(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6161807号
(P6161807)
(45)発行日　平成29年7月12日(2017.7.12)　(24)登録日　平成29年6月23日(2017.6.23)

(51)Int.Cl.　F I
G06F 21/56 (2013.01)　G06F 21/56

請求項の数 20　(全 48 頁)

(21)出願番号　特願2016-519988(P2016-519988)
(86)(22)出願日　平成26年9月19日(2014.9.19)
(65)公表番号　特表2016-538618(P2016-538618A)
(43)公表日　平成28年12月8日(2016.12.8)
(86)国際出願番号　PCT/US2014/056666
(87)国際公開番号　WO2015/050727
(87)国際公開日　平成27年4月9日(2015.4.9)
審査請求日　平成29年4月4日(2017.4.4)
(31)優先権主張番号　14/044,937
(32)優先日　平成25年10月3日(2013.10.3)
(33)優先権主張国　米国(US)

早期審査対象出願

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　ヴィナイ・シュリダラ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】構成経路に基づく起こり得る悪意のある挙動の事前識別

(57)【特許請求の範囲】
【請求項１】
モバイルコンピューティングデバイスで起こり得る悪意のある挙動を予測する方法であって、
前記モバイルコンピューティングデバイスのプロセッサを介して、サーバコンピューティングデバイスから経路構成のデータベースを受信するステップであって、前記受信した経路構成のデータベースは、
構成パターンと、
良性ではない構成につながる構成間の経路構成と、
前記経路構成が良性ではない挙動につながる確率を識別する確率値と、
を識別する情報を含む、ステップと、
前記プロセッサを介して、前記受信された経路構成のデータベースに含まれる前記情報に基づいて、スケジュールされた動作の実行が前記モバイルコンピューティングデバイス内の前記良性ではない挙動をもたらす確率を決定するステップと、
前記スケジュールされた動作の実行が前記良性ではない挙動をもたらす確率がしきい値を超えると判定することに応答して、予防措置を実施するステップと
を含む、方法。
【請求項２】
予防措置を実施するステップが、
前記モバイルコンピューティングデバイスでの実行のためにスケジュールされた動作に

関連するプロセスを識別するステップと、
前記プロセスの実行を減速するステップと
を含む、請求項1に記載の方法。
【請求項３】
前記モバイルコンピューティングデバイスで起きている他の挙動を検査するステップと、
前記モバイルコンピューティングデバイスの現在の構成を決定するステップと、
前記他の挙動の検査に基づいて、前記現在の構成が前記良性ではない挙動をもたらす可能性がかなりあるかどうかを判定するステップと、
前記他の挙動の検査に基づいて、前記現在の構成が前記良性ではない挙動をもたらす可能性がかなりあると判定することに応答して、前記プロセスに対して前記予防措置を実施するステップと
をさらに含む、請求項2に記載の方法。
【請求項４】
前記モバイルコンピューティングデバイスの現在の構成の分類を決定するステップと、
前記モバイルコンピューティングデバイスの潜在的な将来の構成の分類を決定するステップと、
前記現在の構成の前記分類および前記潜在的な将来の構成の前記分類に基づいて、前記現在の構成が前記良性ではない挙動を引き起こす可能性を決定するステップと、
前記可能性がかなりあるかどうかを判定するステップと、
前記可能性がかなりあると判定することに応答して、前記プロセスに対して前記予防措置を実施するステップと
をさらに含む、請求項2に記載の方法。
【請求項５】
前記モバイルコンピューティングデバイスの現在の構成を決定するステップと、
前記現在の構成および前記受信された経路構成のデータベースに含まれる前記確率値に基づいて、前記良性ではない挙動を引き起こす前記現在の構成の確率を決定するステップと、
前記現在の構成が前記良性ではない挙動につながる確率がリスクしきい値を超えるかどうかを判定するステップと、
前記現在の構成が前記良性ではない挙動を引き起こす確率が前記リスクしきい値を超えると判定することに応答して、前記プロセスに対して前記予防措置を実施するステップと
をさらに含む、請求項2に記載の方法。
【請求項６】
モバイルコンピューティングデバイスであって、
メモリと、
トランシーバと、
前記メモリおよび前記トランシーバに結合されたプロセッサとを備え、前記プロセッサが、
サーバコンピューティングデバイスから経路構成のデータベースを受信することであって、前記受信した経路構成のデータベースは、
構成パターンと、
良性ではない構成につながる構成間の経路構成と、
前記経路構成が良性ではない挙動につながる確率を識別する確率値と、
を識別する情報を含む、ことと、
前記モバイルコンピューティングデバイスでの実行のためにスケジュールされた動作を決定することと、
前記受信された経路構成のデータベースに含まれる前記情報に基づいて、スケジュールされた動作の実行が前記モバイルコンピューティングデバイス内の前記良性ではない挙動をもたらす確率を決定することと、

