(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6183889号
(P6183889)
(45)発行日　平成29年8月23日(2017.8.23)　(24)登録日　平成29年8月4日(2017.8.4)

(51)Int.Cl.　F I
G06F 21/62 (2013.01)　G06F 21/62 318
G06F 9/48 (2006.01)　G06F 9/46 457

請求項の数 7　外国語出願　(全 28 頁)

(21)出願番号　特願2013-90839(P2013-90839)
(22)出願日　平成25年4月24日(2013.4.24)
(65)公開番号　特開2013-242860(P2013-242860A)
(43)公開日　平成25年12月5日(2013.12.5)
審査請求日　平成28年4月19日(2016.4.19)
(31)優先権主張番号　1207404.3
(32)優先日　平成24年4月27日(2012.4.27)
(33)優先権主張国　英国(GB)

(73)特許権者　509133300
ジーイー・アビエイション・システムズ・リミテッド
GE AVIATION SYSTEMS LIMITED
英国、ジーエル５２　８エスエフ、グロースターシャー、チェルテナム、ビショップス・クリーヴ、チェルテナム・ロード（番地なし）
(74)代理人　100137545
弁理士　荒川　聡志
(74)代理人　100105588
弁理士　小倉　博
(74)代理人　100129779
弁理士　黒川　俊久

最終頁に続く

(54)【発明の名称】コンピュータシステムの構成要素間の相互作用を制御するためのセキュリティシステムおよびセキュリティ方法

(57)【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、前記方法が、
固定セキュリティレベルを前記コンピュータシステムのそれぞれの構成要素にコンピュータが割り当てるステップと、
前記コンピュータ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コンピュータが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コンピュータが禁じ、
前記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場合、前記要求された相互作用をコンピュータが禁じ、
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場合、前記要求された相互作用をコンピュータが禁じ、
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場合、前記要求された相互作用をコンピュータが禁じ、
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場合、前記要求された相互作用をコンピュータが禁じ、
そうでない場合、前記要求された相互作用をコンピュータが許可する、
方法。
【請求項２】
前記コンピュータ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コンピュータが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コンピュータが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コンピュータが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コンピュータが課すステップと、
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コンピュータが禁じるステップと、
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コンピュータが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コンピュータが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コンピュータが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コンピュータが解除して、前記要求された相互作用をコンピュータが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コンピュータが維持して、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コンピュータが禁じるステップと、
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コンピュータが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コンピュータが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コンピュータが割り当て、

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コンピュータが割り当て、

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コンピュータが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、前記セキュリティシステムが、

固定セキュリティレベルを前記コンピュータシステムのそれぞれの構成要素に割り当て、

前記コンピュータ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、前記セキュリティモデル実施機構が前記要求された相互作用を禁じるように構成され、

前記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場合、前記セキュリティモデル実施機構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場合、前記セキュリティモデル実施機構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場合、前記セキュリティモデル実施機構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場合、前記セキュリティモデル実施機構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、前記セキュリティモデル実施機構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、前記コンピュータ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。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータシステムに関し、詳細には、コンピュータシステム内のアクセス制御に関する。
【背景技術】
【０００２】
情報技術が普及し続けるのに伴って、増え続けるデータ量はデジタル形態であり、より安全であると同時に、よりアクセス可能なシステムを配備することによって、すべてのアクセスポイントにおけるデータの保護を必要とする、そのようなデータの保全は、ほとんどの企業が今日直面する主な課題である。営利会社は、その組織のコンピュータ資産の他のサーバとネットワークで接続されたサーバ上でそのウェブサイトをホストする。多くの営利組織および非営利（例えば、政府、軍隊、保健、および教育）組織は、ネットワークを介して通信し、秘密データを記憶および処理するシステムとやはりネットワーク接続されたワークステーションからそのウェブにアクセスする。移動体デバイスおよび関連アプリケーションの幅広い採用は、そのようなデバイスが銀行取引および消費者取引に関してますます使用されるのに伴って、さらなる範囲を加えた。単一のクライアントまたはサーバのサブバージョンは、攻撃者に組織全体の情報リソースおよびコンピューティングリソースに対する即座の接続性を提供し、それによって、機密情報を危険にさらし、潜在的に組織の経営に大損害を与える。データ攻撃の数は過去５年間で３倍を上回り、セキュリティと増大するアクセス需要との間の均衡を保つ必要をさらに重要な優先事項にした。
【０００３】
セキュリティモデルを構築する際の一般的な要素は、機密性、完全性、アクセス性、およびデータ保証である。データ機密性は認可を受けたアクセスだけに開示を制限することによって保証されるのに対して、データ完全性は、意図的であれ、偶発的であれ、データが修正から保護されることを保証する。データアクセス性はデータに対するアクセスの容易さを意味するのに対して、データ保証は特定の実施が事前に確立されたセキュリティ目標に関してある程度の信頼を提供することを意味し、例えば、機密性は防衛適用業務において最重要であり、機密性とデータ完全性は両方とも医療管理適用業務および金融適用業務において等しく適切である。
【０００４】
マルチレベルセキュリティモデルは、データの秘密性に従った機密指定（ｃｌａｓｓｉｆｉｃａｔｉｏｎ）手法を使用する。異なるセキュリティ機密指定を有するデータは、すべて単一の領域内に存在することができ、その領域内のすべてのユーザがその領域内のすべてのデータにアクセスするためのセキュリティクリアランスを有するとは限らないにもかかわらず、そのデータを受信、処理、記憶、および普及することが可能である。最もよく知られているマルチレベルセキュリティモデルは、システムが主体と対象物とを備えるＢｅｌｌ－ＬａＰａｄｕｌａおよびＢｉｂａであり、読取り動作はデータが対象物から主体に流れることに関し、書込み動作はデータが主体から対象物に流れることに関する。Ｂｅｌｌ－ＬａＰａｄｕｌａモデルはデータ機密性だけに対処し、それぞれの主体および対象物は、データの保護レベルを示す、機密指定またはクリアランスからなるセキュリティ

レベル（すなわち、秘密、機密扱いなど）を有する。Ｂｅｌｌ－ＬａＰａｄｕｌａモデルは、２つの特性を実施する。すなわち：
（ｉ）単純なセキュリティ特性：所与のセキュリティレベルの主体は、上位セキュリティレベルの対象物を読み取ってはならない（上位読取り禁止（ｎｏ　ｒｅａｄ　ｕｐ））、および
（ｉｉ）*－特性：所与のセキュリティレベルの主体は、下位セキュリティレベルの対象物に書き込んではならない（下位書込み禁止（ｎｏ　ｗｒｉｔｅ　ｄｏｗｎ））、である。

【０００５】
Ｂｉｂａモデルは、完全性だけに対処し、機密性を完全に無視し、Ｂｅｌｌ－ＬａＰａｄｕｌａの特性とは逆の２つの特性をやはり実施する。すなわち：
（ｉ）単純な完全性特性：所与のレベルの完全性の主体は、下位完全性レベルの対象物を読み取ってはならない（下位読取り禁止（ｎｏ　ｒｅａｄ　ｄｏｗｎ））、
（ｉｉ）*完全性特性：所与の完全性レベルの主体は、上位完全性レベルのいずれかの対象物に書き込んではならない（上位書込み禁止（ｎｏ　ｗｒｉｔｅ　ｕｐ））、である。

