

【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6月16日(2016.6.16)

【公開番号】特開2013-242860(P2013-242860A)

【公開日】平成25年12月5日(2013.12.5)

【年通号数】公開・登録公報2013-065

【出願番号】特願2013-90839(P2013-90839)

【国際特許分類】

G 06 F 21/62 (2013.01)

G 06 F 9/48 (2006.01)

【F I】

G 06 F 21/24 1 6 2

G 06 F 9/46 4 5 7

【手続補正書】

【提出日】平成28年4月19日(2016.4.19)

【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】

コンピュータシステムの1つまたは複数の構成要素間の相互作用を制御する方法であって、前記システムが、互いに相互作用して、活動に従事するように適合された複数の構成要素を含み、前記方法が、

固定セキュリティレベルを前記システムのそれぞれの構成要素に割り当てるステップと、

前記システムの構成要素間のすべての現在アクティブな相互作用および新しく要求された相互作用を監視するステップであって、新しく要求された相互作用が、宛先構成要素と相互作用するための、発信元構成要素による要求を含む、監視するステップと、を含み、

前記発信元構成要素および前記宛先構成要素の前記セキュリティレベル間の差が1つのレベルを上回る場合、前記要求された相互作用を禁じ、

構成発信元要素がそれ自体のセキュリティレベルよりもより低く割り当てられたセキュリティレベルを有するいずれかの構成要素との相互作用に従事しており、前記要求された相互作用が、より高く割り当てられたセキュリティレベルを有する宛先構成要素に関わっているか、または前記要求された相互作用がより高く割り当てられたセキュリティレベルを有するいずれかの構成要素との相互作用に現在従事している場合、前記要求された相互作用を禁じ、

発信元構成要素がそれ自体のセキュリティレベルよりもより高く割り当てられたセキュリティレベルを有するいずれかの構成要素との相互作用に従事しており、前記要求された相互作用がより低く割り当てられたセキュリティレベルを有する宛先構成要素に関わっているか、または前記要求された相互作用がより低く割り当てられたセキュリティレベルを有するいずれかの構成要素との相互作用に現在従事している場合、前記要求された相互作用を禁じ、

発信元構成要素が前記発信元構成要素に割り当てられたセキュリティレベルよりもより高いセキュリティレベルを有するデータを含み、前記要求された相互作用がより低く割り当てられたセキュリティレベルを有する宛先構成要素に関わっているか、または前記要求

された相互作用がより低く割り当てられたセキュリティレベルを有するいずれかの構成要素との相互作用に現在従事している場合、前記要求された相互作用を禁じ、

発信元構成要素が前記発信元構成要素に割り当てられたセキュリティレベルよりもより低いセキュリティレベルを有するデータを含み、前記要求された相互作用がより高く割り当てられたセキュリティレベルを有する宛先構成要素に関わっているか、または前記要求された相互作用がより高く割り当てられたセキュリティレベルを有するいずれかの構成要素との相互作用に現在従事している場合、前記要求された相互作用を禁じ、

そうでない場合、前記要求された相互作用を許可する、
方法。

【請求項 2】

前記システムの構成要素間のすべての現在アクティブな相互作用および新しく要求された相互作用を監視するステップが、

要求された相互作用の前記発信元構成要素および前記宛先構成要素のそれぞれに関する状態値を判断するステップであって、前記状態値が、前記要求された相互作用の前記発信元構成要素および前記宛先構成要素との相互作用に現在従事している構成要素の前記割り当てられたセキュリティレベルに依存して判断されている、判断するステップと、

前記要求された相互作用の前記発信元構成要素および前記宛先構成要素の前記状態値を比較するステップと、

前記要求された相互作用の前記発信元構成要素および前記宛先構成要素の前記状態値間に1つを超えるセキュリティレベルの差が存在するとき、状態ブロック条件を課すステップと、

状態ブロック条件が存在する間、前記要求された相互作用を禁じるステップと、
を含む、請求項1に記載の方法。

【請求項 3】

相互作用の間に構成要素が従事できるそれぞれの活動に優先レベルを割り当てるステップと、

状態ブロック条件が課されているとき、前記状態ブロック条件を引き起こした前記発信元構成要素および前記宛先構成要素の前記既存の相互作用を分離するステップと、

前記分離された相互作用に関わる前記活動に関連する前記優先レベルを前記発信元構成要素および前記宛先構成要素の間で前記要求された相互作用に関わる前記活動に関連する前記優先レベルと比較するステップと、

前記分離された相互作用の前記活動の前記優先レベルが前記発信元構成要素および前記宛先構成要素の間で前記要求された相互作用の活動の優先レベルよりもより低いとき、前記状態ブロック条件を解除して、前記要求された相互作用を許可するステップと、