前記スケジュールされた動作の実行が前記良性ではない挙動をもたらす確率がしきい値を超えると判定することに応答して、予防措置を実施することと
を含む動作を実行するように、プロセッサ実行可能命令で構成された、
モバイルコンピューティングデバイス。
【請求項７】
前記予防措置を実施することが、
前記モバイルコンピューティングデバイス上での実行のためにスケジュールされた動作に関連するプロセスを識別することと、
前記プロセスの実行を減速することと
を含むような動作を実行するように、前記プロセッサがプロセッサ実行可能命令で構成された、請求項6に記載のモバイルコンピューティングデバイス。
【請求項８】
前記プロセッサが、
前記モバイルコンピューティングデバイスで起きている他の挙動を検査することと、
前記モバイルコンピューティングデバイスの現在の構成を決定することと、
前記他の挙動の検査に基づいて、前記現在の構成が前記良性ではない挙動をもたらす可能性がかなりあるかどうかを判定することと、
前記他の挙動の検査に基づいて、前記現在の構成が前記良性ではない挙動をもたらす可能性がかなりあると判定することに応答して、前記プロセスに対して前記予防措置を実施することと
をさらに含む動作を実行するように、プロセッサ実行可能命令で構成された、請求項7に記載のモバイルコンピューティングデバイス。
【請求項９】
前記プロセッサが、
前記モバイルコンピューティングデバイスの現在の構成の分類を決定することと、
前記モバイルコンピューティングデバイスの潜在的な将来の構成の分類を決定することと、
前記現在の構成の前記分類および前記潜在的な将来の構成の前記分類に基づいて、前記現在の構成が前記良性ではない挙動を引き起こす可能性を決定することと、
前記可能性がかなりあるかどうかを判定することと、
前記可能性がかなりあると判定することに応答して、前記プロセスに対して前記予防措置を実施することと
をさらに含む動作を実行するように、プロセッサ実行可能命令で構成された、請求項7に記載のモバイルコンピューティングデバイス。
【請求項１０】
前記プロセッサが、
前記モバイルコンピューティングデバイスの現在の構成を決定することと、
前記現在の構成および前記受信された経路構成のデータベースに含まれる前記確率値に基づいて、前記良性ではない挙動を引き起こす前記現在の構成の確率を決定することと、
スケジュールされた動作の実行が前記良性ではない挙動を引き起こす確率がリスクしきい値を超えるかどうかを判定することと、
前記現在の構成が前記良性ではない挙動を引き起こす確率が前記リスクしきい値を超えると判定することに応答して、前記プロセスに対して前記予防措置を実施することと
をさらに含む動作を実行するように、プロセッサ実行可能命令で構成された、請求項7に記載のモバイルコンピューティングデバイス。
【請求項１１】
モバイルコンピューティングデバイスであって、
サーバコンピューティングデバイスから経路構成のデータベースを受信するための手段であって、前記受信した経路構成のデータベースは、
構成パターンと、

良性ではない構成につながる構成間の経路構成と、
前記経路構成が良性ではない挙動につながる確率を識別する確率値と、
を識別する情報を含む、手段と、
前記モバイルコンピューティングデバイスでの実行のためにスケジュールされた動作を決定するための手段と、
前記受信された経路構成のデータベースに含まれる前記情報に基づいて、前記スケジュールされた動作の実行が前記モバイルコンピューティングデバイス内の前記良性ではない挙動をもたらす確率を決定するための手段と、
前記スケジュールされた動作の実行が前記良性ではない挙動をもたらす確率がしきい値を超えると判定することに応答して、予防措置を実施するための手段と
を備える、モバイルコンピューティングデバイス。