【０００６】
Ｂｅｌｌ－ＬａＰａｄｕｌａセキュリティモデルとＢｉｂａセキュリティモデルは両方とも、複数のセキュリティレベルのデータフローに対処することを試みたが、これらは両方とも、限定的であり、柔軟性がないことで知られている。これらのモデルは両方とも、一方向のデータフローだけを効果的に可能にし、Ｂｅｌｌ－ＬａＰａｄｕｌａは（セキュリティレベルに対して）下位読取りと上位書込みだけを許可し、それによって、データ機密性を保証し、Ｂｉｂａは上位読取りと下位書込みだけを許可し、それによって、データ完全性を保証する。しかし、いずれのモデルも、データの完全性と機密性の両方を保証しない。厳密に実施された場合、データが一方向だけに進むシステムを実施するのは実際的には不可能であるため、これらのモデルは両方とも固有の問題を有する。

【０００７】
実際の状況で、これら両方のモデルを実施するために、禁じられた方向に限定された帯域幅のフローを許可する「ワークアラウンド（ｗｏｒｋａｒｏｕｎｄ）」が考案された。しかし、これは、実際には、機密指定解除（ｄｅｃｌａｓｓｉｆｉｃａｔｉｏｎ）の形態は、少なくともある程度、システムのセキュリティを常に危険にさらすことになる。加えて、そのような機密指定解除は、通常、リスクを最小化するために、主体もしくは対象物のセキュリティレベルまたは完全性レベルを増大させることを伴い、これは、最終的に、大部分の主体／対象物にトップレベルのセキュリティまたは完全性を持たせることになり、結果として、セキュリティレベルまたは完全性レベルのパーティションがないシステムを事実上もたらす。システムの最も秘密性の高い構成要素およびデータのセキュリティを保証するために、これらの構成要素の周囲に巨大な防衛機構を構築することを伴うチャイニーズウォール手法が使用されているが、この場合も、これは、結果的に、柔軟性のないシステムをもたらし、経済的なリソース使用法ではない。

【発明の概要】

【０００８】
システムまたはデータのセキュリティが害されないような形で、コンピュータシステムの構成要素間の相互作用を制御する様式を提供することが本発明の目的である。

【０００９】
システムまたはデータのセキュリティが害されず、かつ双方向のデータフローを許可するように、異なるセキュリティレベルで存在する構成要素間の相互作用を制御するための様式を提供することが本発明のさらなる目的である。

【００１０】
本発明は、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にあり、このシステムは、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、この方法は、固定セキュリティレベルを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、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む。まず、構成要素に割り当てられたセキュリティレベルが査定されて、発信元構成要素および宛先構成要素の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、要求された相互作用は禁じられる。これらの構成要素のセキュリティレベル間に１つのレベルの差が存在する場合、両方の構成要素の相互作用が査定される。構成要素が、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、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発信元構成要素もしくは宛先構成要素に関わっているか、または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、要求された相互作用は禁じられる。しかし、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、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発信元構成要素もしくは宛先構成要素に関わっているか、または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、要求された相互作用は禁じられる。さらに、構成要素がその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、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発信元構成要素もしくは宛先構成要素に関わっているか、または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、要求された相互作用は禁じられる。しかし、構成要素が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、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発信元構成要素もしくは宛先構成要素に関わっているか、または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、要求された相互作用は禁じられる。すべてのその他の場合、要求された相互作用は許可される。

【００１１】

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際に、要求された相互作用の発信元構成要素および宛先構成要素のそれぞれに関する状態値が判断され、これらの状態値は、要求された相互作用の発信元構成要素および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割り当てられたセキュリティレベルに依存している。要求された相互作用の発信元構成要素および宛先構成要素の状態値が比較され、宛先構成要素および発信元構成要素の状態値間に１つを超えるセキュリティレベルの差が存在するとき、状態ブロック条件が課される。状態ブロック条件が存在する間、要求された相互作用は禁じられる。

【００１２】

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が割り当てられる。状態ブロック条件が課せられているとき、状態ブロック条件を引き起こした発信元構成要素および宛先構成要素の既存の相互作用は分離されて、分離された相互作用に関わる活動に関連する優先レベルが発信元構成要素および宛先構成要素の間で要求された相互作用に関わる活動に関連する優先レベルと比較される。分離された相互作用の活動の優先レベルが発信元構成要素および宛先構成要素の間で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、状態ブロック条件は解除され、要求された相互作用は許可される。そうでない場合、状態ブロック条件は維持され、発信元構成要素および宛先構成要素の間で要求された相互作用は禁じられた状態に留まる。

【００１３】

本発明は、さらに、上述の方法のすべてのステップを実行するように適合されたコンピュータプログラムコード手段を備えたコンピュータプログラムと、コンピュータ可読媒体

上に埋め込まれたコンピュータプログラムとにある。
【００１４】
別の態様では、本発明は、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にあり、このコンピュータシステムは、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、このシステムは、上記のコンピュータプログラムを含むセキュリティモデル実施機構ＳＭＥＭを含む。
【００１５】
次に、添付の図を参照して、単なる例として、本発明の実施形態が説明される。
【図面の簡単な説明】
【００１６】
【図１】本発明を実施できるコンピュータシステムのシステムブロック図である。
【図２】本発明によって実施されるセキュリティモデルの単純な実用的な実装形態の例を示す図である。
【図３】本発明によって実施されるセキュリティモデルの単純な実用的な実装形態の例を示す図である。
【図４】本発明によって実施されるセキュリティモデルの単純な実用的な実装形態の例を示す図である。
【図５】新しく要求されたトランザクションの２つの構成要素の既存の相互作用を例示するブロック図である。
【図６】構成要素の状態、および状態ブロックが存在するかどうかがどのように判断されるかを例示する流れ図である。
【図７】本明細書の方程式７を例示する図である。
【発明を実施するための形態】
【００１７】
本出願で使用される場合、「構成要素」という用語は、ハードウェア、ハードウェアとソフトウェアの組合せ、ソフトウェア、または実行中のソフトウェアのいずれかのコンピュータ関連エンティティを指す。例えば、構成要素は、プロセッサ上で実行しているプロセス、プロセッサ、オブジェクト、実行可能物、実行のスレッド、プログラム、および／またはコンピュータであってよいが、これらであると限定されない。１つもしくは複数の構成要素はプロセス内および／または実行のスレッド内に存在することが可能であり、構成要素は、１つのコンピュータ上に配置されてよく、かつ／または２つ以上のコンピュータ間で分散されてもよい。本発明はソフトウェア構成要素の観点から説明されるが、本発明はこれに限定されない点を理解されたい。
【００１８】
図１を参照すると、セキュリティモデル実施機構ＳＭＥＭ（１３０）を含むオペレーティングシステム１２０の制御下で実行している複数の構成要素１１０を含むコンピュータシステム１００が示される。セキュリティモデル実施機構ＳＭＥＭ（１３０）は、コンピュータシステム１００のすべての構成要素１１０間のすべての相互作用１４０を制御し、オペレーティングシステム１２０と同じ権利を有するコンピュータオペレーティングシステム１２０のカーネルレベルで実行し、その結果、すべての相互作用を監視および制御することができる。相互作用１４０は、１つもしくは複数のプロセスまたはアクセスデータを実行するために相互作用するための、ある構成要素１１０から別の構成要素に対する要求であり、相互作用の間に構成要素１１０間で送信されているデータを含むことが可能である。セキュリティモデル実施機構ＳＭＥＭ１３０は、システムの構成要素１１０間のすべての要求された相互作用を評価して、その評価に基づいて、構成要素１１０間に要求された相互作用を許可または拒否するセキュリティモデル１５０を実施するように構成される。セキュリティモデル実施機構ＳＭＥＭ１３０は、システム１００のいずれかの構成要素１１０がアクセスまたは回避することができない安全な環境で実施される。
【００１９】
セキュリティモデル１５０は、用いられるアーキテクチャに応じて、多くの形で実施可