そうでない場合、前記状態ブロック条件を維持して、前記発信元構成要素および前記宛先構成要素の間で前記要求された相互作用を禁じるステップと、
をさらに含む、請求項2に記載の方法。

【請求項 4】

要求された相互作用の前記発信元構成要素および前記宛先構成要素に関する状態値を判断する前記ステップが、

前記発信元構成要素および前記宛先構成要素に割り当てられた前記セキュリティレベルを比較するステップを含み、

前記発信元構成要素の前記割り当てられたセキュリティレベルが前記宛先構成要素の前記割り当てられたセキュリティレベルよりもより低い場合、前記発信元構成要素が相互作用に現在従事している最も安全でない構成要素の前記セキュリティレベルに対応する状態値を前記発信元構成要素に割り当て、前記宛先構成要素が相互作用に現在従事している最も安全な構成要素の前記セキュリティレベルに対応する状態値を前記宛先構成要素に割り当て、

前記発信元構成要素の前記割り当てられたセキュリティレベルが前記宛先構成要素の前記割り当てられたセキュリティレベルよりもより高い場合、前記発信元構成要素が相互作

用に現在従事している最も安全な構成要素の前記セキュリティレベルに対応する状態値を前記発信元構成要素に割り当て、前記宛先構成要素が相互作用に現在従事している最も安全でない構成要素の前記セキュリティレベルに対応する状態値を前記宛先構成要素に割り当て、

そうでない場合、前記それぞれの発信元構成要素および宛先構成要素が相互作用に現在従事している最も安全な構成要素の前記セキュリティレベルに対応する状態値を前記発信元構成要素および前記宛先構成要素に割り当てるステップと、
を含む、請求項 2 または 3 に記載の方法。

【請求項 5】

コンピュータシステムの 1 つまたは複数の構成要素間の相互作用を制御するセキュリティシステムであって、前記コンピュータシステムが、互いと相互作用して、活動に従事するように適合された複数の構成要素を含み、前記システムが、

固定セキュリティレベルを前記システムのそれぞれの構成要素に割り当て、

前記システムの構成要素間のすべての現在アクティブな相互作用および新しく要求された相互作用を監視する

ように構成されたセキュリティモデル実施機構 S M E M を含み、

新しく要求された相互作用が、宛先構成要素と相互作用するための、発信元構成要素による要求を含み、

前記発信元構成要素および前記宛先構成要素の前記セキュリティレベル間の差が 1 つのレベルを上回る場合、前記 S M E M が前記要求された相互作用を禁じるように構成され、

構成発信元要素がそれ自体のセキュリティレベルよりもより低く割り当てられたセキュリティレベルを有するいずれかの構成要素との相互作用に従事しており、前記要求された相互作用が、より高く割り当てられたセキュリティレベルを有する宛先構成要素に関わっているか、または前記要求された相互作用がより高く割り当てられたセキュリティレベルを有するいずれかの構成要素との相互作用に現在従事している場合、前記 S M E M が前記要求された相互作用を禁じるように構成され、

発信元構成要素がそれ自体のセキュリティレベルよりもより高く割り当てられたセキュリティレベルを有するいずれかの構成要素との相互作用に従事しており、前記要求された相互作用がより低く割り当てられたセキュリティレベルを有する宛先構成要素に関わっているか、または前記要求された相互作用がより低く割り当てられたセキュリティレベルを有するいずれかの構成要素との相互作用に現在従事している場合、前記 S M E M が前記要求された相互作用を禁じるように構成され、

発信元構成要素が前記発信元構成要素に割り当てられたセキュリティレベルよりもより高いセキュリティレベルを有するデータを含み、前記要求された相互作用がより低く割り当てられたセキュリティレベルを有する宛先構成要素に関わっているか、または前記要求された相互作用がより低く割り当てられたセキュリティレベルを有するいずれかの構成要素との相互作用に現在従事している場合、前記 S M E M が前記要求された相互作用を禁じるように構成され、

発信元構成要素が前記発信元構成要素に割り当てられたセキュリティレベルよりもより低いセキュリティレベルを有するデータを含み、前記要求された相互作用がより高く割り当てられたセキュリティレベルを有する宛先構成要素に関わっているか、または前記要求された相互作用がより高く割り当てられたセキュリティレベルを有するいずれかの構成要素との相互作用に現在従事している場合、前記 S M E M が前記要求された相互作用を禁じるように構成され、

そうでない場合、前記 S M E M が前記要求された相互作用を許可するように構成された、

セキュリティシステム。

【請求項 6】

前記セキュリティモデル実施機構が、前記コンピュータシステムのオペレーティングシステム内で実施される、請求項 5 に記載のシステム。

【請求項 7】

前記セキュリティモデル実施機構が、前記システムのいずれかの構成要素によってアクセスまたは回避可能でない安全な環境で実施される、請求項 5 または 6 に記載のシステム。