【請求項１２】
予防措置を実施するための手段が、
現在の構成に関連するプロセスを識別するための手段と、
前記プロセスの実行を減速するための手段と
を備える、請求項11に記載のモバイルコンピューティングデバイス。

【請求項１３】
前記モバイルコンピューティングデバイスで起きている他の挙動を検査するための手段と、
前記他の挙動の前記検査に基づいて、前記現在の構成が前記良性ではない挙動をもたらす可能性がかなりあるかどうかを判定するための手段と、
前記他の挙動の前記検査に基づいて、前記現在の構成が前記良性ではない挙動をもたらす可能性がかなりあると判定することに応答して、前記プロセスに対して予防措置を実施するための手段と
をさらに備える、請求項12に記載のモバイルコンピューティングデバイス。

【請求項１４】
前記現在の構成の分類を決定するための手段と、
潜在的な将来の構成の分類を決定するための手段と、
前記現在の構成の前記分類および前記潜在的な将来の構成の前記分類に基づいて、前記現在の構成が前記良性ではない挙動を引き起こす可能性を決定するための手段と、
前記可能性がかなりあるかどうかを判定するための手段と、
前記可能性がかなりあると判定することに応答して、前記プロセスに対して予防措置を実施するための手段と
をさらに備える、請求項12に記載のモバイルコンピューティングデバイス。

【請求項１５】
前記現在の構成および前記受信された経路構成のデータベースに含まれる前記確率値に基づいて、前記現在の構成が悪意のある構成につながる確率を決定するための手段と、
前記現在の構成が前記悪意のある構成につながる前記確率がリスクしきい値を超えるかどうかを判定するための手段と、
前記現在の構成が前記悪意のある構成につながる前記確率が前記リスクしきい値を超えると判定することに応答して、前記プロセスに対して予防措置を実施するための手段と
をさらに備える、請求項12に記載のモバイルコンピューティングデバイス。

【請求項１６】
サーバコンピューティングデバイスから経路構成のデータベースを受信することであって、前記受信した経路構成のデータベースは、
構成パターンと、
良性ではない構成につながる構成間の経路構成と、
前記経路構成が良性ではない挙動につながる確率を識別する確率値と、
を識別する情報を含む、ことと、
前記受信された経路構成のデータベースに含まれる前記情報に基づいて、スケジュール