能であることを理解されたい。例えば、ＳＭＥＭ１３０は、すべての相互作用を監視および制御する権利を有する独立した安全なアプリケーションであり得る。

【００２０】

システム１００のそれぞれの構成要素１１０には、その機能性および／または記憶されたデータの相対的な重要性もしくは秘密性に基づいて、セキュリティレベルｑ１．．．ｑｎが割り当てられ、この場合、ｑ１は最高のセキュリティレベルを示し、ｑｎは最低のセキュリティレベルを示す。本発明のオペレーティングシステム１２０は、それぞれの構成要素１１０がシステム１００の１つもしくは複数の他の構成要素と相互作用して、１つもしくは複数の活動またはプロセス１６０を同時に実行することができるマルチタスク環境を動作させる。本発明を説明するために、発信元構成要素１１２は、相互作用１４０を要求している構成要素であり、宛先構成要素１１４は、相互作用が望まれる相手の構成要素である。本発明のセキュリティモデル１５０によれば、２つの構成要素１１０間の相互作用が許容できるかどうかに関してＳＭＥＭ１３０によって行われる評価は、構成要素の割り当てられたセキュリティレベルｑ１．．．ｑｎに基づいてだけでなく、２つの構成要素１１０のそれぞれによって実行されている現在の活動１６０にも依存して行われる。

【００２１】

ＳＭＥＭ１３０によって実施される本発明のセキュリティモデル１５０の規則の簡素化された要約は、以下のとおりである。

【００２２】

１．構成要素１１０がより低いセキュリティレベルの構成要素１１０との相互作用１４０に従事している場合、その構成要素１１０は、自らよりもより高いセキュリティレベルのものであるか、もしくは自らよりもより高いセキュリティレベルの構成要素との相互作用に現在従事している構成要素１１０との新しい相互作用１４０を開始すること、またはその構成要素１１０からの新しい相互作用要求を受け入れることはできない。

【００２３】

２．構成要素１１０がより高いセキュリティレベルの構成要素１１０との相互作用１４０に従事している場合、その構成要素１１０は、自らよりもより低いセキュリティレベルのものであるか、もしくは自らよりもより低いセキュリティレベルの構成要素との相互作用１４０に現在従事している構成要素１１０との相互作用１４０を開始すること、またはその構成要素１１０からの相互作用１４０要求を受け入れることはできない。

【００２４】

３．構成要素１１０がその構成要素１１０よりもより高いセキュリティレベルのデータを含む場合、その構成要素１１０は、自らよりもより低いセキュリティレベルのものであるか、もしくは自らよりもより低いセキュリティレベルの構成要素１１０との相互作用１４０に現在従事している構成要素１１０との相互作用１４０を開始すること、またはその構成要素１１０からの相互作用要求を受け入れることはできない。

【００２５】

４．構成要素１１０がその構成要素１１０よりもより低いセキュリティレベルのデータを含む場合、その構成要素１１０は、自らよりもより高いセキュリティレベルのものであるか、もしくは自らよりもより高いセキュリティレベルの構成要素１１０との相互作用１４０に現在従事している構成要素との相互作用１４０を開始すること、またはその構成要素１１０からの相互作用要求を受け入れることはできない。

【００２６】

図２から４は、本発明のセキュリティモデル１５０の規則の実用的な実装形態の３つの異なる単純な例を示す。レベル１からレベル４（Ｌ１～Ｌ４）に及ぶセキュリティレベルｑがそれぞれの構成要素１１０に割り当てられ、レベル１は最も安全であることを示し、レベル４は最も安全でないことを示す。図２を参照すると、レベル２のセキュリティレベルを有する構成要素１１２は、その中に秘密性の高いデータを記憶していることにより、レベル１のセキュリティレベルが割り当てられた構成要素１１６からのデータにアクセスしているのに対して、やはりレベル２のセキュリティレベルを有する構成要素１１４は、

それらの両方ともレベル３のセキュリティレベルが割り当てられている構成要素１１７および１１８と相互作用している。この状況で、構成要素１１２はより高いセキュリティレベルを有する構成要素１１６と相互作用しており、構成要素１１４はより低いセキュリティレベルの構成要素１１７および１１８との相互作用に現在関わっているため、構成要素１１２および１１４の間の相互作用は禁じられる。構成要素１１４がより低いセキュリティレベルの構成要素１１７および１１８との相互作用に現在従事している結果として、構成要素１１４と構成要素１１６の間の相互作用は禁じられる。構成要素１１７および１１８は、同じセキュリティレベルを有するため、より高いセキュリティレベルの構成要素１１４とのその相互作用に依存せずに、互いと相互作用することができるが、より低いセキュリティレベルのいずれかの構成要素１１０との通信は禁じられることになる。構成要素１１２が構成要素１１６内のデータに現在アクセスしている結果として、構成要素１１７および１１８と構成要素１１２との通信は禁じられる。

【００２７】

図３を参照すると、構成要素１１２および１１４は両方とも、構成要素１１６内の秘密性の高いデータにアクセスしている。構成要素１１２および１１４は同じセキュリティレベルを有するため、構成要素１１２および１１４は両方とも構成要素１１６との構成要素に関わっているにもかかわらず、データを共有するための構成要素１１２および１１４の間の相互作用は許可される。しかし、構成要素１１２および１１４が構成要素１１６内のデータに現在アクセスしている結果として、構成要素１１２および１１４のいずれか、ならびに構成要素１１７または１１８のいずれかに関わる相互作用トランザクションは禁じられることになる。構成要素１１７および１１８は同じセキュリティレベルを有し、いずれもより高いセキュリティレベルまたはより低いセキュリティレベルの構成要素１１０とのいずれの相互作用にも関わっていないため、構成要素１１７および１１８の間の相互作用は許可される。

