

【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22年4月2日(2010.4.2)

【公表番号】特表2009-528632(P2009-528632A)

【公表日】平成21年8月6日(2009.8.6)

【年通号数】公開・登録公報2009-031

【出願番号】特願2008-557407(P2008-557407)

【国際特許分類】

G 06 F 12/14 (2006.01)

G 06 F 21/24 (2006.01)

【F I】

G 06 F 12/14 5 1 0 E

G 06 F 12/14 5 6 0 C

【手続補正書】

【提出日】平成22年2月12日(2010.2.12)

【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】

コンピュータのオペレーティングシステム(OS)のユーザモードにおいて、呼び出し元から実行可能コードを受信するステップと、

前記実行可能コードが、実行可能メモリページを割り当てる命令、または、実行可能メモリページの属性を変更する命令を含んでいるか否かを、コンピュータにより判定するステップと、を含み、

前記実行可能コードが、実行可能メモリページを割り当てる命令、または、実行可能メモリページの属性を変更する命令を含んでいる場合には、

前記呼び出し元の特権を検査するために、前記コンピュータにより、前記コンピュータのOSをカーネルモードに切り換えるステップと、

前記コンピュータが、前記実行可能コードをメモリに読み込む関数を、前記コンピュータのOSの特権リングに限定するステップと、

を含むステップを実行する、実行可能コード変更の防止のための方法。

【請求項2】

前記実行可能コードのページレベル保護を実施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3】

前記呼び出し元の特権を検査するためのステップが、

前記実行可能ページの前記割り当て、または、前記実行可能ページの前記属性の変更を許す前に、前記OSの前記特権リングだけに割り当てられた特権が存在するか否かを判定するステップ、

を含む請求項1に記載の方法。

【請求項4】

前記実行可能コードが読み込まれた後、前記実行可能コードの完全性を検査するステップをさらに含む請求項3に記載の方法。

【請求項5】

前記ページレベル保護は、ハードウェアベースの実施、および、実行可能ページの追跡

を使用して実行される請求項 4 に記載の方法。

【請求項 6】

請求項 1 から 5 のいずれかに記載のステップを、コンピュータで実行するための命令を有するコンピュータ可読媒体。

【請求項 7】

コンピュータのオペレーティングシステム(OS)のユーザモードにおいて、呼び出し元から実行可能コードを受信する手段と、

前記実行可能コードが、実行可能メモリページを割り当てる命令、または、実行可能メモリページの属性を変更する命令を含んでいるか否かを判定する手段と、

前記実行可能コードが、実行可能メモリページを割り当てる命令、または、実行可能メモリページの属性を変更する命令を含んでいる場合には、前記呼び出し元の特権を検査するために、前記コンピュータのOSをカーネルモードに切り換える手段と、

前記実行可能コードをメモリに読み込む関数を、前記コンピュータのOSの特権リングに限定する手段と、

を備えた、実行可能コード変更の防止のためのシステム。

【請求項 8】

前記実行可能コードのページレベル保護を実施するための手段をさらに含む請求項 7 に記載のシステム。

【請求項 9】

前記呼び出し元の特権を検査する手段は、前記実行可能ページの前記割り当て、または、前記実行可能ページの前記属性の変更を許す前に、前記OSの前記特権リングだけに割り当てられた特権が存在するかどうかを判定する請求項 7 に記載のシステム。

【請求項 10】

前記実行可能コードが読み込まれた後、前記実行可能コードの完全性を検査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 11】

ページレベル保護を実施するための前記手段は、ハードウェアベースの実施、および実行可能ページの追跡のための手段を含む請求項 10 に記載のシステム。

【請求項 12】

コンピュータのオペレーティングシステム(OS)のユーザモードにおいて、呼び出し元から実行可能コードを受信するステップと、

前記実行可能コードが、実行可能メモリページを割り当てる命令、または、実行可能メモリページの属性を変更する命令を含んでいるか否かを、コンピュータにより判定するステップと、を含み、

前記実行可能コードが、実行可能メモリページを割り当てる命令、または、実行可能メモリページの属性を変更する命令を含んでいる場合には、

前記呼び出し元の特権を検査するために、前記コンピュータにより、前記コンピュータのOSをカーネルモードに切り換えるステップと、

前記コンピュータが、前記実行可能コードをメモリに読み込む関数を、前記コンピュータのOSの特権リングに限定するステップと、

前記実行可能コードが読み込まれた後、前記実行可能コードの完全性を検査するステップと、

を含むステップを実行し、

前記ページレベル保護は、ハードウェアベースの実施、および、実行可能ページの追跡を使用して実行されることを特徴とする、データページの変更の防止のための方法。

【請求項 13】

請求項 12 に記載のステップを、コンピュータで実行するための命令を有するコンピュータ可読媒体。