された動作の実行がモバイルコンピューティングデバイス内の前記良性ではない挙動をもたらす確率を決定することと、
前記スケジュールされた動作の実行が前記良性ではない挙動をもたらす確率がしきい値を超えると判定することに応答して、予防措置を実施することと
を含む動作を前記モバイルコンピューティングデバイスのモバイルコンピューティングデバイスプロセッサに実行させるように構成されたプロセッサ実行可能命令を記憶した、非一時的プロセッサ可読記憶媒体。
【請求項１７】
前記予防措置を実施することが、
前記モバイルコンピューティングデバイスでの実行のためにスケジュールされた動作に関連するプロセスを識別することと、
前記プロセスの実行を減速することと
を含むような動作をモバイルコンピューティングデバイスプロセッサに実行させるように、前記記憶されたプロセッサ実行可能命令が構成された、請求項16に記載の非一時的プロセッサ可読記憶媒体。
【請求項１８】
前記記憶されたプロセッサ実行可能命令が、
モバイルコンピューティングデバイスで起きている他の挙動を検査することと、
前記モバイルコンピューティングデバイスの現在の構成を決定することと、
他の挙動の検査に基づいて、前記現在の構成が前記良性ではない挙動をもたらす可能性がかなりあるかどうかを判定することと、
前記他の挙動の検査に基づいて、前記現在の構成が前記良性ではない挙動をもたらす可能性がかなりあると判定することに応答して、前記プロセスに対して前記予防措置を実施することと
をさらに含む動作をモバイルコンピューティングデバイスプロセッサに実行させるように構成された、請求項17に記載の非一時的プロセッサ可読記憶媒体。
【請求項１９】
前記記憶されたプロセッサ実行可能命令が、
前記モバイルコンピューティングデバイスの現在の構成の分類を決定することと、
前記モバイルコンピューティングデバイスの潜在的な将来の構成の分類を決定することと、
前記現在の構成の前記分類および前記潜在的な将来の構成の前記分類に基づいて、前記現在の構成が前記良性ではない挙動を引き起こす可能性を決定することと、
前記可能性がかなりあるかどうかを判定することと、
前記可能性がかなりあると判定することに応答して、前記プロセスに対して前記予防措置を実施することと
をさらに含む動作をモバイルコンピューティングデバイスプロセッサに実行させるように構成された、請求項17に記載の非一時的プロセッサ可読記憶媒体。
【請求項２０】
前記記憶されたプロセッサ実行可能命令が、
前記モバイルコンピューティングデバイスの現在の構成を決定することと、
前記現在の構成および前記受信された経路構成のデータベースに含まれる前記確率値に基づいて、前記良性ではない挙動を引き起こす前記現在の構成の確率を決定することと、
スケジュールされた動作の実行が前記良性ではない挙動を引き起こす確率がリスクしきい値を超えるかどうかを判定することと、
前記現在の構成が前記良性ではない挙動を引き起こす確率が前記リスクしきい値を超えると判定することに応答して、前記プロセスに対して前記予防措置を実施することと
をさらに含む動作をモバイルコンピューティングデバイスプロセッサに実行させるように構成された、請求項17に記載の非一時的プロセッサ可読記憶媒体。
【発明の詳細な説明】

【技術分野】
【０００１】
関連出願
本出願は、2013年10月3日に出願され、その全体が参照により本明細書に組み込まれる、「Malware Detection and Prevention by Monitoring and Modifying a Hardware Pipeline」と題する米国特許出願第14/044,956号(代理人整理番号133068U2)に関する。
【背景技術】
【０００２】
一般に、モバイルコンピューティングデバイスの性能および電力効率は、時間とともに劣化する。アンチウイルス会社(たとえば、McAfee、Symantecなど)は、現在、この劣化を遅くすることを目的とするモバイル用アンチウイルス、ファイアウォール、および暗号化の製品を販売している。しかしながら、これらのソリューションの多くは、モバイルコンピューティングデバイス上でコンピュータ集約的なスキャニングエンジンの周期的な実行に依存しており、そのことが、モバイルコンピューティングデバイスの処理およびバッテリリソースの多くを消費し、モバイルコンピューティングデバイスを遅くさせるか、もしくは長期間の間使えなくさせ、かつ/または場合によってはユーザ体験を劣化させる場合がある。加えて、これらのソリューションは、通常、知られているウイルスおよびマルウェアの検出に限定され、(たとえば、性能劣化がウイルスまたはマルウェアによって引き起こされないときに)経時的なモバイルコンピューティングデバイスの劣化にしばしば重なって寄与する、複数の複雑な要因および/または相互作用には対処しない。上記およびその他の理由のために、既存のアンチウイルス、ファイアウォール、および暗号化の製品は、経時的なモバイルコンピューティングデバイスの劣化に寄与する可能性がある多くの要因を識別するため、またはモバイルコンピューティングデバイスの劣化を防止するための十分なソリューションを提供しない。
【発明の概要】
【課題を解決するための手段】
【０００３】
様々な態様は、悪意のある挙動が発生または開始した後ではなく、悪意のある挙動が開始する前に、モバイルコンピューティングデバイス上の悪意のある挙動を予想するためのシステムを提供する。様々な態様では、ネットワークサーバは、複数のモバイルコンピューティングデバイスから挙動ベクトル情報を受信することができ、受信された挙動ベクトル情報に対して様々なパターン認識技法を実施して、悪意のある構成、およびそれらの悪意のある構成につながる経路構成を識別することができる。ネットワークサーバは、識別された悪意のある構成および対応する経路構成をモバイルコンピューティングデバイスに通知することができ、それにより、モバイルコンピューティングデバイスが、悪意のある挙動につながる経路構成に入ったが、または入ろうとするときを認識することによって、リアルタイムで悪意のある挙動を予想し防止することが可能になる。
【０００４】
一態様では、ネットワークサーバは、モバイルコンピューティングデバイスが進行中の悪意のある活動を検出した後、複数のモバイルコンピューティングデバイスから構成情報を受信することができる。構成情報は、悪意のある挙動が検出されたときのモバイルコンピューティングデバイスの構成または状態、ならびに悪意のある挙動につながるモバイルコンピューティングデバイスの構成および状態の履歴を示すことができる。ネットワークサーバは、集められたモバイルコンピューティングデバイスの構成情報を分析して、悪意のある挙動を示す構成、ならびに悪意のある構成につながる構成間の構成パターンおよび経路(すなわち、経路構成)を決定することができる。サーバは、識別された経路構成をデータベースまたは他の適切なデータ構造に集めることができ、モバイルコンピューティングデバイスがそれら自体の挙動および構成を分析する際に使用することができる、識別された悪意のある構成および経路構成のデータベースまたはデータ構造を提供する、悪意のある構成および経路構成のデータベースをモバイルコンピューティングデバイスに送るこ