【００２８】

図４に示されたシナリオでは、構成要素１１２は、構成要素１１７との相互作用に関わっているのに対して、構成要素１１４は、構成要素１１８とのトランザクションに関わっている。本発明のモデル１５０の規則を適用すると、より低いセキュリティレベルの構成要素１１７および１１８との相互作用に関わっている結果として、構成要素１１２および１１４は両方とも構成要素１１６内のデータにアクセスすることを禁じられるが、互いとの相互作用を要求すること、または互いからの相互作用要求を受け入れることは可能である。構成要素１１２は、構成要素１１８との通信を開始すること、または構成要素１１８から要求を受け入れることも可能であるのに対して、構成要素１１４は、構成要素１１７との相互作用を要求すること、または構成要素１１７から相互作用に関する要求を受け入れることが可能である。構成要素１１７および１１８は同じセキュリティレベルを有するため、構成要素１１７および１１８は、互いと通信することも可能であるが、より低いセキュリティレベルの構成要素１１０とのいずれの通信も禁じられることになる。

【００２９】

ＳＭＥＭ１３０によって実施される本発明のセキュリティモデル１５０が次により詳細に説明される。形式的に表すと、セキュリティモデル１５０は、以下のセットに基づく：

（ｉ）システム構成要素ｃ：システムのそれぞれの構成要素を識別するｃ∈Ｃ（c_1．．．　．．．c_n）、

（ｉｉ）特定の時点で、構成要素によって実行されている特定の活動に依存する動的値であるセキュリティ状態Ｓ、

（ｉｉｉ）セキュリティレベルｑ：その機能性もしくはその中に記憶されたいずれかのデータの相対的な重要性または秘密性に基づいて、それぞれの構成要素に割り当てられた固定値であるｑ＝Ｑ（q_1．．．　．．．q_n）であり、式中、q_1は最高のセキュリティ度を示し、q_nは最低のセキュリティ度を示す。ｑの値が高ければ高いほど、それに割り当てられるセキュリティレベルは低くなること（すなわち、q_1の値が割り当てられた構成要素は、q_3の値が割り当てられた構成要素よりもより高いセキュリティレベルを有す

る）ことを理解されたい。例えば、航空機システムでは、航空機の制御に関する構成要素には、安全性の理由から、最高のセキュリティレベルq_1を割り当てることができるのに対して、航空機の機構部品の動きを監視および航空機の機構部品の動きに関するデータ提供する、航空機システム内のセンサネットワークは、それぞれq_3のより低いセキュリティレベルが割り当てられたセンサノードを有する場合があるが、これは、それらの構成要素の重要性が航空機の制御よりもより低いためである。センサと制御の間に機能的な関連性が存在するが、これらはq_2のセキュリティレベルが割り当てられた意思決定機能エンティティによって分離されている。構成要素のセキュリティレベルｑはシステムの実行時間に固定されるが、割り当てられたセキュリティレベルは、システム要件が変更するにつれて、必要に応じて再構成可能である点を理解されたい。

【００３０】

（ｉｖ）優先レベルｐ：構成要素のそれぞれの活動に割り当てられた固定値であるｐ＝Ｐ（p_1．．．　．．．p_n）であり、式中、p_1は最高優先度を示し、p_nは最低優先度を示す。セキュリティレベルｑと同様に、ｐの値が高ければ高いほど、それに割り当てられる優先度は低くなる（すなわち、p_1の値が割り当てられた活動は、p_3の値が割り当てられた活動に勝る優先度を有することになる）点を理解されたい。例えば、航空機システムでは、アクチュエータの駆動など、優先レベルp_3が割り当てられたルーチン機能は、より高いp_2の優先レベルを有する、センサによって検出された警告しきい値など、特殊な条件によって割り込まれる場合がある。

【００３１】

（ｖ）構成要素のアクティブな関連性ｔ∈Ｔ（t_1．．．．．．t_l）^{c}であり、式中、$t_l \subseteq c_k \times c_n$は、２つの構成要素$c_k$および$c_n$の間の現在の相互作用を示し、$t_{l+1}$はＳＭＥＭ１３０によって評価されることになる、新しく要求された相互作用を示す。

【００３２】

システムのそれぞれの構成要素c_k１１０は、そのセキュリティ状態

【００３３】

【数１】

$$S_{c_K}$$

、その構成要素に割り当てられた固定セキュリティレベル

【００３４】

【数２】

$$q_{c_k}$$

、および構成要素のアクティブな関連性の現在のセット

【００３５】

【数３】

$$T^{c_k}$$

の点で定義され、

【００３６】

【数４】

$$c_k = S_{c_k} \times q_{c_k} \times T^{c_k}$$

は

【００３７】

【数５】

$$c_k = (c_1^k, c_2^k, c_3^k)$$

方程式１

として表される。

【００３８】

それぞれの活動ｔは、その活動に関わる２つの構成要素１１０（すなわち、相互作用を要求した発信元構成要素ｋ１１２、およびその相互作用が要求される相手の宛先構成要素ｎ１１４）および活動ｔに割り当てられる固定優先レベル

【００３９】

【数６】

$$p_{t_l}$$

の点で定義され、

【００４０】

【数７】

$$t_l = c_k \times c_n \times p_{t_l}$$

は

【００４１】

【数８】

$$t_l = (t_1^l, t_2^l, t_3^l)$$

方程式２

として表される。

【００４２】

既存の活動は、構成要素ｋ

【００４３】

【数９】

$$(t_1^l)$$

および構成要素ｎ

【００４４】

【数１０】

$$(t_2^l)$$

に関わる現在の活動を示すｔ$_l$として表され、式中、構成要素ｋは、宛先構成要素ｎと相互作用を開始した発信元構成要素である。新しい活動は、構成要素ｋによって開始され、その相互作用が許可される前に、ＳＭＥＭ１３０によって評価されることになる構成要素ｋ

【００４５】

【数１１】

$$(t_1^{l+1})$$

と構成要素ｎ

【００４６】

【数１２】

$$(t_2^{l+1})$$

の間の相互作用に関わる、新しく要求された活動を示す（ｔ$_{l+1}$）として表される。

【００４７】

状態値Ｓは、それぞれの新しい相互作用要求の発信元構成要素１１２および宛先構成要素１１４に関してＳＭＥＭ１３０によって判断された動的値であり、それぞれの構成要素の現在の活動を反映する。判断された状態値は、発信元構成要素１１２または宛先構成要素１１４が現在アクティブに関連している（すなわち、それらの構成要素との相互作用に関わっている）すべての構成要素１１０間のセキュリティレベルの差を考慮に入れなければならない。例えば、図５に例示されるように、構成要素ｋは、構成要素ｄ、ｅ、ｆ、およびｇと現在相互作用しており、この場合、構成要素ｄにはｑ$_2$のセキュリティレベル、構成要素ｅにはｑ$_1$のセキュリティレベル、構成要素ｆおよびｇにはｑ$_3$のセキュリティレベルが割り当てられている（すなわち、構成要素ｅはすべての相互作用している構成要素のうち最も安全であり、構成要素ｆおよびｇは最も安全でない、ｑ$_f$＞ｑ$_e$）。一方、構成要素ｎは、構成要素ｈおよびｉと現在相互作用しており、この場合、構成要素ｉにはｑ$_2$のセキュリティレベル、構成要素ｈにはｑ$_3$のセキュリティレベルが割り当てられている（すなわち、構成要素ｉは構成要素ｈよりもより安全である）。このとき、構成要素ｋおよび構成要素ｎに関わるさらなる相互作用が発信元構成要素ｋによって要求される。

