリケーション機能の改訂された仮想アドレスにより前記仮想アドレスマッピングテーブルを更新するための手段
をさらに含む、請求項9に記載のシステム。
【請求項１２】
前記アプリケーションの実行に関連付けられた1つまたは複数の例外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
をさらに含む、請求項9に記載のシステム。
【請求項１３】
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、請求項12に記載のシステム。
【請求項１４】
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9に記載のシステム。
【請求項１５】
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9に記載のシステム。
【請求項１６】
前記アプリケーションバイナリコードは、関連する仮想機械を含む、請求項9に記載の

システム。
【請求項１７】
メモリ内で具現化され、コンピュータ可読プログラムコードを含むコンピュータプログラムであって、前記コンピュータ可読プログラムコードは、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り、前記コンピュータ可読プログラムコードは、
コンピューティングデバイス上のセキュアなメモリに、複数の仮想アドレスマッピングテーブルを記憶するためのコードであって、各仮想アドレスマッピングテーブルは、複数のアプリケーションのうちの1つに対応し、各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の複数の仮想アドレスを含む、コードと、
ハイレベルオペレーティングシステム(HLOS)に前記アプリケーションを登録するためのコードと、
前記アプリケーションバイナリコードの実行中に、前記HLOSが、前記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仮想アドレスのうちの1つまたは複数が実行されるときを検出するためのコードと
を含む、コンピュータプログラム。
【請求項１８】
前記セキュアなメモリは、前記HLOSにおける信頼できるゾーンを含む、請求項17に記載のコンピュータプログラム。
【請求項１９】
前記コンピュータ可読プログラムコードは、
前記アプリケーションバイナリコードが更新されたときに、前記ターゲットアプリケーション機能の改訂された仮想アドレスにより前記仮想アドレスマッピングテーブルを更新するためのコード
をさらに含む、請求項17に記載のコンピュータプログラム。
【請求項２０】
前記コンピュータ可読プログラムコードは、
前記アプリケーション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コード
をさらに含む、請求項17に記載のコンピュータプログラム。
【請求項２１】
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、請求項20に記載のコンピュータプログラム。
【請求項２２】
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17に記載のコンピュータプログラム。
【請求項２３】
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17に記載のコンピュータプログラム。
【請求項２４】
前記アプリケーションバイナリコードは、関連する仮想機械を含む、請求項17に記載のコンピュータプログラム。
【請求項２５】
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、
複数の仮想アドレスマッピングテーブルを含むハイレベルオペレーティングシステム(HLOS)であって、各仮想アドレスマッピングテーブルは、複数のアプリケーションのうちの

1つに対応し、各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前記アプリケーションバイナリコードの複数の仮想アドレスを含む、前記ターゲットアプリケーション機能に対応する前記仮想アドレスのうちの1つまたは複数が実行されるときを検出するように構成されたHLOSと
を含むシステム。
【請求項２６】
セキュアなメモリが、前記HLOSにおける信頼できるゾーンを含む、請求項25に記載のシステム。
【請求項２７】
前記HLOSは、前記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受信し、前記アプリケーションの実行に関連付けられた1つまたは複数の例外を検出するように構成された例外処理モジュールをさらに含む、請求項25に記載のシステム。
【請求項２８】
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、請求項27に記載のシステム。
【請求項２９】
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25に記載のシステム。
【請求項３０】
前記アプリケーションバイナリコードは、関連する仮想機械を含む、請求項25に記載のシステム。