とができる。

【０００５】

一態様では、悪意のある構成および経路構成のデータベースを受信した後、モバイルコンピューティングデバイスは、その現在の構成を決定し、その現在の構成を悪意のある構成および経路構成のデータベースに含まれる構成と比較して、その現在の構成が悪意のある挙動につながる(すなわち、経路構成である)かどうかを判定することができる。モバイルコンピューティングデバイスの現在の構成が経路構成であるとき、モバイルコンピューティングデバイスは、様々な予防措置を実施して悪意のある挙動を最初から阻止または防止することができる。

【０００６】

別の態様では、ネットワークサーバはまた、経路構成が悪意のある挙動につながる確率を計算することができる。そのような態様では、ネットワークサーバは、特定の経路構成が悪意のある構成につながる確率を構成データベースまたはデータ構造とともに送ることができ、モバイルコンピューティングデバイスは、構成データベースまたはデータ構造内の経路構成に加えて受信された確率を参照して、その現在の構成が悪意のある構成につながる可能性があるかどうかを判定することができる。

【０００７】

別の態様では、ネットワークサーバは、実行された場合、経路構成を悪意のある構成に変化させる特定の命令を識別することができる。ネットワークサーバは、そのような識別された命令を構成データベースまたはデータ構造に含めることができ、モバイルコンピューティングデバイスは、構成データベースまたはデータ構造を参照して、デバイスの現在の構成が経路構成であるとき、識別された命令の実行を警戒し防止することができる。

【０００８】

様々な態様は、複数のモバイルコンピューティングデバイスから構成情報および構成履歴を受信することと、構成情報を分析して悪意のある構成を識別することと、識別された悪意のある構成および構成履歴に基づいて経路構成を識別することと、識別された悪意のある構成および識別された経路構成を含む悪意のある構成および経路構成のデータベースを生成することと、複数のモバイルコンピューティングデバイスに悪意のある構成および経路構成のデータベースを送ることとによって、悪意のある挙動につながるモバイルコンピューティングデバイスの構成を識別するための、ネットワークサーバによって実施される方法を含む。一態様では、方法は、識別された経路構成の各々について悪意のある構成に遷移する確率を計算することと、悪意のある構成および経路構成のデータベースに計算された確率を含めることとを含む場合もある。別の態様では、方法は、識別された経路構成内にいる間に実行されたとき識別された悪意のある構成につながる、悪意のある経路命令を識別することと、実行されたとき識別された悪意のある構成につながる識別された命令のリストを、悪意のある構成および経路構成のデータベースに含めることとを含む場合もある。