【００４８】

まず、構成要素ｋおよびｎのセキュリティレベルに関して、その要求の正当性が判断されなければならない。構成要素が１つを超えるセキュリティレベルだけ離れている場合、通信は禁じられ、いずれのさらなる査定も不要である。

【００４９】

【数１３】

$$\varphi\left(\left(c_2^{t_1^{l+1}} \doteq c_2^{t_2^{l+1}}\right) > 1\right) \rightarrow \psi\left(t_{l+1} = \text{偽}\right) \qquad \text{方程式３}$$

次に、ＳＭＥＭ１３０が本発明のセキュリティモデル１５０を適用することによる、図５に例示されるような構成要素ｋおよびｎに関する状態値の判断が、図６の流れ図を参照して説明される。このプロセスは、ステップ２００で開始し、ステップ２０２で、構成要素ｋおよびｎの割り当てられたセキュリティレベルq_kならびにq_nが読み取られる。ステップ２０４で、ＳＭＥＭは、構成要素ｋおよびｎのそれぞれのすべての現在アクティブな関連性（すなわち、現在の相互作用）を調べ、関わっている構成要素のセキュリティレベルを読み取る。ステップ２０６で、ＳＭＥＭは、構成要素ｋおよびｎのセキュリティレベルq_kならびにq_nを比較する。ステップ２０８で、構成要素ｋが構成要素ｎのセキュリティ度よりもより低いセキュリティ度を有する（すなわち、安全性がより低い）（すなわち、$q_k > q_n$）と判断された場合、構成要素ｋの状態

【００５０】

【数１４】

$$S_{c_k}$$

には、構成要素ｋがアクティブに関連している最も安全でない構成要素１１０のセキュリティレベルに対応する値（すなわち、Q^{max}）を割り当てなければならないのに対して、構成要素ｎの状態

【００５１】

【数１５】

$$S_{c_n}$$

には、構成要素ｎが関連している最も安全な構成要素１１０に対応する値（すなわち、Q^{min}）を割り当てなければならない。したがって、ステップ２１０で、構成要素ｋには、構成要素ｆまたはｇのセキュリティレベルに対応する状態値

【００５２】

【数１６】

$$S_{c_k}$$

を割り当てることになり

【００５３】

【数１７】

$$(S_{c_k} = q_{f,g} = q_3)$$

、構成要素ｎには、構成要素ｉのセキュリティレベルに対応する状態値

【００５４】

【数１８】

$$S_{c_n}$$

を割り当てることになる

【００５５】

【数１９】

$$(S_{c_n} = q_h = q_2)$$

。

【００５６】

しかし、ステップ２０８で、構成要素ｋが構成要素ｎのセキュリティ度よりもより低いセキュリティ度を有さない（すなわち、$q_k > q_n$）と判断された場合、プロセスはステップ２１２に続き、ここで、構成要素ｋが構成要素ｎよりもより高いセキュリティ度を有する（$q_k < q_n$）（すなわち、より安全である）かどうかが判断される。そうである場合、構成要素ｋの状態

【００５７】

【数２０】

$$S_{c_k}$$

には、構成要素ｋがアクティブに関連している、最も安全な構成要素１１０のセキュリティレベルに対応する値（すなわち、Q^{min}）を割り当てなければならないのに対して、構成要素ｎの状態

【００５８】

【数２１】

$$S_{c_n}$$

には、構成要素ｎがアクティブに関連している最も安全でない構成要素１１０のセキュリティレベルに対応する値（すなわち、Q^{max}）を割り当てなければならない。したがって、ステップ２１４で、構成要素ｋには、構成要素ｅのセキュリティレベルに対応する状態値

【００５９】
【数２２】

$$S_{c_k}$$

を割り当てなければならず
【００６０】
【数２３】

$$(S_{c_k} = q_e = q_1)$$

、構成要素ｎには、構成要素ｈのセキュリティレベルに対応する状態値Ｓを割り当てることになる
【００６１】
【数２４】

$$(S_{c_n} = q_h = q_3)$$

。
【００６２】
しかし、ステップ２１２で、構成要素ｋおよびｎに同じセキュリティレベルが割り当てられていることが判断された場合、状態Ｓには、構成要素ｋまたはｎが現在アクティブに関連している最も安全な構成要素１１０のセキュリティレベルに対応する値（すなわち、Q_{min}）が割り当てられる。したがって、ステップ２１６で、構成要素ｋには、構成要素ｅのセキュリティレベルに対応する状態値
【００６３】
【数２５】

$$S_{c_k}$$

が割り当てられることになり
【００６４】
【数２６】

$$(S_{c_k} = q_e = q_1)$$

、構成要素ｎには、構成要素ｉのセキュリティレベルに対応する状態値
【００６５】

【数２７】

$$S_{c_n}$$

が割り当てられることになる

【００６６】

【数２８】

$$(S_{c_n} = q_i = q_2)$$

。

【００６７】

構成要素ｋおよびｎのそれぞれの状態を構成要素ｋおよびｎが現在アクティブに関連しているいずれかの構成要素１１０の最低または最高のセキュリティレベルのうちの１つに対応する値に設定することによって、任意の時点ですべてのアクティブな関連性同士の間に最大のセキュリティクリアランスが存在することを確実にする。これは、異なるセキュリティレベルの構成要素間で禁じられた相互作用のリスクを除去する。

【００６８】

形式的に表すと、アクティブに関連している構成要素のセキュリティ状態は、以下のように割り当てられる：

【００６９】

【数２９】

$$c_k \rightarrow c_n \begin{Bmatrix} c_2^k > c_2^n, c_1^k = Q^{\max}(c_3^k) \text{および} c_1^n = Q^{\min}(c_3^n) \\ c_2^k < c_2^n, c_1^k = Q^{\min}(c_3^k) \text{および} c_1^n = Q^{\max}(c_3^n) \\ c_2^k = c_2^n, c_1^k = Q^{\min}(c_3^k) \text{および} c_1^n = Q^{\min}(c_3^n) \end{Bmatrix} \text{の場合} \qquad \text{方程式４}$$

発信元構成要素１１２および宛先構成要素１１４のそれぞれの状態値

【００７０】

【数３０】

$$S_{c_k}$$

ならびに

【００７１】

【数３１】

$$S_{c_n}$$

が、上で図５および６を参照して説明されたように、ＳＭＥＭ１３０によって判断された後で、構成要素ｋおよびｎの状態値の差に基づいて、要求された相互作用が許可されることになるかどうかが決定される。構成要素ｋおよびｎの判断された状態Ｓ値の差が１を超