【０００９】

さらなる態様は、悪意のある構成および経路構成のデータベースを受信することと、現在の構成を決定することと、悪意のある構成および経路構成のデータベースに基づいて、現在の構成が悪意のある構成につながるかどうかを判定することと、現在の構成が悪意のある構成につながると判定することに応答して、予防措置を実施して悪意のある構成を回避することとによって、モバイルコンピューティングデバイス上の起こり得る悪意のある挙動を、それが起きる前に予測するための、モバイルコンピューティングデバイスによって実施される方法を含む。一態様では、予防措置を実施して悪意のある構成を回避することは、現在の構成に関連するプロセスを識別することと、プロセスの実行を減速することとを含む場合がある。

【００１０】

別の態様では、方法は、モバイルコンピューティングデバイス上で起きている他の挙動を検査することと、他の挙動の検査に基づいて、現在の構成が悪意のある構成につながる

可能性がかなりあるかどうかを判定することと、現在の構成が悪意のある構成につながる可能性がかなりあると判定することに応答して、プロセスに対して予防措置を実施することとを含む場合もある。さらに別の態様では、方法は、現在の構成の分類を決定することと、潜在的な将来の構成の分類を決定することと、現在の構成の分類および潜在的な将来の構成の分類に基づいて、現在の構成が悪意のある構成につながる可能性を決定することと、可能性がかなりあるかどうかを判定することと、可能性がかなりあると判定することに応答して、プロセスに対して予防措置を実施することとを含む場合もある。別の態様では、方法は、現在の構成および構成遷移確率に基づいて、現在の構成が悪意のある構成につながる確率を決定することであって、構成遷移確率が悪意のある構成および経路構成のデータベースに含まれる、決定することと、現在の構成が悪意のある構成につながる確率がリスクしきい値を超えるかどうかを判定することと、現在の構成が悪意のある構成につながる確率がリスクしきい値を超えると判定することに応答して、プロセスに対して予防措置を実施することとを含む場合もある。

【００１１】

さらなる態様は、複数のモバイルコンピューティングデバイスから構成情報および構成履歴を受信することと、構成情報を分析して悪意のある構成を識別することと、識別された悪意のある構成および構成履歴に基づいて経路構成を識別することと、識別された悪意のある構成および識別された経路構成を含む悪意のある構成および経路構成のデータベースを生成することと、複数のモバイルコンピューティングデバイスに悪意のある構成および経路構成のデータベースを送ることとを含む動作を実行するように、サーバ実行可能命令で構成されたサーバプロセッサを含む場合がある、ネットワークサーバを含む。一態様では、サーバプロセッサは、識別された経路構成の各々について悪意のある構成に遷移する確率を計算することと、悪意のある構成および経路構成のデータベースに計算された確率を含めることとを含む動作を実行するように、サーバ実行可能命令で構成される場合がある。別の態様では、サーバプロセッサは、識別された経路構成内にいる間に実行されたとき識別された悪意のある構成につながる、悪意のある経路命令を識別することと、実行されたとき識別された悪意のある構成につながる識別された命令のリストを、悪意のある構成および経路構成のデータベースに含めることとを含む動作を実行するように、サーバ実行可能命令で構成される場合がある。

【００１２】

さらなる態様は、メモリと、トランシーバと、メモリおよびトランシーバに結合されたプロセッサとを含む場合があるモバイルコンピューティングデバイスを含み、プロセッサは、悪意のある構成および経路構成のデータベースを受信することと、現在の構成を決定することと、悪意のある構成および経路構成のデータベースに基づいて、現在の構成が悪意のある構成につながるかどうかを判定することと、現在の構成が悪意のある構成につながると判定することに応答して、予防措置を実施して悪意のある構成を回避することと含む動作を実行するように、プロセッサ実行可能命令で構成される場合がある。別の態様では、プロセッサは、予防措置を実施して悪意のある構成を回避することが、現在の構成に関連するプロセスを識別することと、プロセスの実行を減速することとを含むような動作を実行するように、プロセッサ実行可能命令で構成される場合がある。