える（すなわち、構成要素ｋおよびｎの最高レベル／最低レベルの現在の関連活動間に１つを超えるセキュリティレベルが存在する）場合、セキュリティ状態ブロックが発生し、それらの２つの構成要素間の相互作用は禁じられる。すなわち、本発明のセキュリティモデル１５０は、セキュリティレベルを１つだけ上回る構成要素と、セキュリティレベルを１つだけ下回る構成要素との間の相互作用を許可する（すなわち、１つのレベルだけが発見可能である）。したがって、２つの構成要素間で要求される相互作用は、結果として、それら２つの構成要素が現在相互作用しているいずれかの構成要素のセキュリティレベル間の差が１つのセキュリティレベルを上回る場合、状態ブロック条件を引き起こすことになる。

【００７２】

したがって、図６を再び参照すると、ステップ２０８で、構成要素ｋが構成要素ｎのセキュリティ度よりもより低いセキュリティ度（すなわち、$q_k > q_n$）を有することにより、構成要素ｋの状態値が

【００７３】

【数３２】

$$S_{c_k} = q_{f,g} = q_3$$

として割り当てられ、構成要素ｎの状態値が

【００７４】

【数３３】

$$S_{c_n} = q_i = q_2$$

として割り当てられているステップ２１０で、構成要素ｋおよびｎの状態値間（すなわち、q_3とq_2の間）に１つのセキュリティレベルの差が存在する。したがって、ステップ２１８で、セキュリティブロック状況は存在せず、構成要素ｋおよびｎの間で要求された新しい相互作用は許可されることになる。

【００７５】

しかし、ステップ２１２で、構成要素ｋが構成要素ｎのセキュリティ度よりもより高いセキュリティ度（すなわち、$q_k > q_n$）を有することにより、図６のステップ２１４で、構成要素ｋの状態値が

【００７６】

【数３４】

$$S_{c_k} = q_e = q_1$$

と判断され、構成要素ｎの状態値が

【００７７】

【数３５】

$$S_{c_n} = q_h = q_3$$

と判断されている場合、構成要素ｋおよびｎの状態値間（すなわち、q_1とq_3の間）に２

つのセキュリティレベルの差が存在する。したがって、ステップ２２０で、状態ブロック状況が存在し、構成要素ｋおよびｎの間で要求された新しい相互作用は禁じられることになる。図６のステップ２１６の場合、構成要素ｋおよびｎが同じセキュリティレベルを有する（すなわち、ステップ２０８も２１２も真ではない）ことにより、構成要素ｋの状態値が

【００７８】

【数３６】

$$S_{c_k} = q_e = q_1$$

と判断され、構成要素ｎの状態値が

【００７９】

【数３７】

$$S_{c_n} = q_i = q_2$$

と判断されている場合、構成要素ｋおよびｎの状態値間（すなわち、q_1およびq_2の間）に１つのセキュリティレベルの差が存在すると（すなわち、q_1およびq_2の間で）判断される。したがって、ステップ２２２で、状態ブロック状況は存在せず、新しい相互作用は許可される。

【００８０】

これは、形式的には、以下のように表すことができる：

【００８１】

【数３８】

$$(c_1^k \simeq c_1^n) > 1 \begin{cases} 0, t_{l+1} = \text{真} \\ 1, t_{l+1} = \text{偽} \end{cases} \qquad \text{方程式５}$$

要約すると、状態ブロックは、以下の３つの条件下で発生することになる：

（ｉ）発信元構成要素１１２のセキュリティレベル

【００８２】

【数３９】

$$(q_{c_k})$$

が宛先構成要素１１４のセキュリティレベル

【００８３】

【数４０】

$$(q_{c_n})$$

よりもより低く（すなわち、安全がより低く）、発信元構成要素１１２が現在アクティブに関連している最も安全性でない構成要素１１０のセキュリティレベル

【００８４】

【数４１】

$(q(t_1^l))$

と、宛先構成要素１１４がアクティブに関連している最も安全な構成要素１１０のセキュリティレベル

【００８５】

【数４２】

$(q(t_2^l))$

の間の差が１を超える、

（ｉｉ）発信元構成要素１１２のセキュリティレベル

【００８６】

【数４３】

(q_{c_k})

が宛先構成要素１１４のセキュリティレベル

【００８７】

【数４４】

(q_{c_n})

よりもより高く（すなわち、より安全であり）、発信元構成要素１１２がアクティブに関連している最も安全な構成要素１１０のセキュリティレベル

【００８８】

【数４５】

$(q(t_1^l))$

と、宛先構成要素１１４がアクティブに関連している最も安全でない構成要素１１０のセキュリティレベル

【００８９】

【数４６】

$(q(t_2^l))$

の間の差が１を超える、

（ｉｉｉ）発信元構成要素１１２のセキュリティレベル

【００９０】

【数４７】

(q_{c_k})

が宛先構成要素１１４のセキュリティレベル

【００９１】
【数４８】

$$(q_{c_n})$$

と等しく、発信元構成要素１１２および宛先構成要素１１４のそれぞれが現在アクティブに関連している最も安全な構成要素１１０のセキュリティレベル
【００９２】
【数４９】

$$(q(t_1^l))$$

および
【００９３】
【数５０】

$$(q(t_2^l))$$

の間の差が１を超える。
【００９４】
しかし、状態ブロック条件が存在するときですら、優先度ベースの割込みが発生し得る場合、発信元構成要素１１２と宛先構成要素１１４との間の相互作用を依然として許可することが可能である。先に説明されたように、すべての活動に優先値が割り当てられ、状態ブロック条件の場合、要求された相互作用がより高い優先値を有する活動に関わっている場合、より低い優先度の活動に割り込むことができる。優先割込みが発し得るかどうかを判断するために、状態ブロックを引き起こしている相互作用１６０は分離される。
【００９５】
状態ブロック条件の場合、状態ブロックを引き起こしている発信元構成要素１１２の既存の相互作用（t_l）が発信元構成要素１１２によって要求された、構成要素１１２および１１４の間で新しく要求された相互作用（t_{l+1}）よりもより低い優先度を有する
【００９６】
【数５１】

$$(\text{すなわち、}\ t_3^l > t_3^{l+1})$$

場合、ＳＭＥＭ１３０は、優先割込みを発生させて、既存の相互作用
【００９７】
【数５２】

$$(t_1^l)$$

を中断し、構成要素１１２および１１４の間の相互作用に関わっている、より高い優先度の要求された新しい活動（t_{l+1}）を開始すべきであることを判断する。しかし、既存の相互作用（t_l）が新しく要求された活動（t_{l+1}）よりもより低い優先度を有さない

【００９８】
【数５３】

$$(\text{すなわち、}\ t_3^{l} \leq t_3^{l+1}\ ),$$

場合、ＳＭＥＭ１３０は、既存の相互作用は継続し、新しく要求された相互作用は依然として禁じられた状態に留まることを判断する。
【００９９】
要約すれば、状態ブロックを引き起こしているすべての活動に関して、既存の活動の優先度が要求された新しい活動の優先度以上である場合、既存の活動は継続し、要求された相互作用は禁じられた状態に留まる。しかし、要求された新しい活動の優先度が状態ブロックを引き起こしている既存の活動の優先度よりも大きい場合、優先割込みが発生し、既存の活動を中断させ、２つの構成要素間で要求された相互作用を開始させる。
【０１００】
これは、方程式６および７で形式的に表される。
【０１０１】
【数５４】

a b c d e

$$\forall\left(c_3^{t_1^{l+1}}, c_3^{t_2^{l+1}}\right)\begin{cases} c_1^{t_1^{l+1}} > c_1^{t_2^{l+1}} \begin{cases} t_l \in c_3^{t_1^{l+1}}, \max\left(c_2^{t_1^{l}}, c_2^{t_2^{l}}\right) > c_2^{t_1^{l+1}} \begin{cases} 0, t_l = \text{真} \\ 1, t_3^{l} > t_3^{l+1} \begin{cases} 0, t_l = \text{真} \\ 1, t_l = \text{偽} \end{cases} \end{cases} \\ t_l \in c_3^{t_2^{l+1}}, \min\left(c_2^{t_1^{l}}, c_2^{t_2^{l}}\right) < c_2^{t_2^{l+1}} \begin{cases} 0, t_l = \text{真} \\ 1, t_3^{l} > t_3^{l+1} \begin{cases} 0, t_l = \text{真} \\ 1, t_l = \text{偽} \end{cases} \end{cases} \end{cases} \\ c_1^{t_1^{l+1}} < c_1^{t_2^{l+1}} \begin{cases} t_l \in c_3^{t_1^{l+1}}, \min\left(c_2^{t_1^{l}}, c_2^{t_2^{l}}\right) < c_2^{t_1^{l+1}} \begin{cases} 0, t_l = \text{真} \\ 1, t_3^{l} > t_3^{l+1} \begin{cases} 0, t_l = \text{真} \\ 1, t_l = \text{偽} \end{cases} \end{cases} \\ t_l \in c_3^{t_2^{l+1}}, \max\left(c_2^{t_1^{l}}, c_2^{t_2^{l}}\right) > c_2^{t_2^{l+1}} \begin{cases} 0, t_l = \text{真} \\ 1, t_3^{l} > t_3^{l+1} \begin{cases} 0, t_l = \text{真} \\ 1, t_l = \text{偽} \end{cases} \end{cases} \end{cases} \end{cases}$$

方程式６

すなわち、さらに詳細には、
【０１０２】

【数５５】

$$\left(\left(c_2^{t_1^{l+1}} \doteq c_2^{t_2^{l+1}}\right)>1\right)\rightarrow\psi\left(t_{l+1}=\text{偽}\right)\tau\left(\begin{array}{c} t_{l+1}\begin{cases} c_2^k>c_2^n, c_1^k=Q^{max}(c_3^k)\text{および}\ c_1^n=Q^{min}(c_3^n) \\ c_2^k<c_2^n, c_1^k=Q^{min}(c_3^k)\text{および}\ c_1^n=Q^{max}(c_3^n), \text{に関して} \\ c_2^k=c_2^n, c_1^k=Q^{min}(c_3^k)\text{および}\ c_1^n=Q^{min}(c_3^n) \end{cases} \\ \left(\left(c_1^{t_1^{l+1}} \doteq c_1^{t_2^{l+1}}\right)>1\right)\begin{cases} 1,\forall\left(c_3^{t_1^{l+1}}, c_3^{t_2^{l+1}}\right)\begin{cases} c_1^{t_1^{l+1}}>c_1^{t_2^{l+1}}\begin{cases} t_l\in c_3^{t_1^{l+1}}, \max\left(c_2^{t_1^l}, c_2^{t_2^l}\right)>c_2^{t_1^{l+1}}\begin{cases} 0, t_l=\text{真} \\ 1, t_3^l>t_3^{l+1}\begin{cases} 0, t_l=\text{真} \\ 1, t_l=\text{偽} \end{cases} \end{cases} \\ t_l\in c_3^{t_2^{l+1}}, \min\left(c_2^{t_1^l}, c_2^{t_2^l}\right)<c_2^{t_2^{l+1}}\begin{cases} 0, t_l=true \\ 1, t_3^l>t_3^{l+1}\begin{cases} 0, t_l=\text{真} \\ 1, t_l=\text{偽} \end{cases} \end{cases} \end{cases} \\ c_1^{t_1^{l+1}}<c_1^{t_2^{l+1}}\begin{cases} t_l\in c_3^{t_1^{l+1}}, \min\left(c_2^{t_1^l}, c_2^{t_2^l}\right)<c_2^{t_1^{l+1}}\begin{cases} 0, t_l=true \\ 1, t_3^l>t_3^{l+1}\begin{cases} 0, t_l=\text{真} \\ 1, t_l=\text{偽} \end{cases} \end{cases} \\ t_l\in c_3^{t_2^{l+1}}, \max\left(c_2^{t_1^l}, c_2^{t_2^l}\right)>c_2^{t_2^{l+1}}\begin{cases} 0, t_l=true \\ 1, t_3^l>t_3^{l+1}\begin{cases} 0, t_l=\text{真} \\ 1, t_l=\text{偽} \end{cases} \end{cases} \end{cases} \end{cases} 0 \\ t_{l+1}\begin{cases} c_2^k>c_2^n, c_1^k=Q^{max}(c_3^k)\text{および}\ c_1^n=Q^{min}(c_3^n) \\ c_2^k<c_2^n, c_1^k=Q^{min}(c_3^k)\text{および}\ c_1^n=Q^{max}(c_3^n), \text{に関して}\left(c_1^{t_1^{l+1}} \doteq c_1^{t_2^{l+1}}\right)>1\begin{cases} 0, t_{l+1}=\text{真} \\ 1, t_{l+1}=\text{偽} \end{cases} \\ c_2^k=c_2^n, c_1^k=Q^{min}(c_3^k)\text{および}\ c_1^n=Q^{min}(c_3^n) \end{cases} \end{array}\right), \text{方程式７}$$

方程式７は、図７にも示されている。

【０１０３】

要約すると、提案される新しい関連性

【０１０４】

【数５６】

$$c_3^{t_1^{l+1}}$$

の発信元構成要素１１２のすべてのアクティブな関連性（すなわち、他の構成要素とのすべての現在の相互作用）と、提案される新しい関連性

【０１０５】

【数５７】

$$c_3^{t_2^{l+1}}$$

の宛先構成要素１１４のすべてのアクティブな関連性とに関して、提案される新しい関連性

【０１０６】

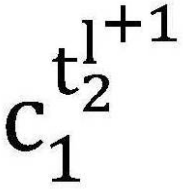
【数５８】

$$c_1^{t_1^{l+1}}$$

の発信元構成要素１１２の状態値が提案される関連性

【０１０７】

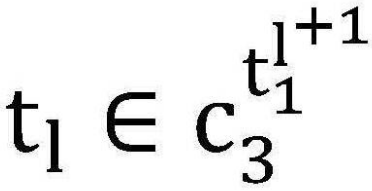
【数５９】



の宛先構成要素１１４の状態値よりもより低いかどうか、またはその逆を判断することがまず必要である。発信元構成要素１１２および宛先構成要素１１４のセキュリティレベル間の差はすでに判断されているため、等しい状態値オプションは存在しない点に留意することが重要である。次に、提案される新しい関連性が、発信元構成要素１１２に属するアクティブな関連性

【０１０８】

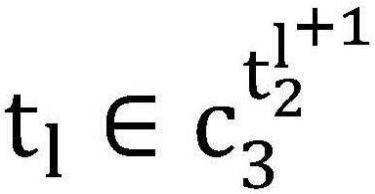
【数６０】



のセットのメンバーであるか、または宛先構成要素に属するアクティブな関連性

【０１０９】

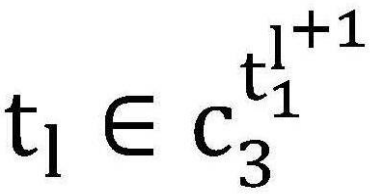
【数６１】



のセットのメンバーであるかが判断される。次いで、既存の関連性（t_l）の構成要素１１０および構成要素１１４のセキュリティレベルの差が状態ブロックを引き起こすことになるかどうかが査定されなければならない。例えば、

【０１１０】

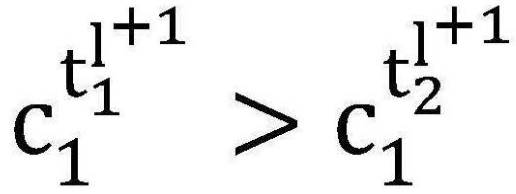
【数６２】



および

【０１１１】

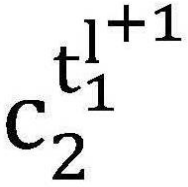
【数６３】



の場合、構成要素１１０のうちの１つが

【０１１２】

【数６４】



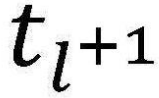
よりもより高いセキュリティレベルを有するいずれのt_lも状態ブロックを引き起こすことになる。状態ブロックが存在しない場合、既存の関連性（t_l）は継続可能である。状態ブロックが存在する場合、優先度査定が行われる。既存の相互作用（t_l）が新しく要求された関連性以上の優先度を有する場合、その関連性は継続可能であり、そうでない場合、既存の相互作用は終了しなければならず、新しく要求された相互作用は許可される。

【０１１３】

上で概要が説明された４つのステップは組み合わされて、発信元構成要素１１０が宛先構成要素１１４との活動を要求しているときはいつでも実行され、結果として、新しい関連性（すなわち、

【０１１４】

【数６５】



＝真）が形成されることを許可するか否かの決定をもたらす単一の査定になる。

【０１１５】

本発明は、現在、最も実用的かつ好ましい実施形態と見なされるものに関して説明されているが、本発明は、開示された実施形態に限定されず、本明細書の基本的な教示から逸脱せずに、改変形態を使用することが可能である点を理解されたい。

【符号の説明】

【０１１６】

１００　コンピュータシステム
１１０　複数の構成要素
１１２　構成要素
　　発信元構成要素
１１４　構成要素
　　宛先構成要素
１１６　構成要素
１１７　構成要素
１１８　構成要素
１２０　オペレーティングシステム
１３０　セキュリティモデル実施機構（ＳＭＥＭ）
１４０　相互作用

１５０　セキュリティモデル
１６０　プロセス
　　活動
　　相互作用

【図１】

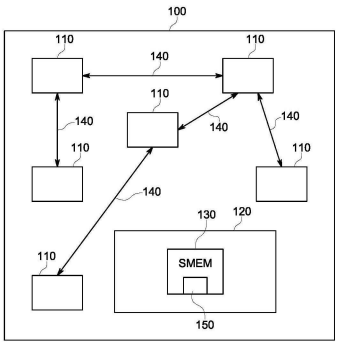


FIG. 1

【図２】

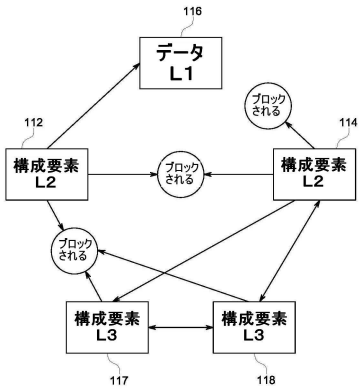


FIG. 2

【図３】

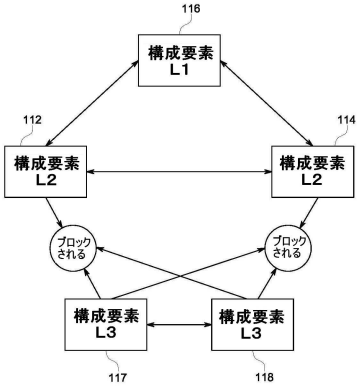


FIG. 3

【図４】

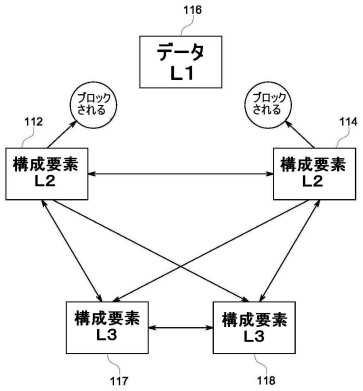


FIG. 4

【図５】

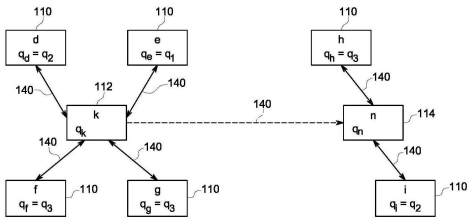


FIG. 5

【図６】

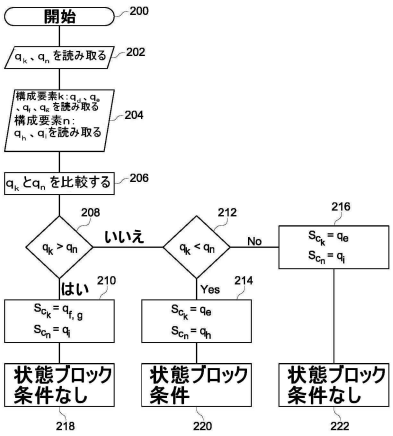


FIG. 6

【図７】

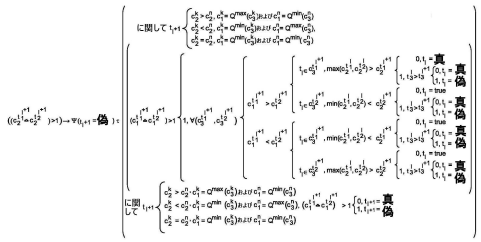


FIG. 7

フロントページの続き

(74)代理人 100113974
弁理士 田中 拓人
(72)発明者 クリストファー・ジェームズ・スライフィルド
英国、ジーエル５２ ８エスティ、グロースターシャー、チェルテナム、ビショップス・クリーヴ、シーエイチ １９ エフ３

審査官 岸野 徹

(56)参考文献 米国特許出願公開第２０１２／００１７２６０（ＵＳ，Ａ１）
特開２００２－２８８３０（ＪＰ，Ａ）
特開２００６－１２７１２７（ＪＰ，Ａ）
米国特許出願公開第２００６／００９５７６２（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／６２
Ｇ０６Ｆ ９／４８