【００１３】

一態様では、プロセッサは、モバイルコンピューティングデバイス上で起きている他の挙動を検査することと、他の挙動の検査に基づいて、現在の構成が悪意のある構成につながる可能性がかなりあるかどうかを判定することと、現在の構成が悪意のある構成につながる可能性がかなりあると判定することに応答して、プロセスに対して予防措置を実施することとを含む動作をさらに実行するように、プロセッサ実行可能命令で構成される場合がある。別の態様では、プロセッサは、現在の構成の分類を決定することと、潜在的な将来の構成の分類を決定することと、現在の構成の分類および潜在的な将来の構成の分類に基づいて、現在の構成が悪意のある構成につながる可能性を決定することと、可能性がかなりあるかどうかを判定することと、可能性がかなりあると判定することに応答して、プ

ロセスに対して予防措置を実施することとをまた含む動作を実行するように、プロセッサ実行可能命令で構成される場合がある。別の態様では、プロセッサは、現在の構成および構成遷移確率に基づいて、現在の構成が悪意のある構成につながる確率を決定することであって、構成遷移確率が悪意のある構成および経路構成のデータベースに含まれる、決定することと、現在の構成が悪意のある構成につながる確率がリスクしきい値を超えるかどうかを判定することと、現在の構成が悪意のある構成につながる確率がリスクしきい値を超えると判定することに応答して、プロセスに対して予防措置を実施することとをまた含む動作を実行するように、プロセッサ実行可能命令で構成される場合がある。

【００１４】

さらなる態様は、複数のモバイルコンピューティングデバイスから構成情報および構成履歴を受信するための手段と、構成情報を分析して悪意のある構成を識別するための手段と、識別された悪意のある構成および構成履歴に基づいて経路構成を識別するための手段と、識別された悪意のある構成および識別された経路構成を含む悪意のある構成および経路構成のデータベースを生成するための手段と、複数のモバイルコンピューティングデバイスに悪意のある構成および経路構成のデータベースを送るための手段とを含むサーバを含む。一態様では、サーバは、識別された経路構成の各々について悪意のある構成に遷移する確率を計算するための手段と、悪意のある構成および経路構成のデータベースに計算された確率を含めるための手段とを含む場合もある。別の実施形態では、サーバは、識別された経路構成内にいる間に実行されたとき識別された悪意のある構成につながる、悪意のある経路命令を識別するための手段と、実行されたとき識別された悪意のある構成につながる識別された命令のリストを、悪意のある構成および経路構成のデータベースに含めるための手段とを含む場合もある。

【００１５】

さらなる態様は、悪意のある構成および経路構成のデータベースを受信するための手段と、現在の構成を決定するための手段と、悪意のある構成および経路構成のデータベースに基づいて、現在の構成が悪意のある構成につながるかどうかを判定するための手段と、現在の構成が悪意のある構成につながると判定することに応答して、予防措置を実施して悪意のある構成を回避するための手段と含むモバイルコンピューティングデバイスを含む。一態様では、予防措置を実施して悪意のある構成を回避するための手段は、現在の構成に関連するプロセスを識別するための手段と、プロセスの実行を減速するための手段とを含む場合がある。

【００１６】

一態様では、モバイルコンピューティングデバイスは、モバイルコンピューティングデバイス上で起きている他の挙動を検査するための手段と、他の挙動の検査に基づいて、現在の構成が悪意のある構成につながる可能性がかなりあるかどうかを判定するための手段と、現在の構成が悪意のある構成につながる可能性がかなりあると判定することに応答して、プロセスに対して予防措置を実施するための手段とを含む場合がある。別の態様では、モバイルコンピューティングデバイスは、現在の構成の分類を決定するための手段と、潜在的な将来の構成の分類を決定するための手段と、現在の構成の分類および潜在的な将来の構成の分類に基づいて、現在の構成が悪意のある構成につながる可能性を決定するための手段と、可能性がかなりあるかどうかを判定するための手段と、可能性がかなりあると判定することに応答して、プロセスに対して予防措置を実施するための手段とを含む場合もある。別の態様では、モバイルコンピューティングデバイスは、現在の構成および構成遷移確率に基づいて、現在の構成が悪意のある構成につながる確率を決定するための手段であって、構成遷移確率が悪意のある構成および経路構成のデータベースに含まれる、手段と、現在の構成が悪意のある構成につながる確率がリスクしきい値を超えるかどうかを判定するための手段と、現在の構成が悪意のある構成につながる確率がリスクしきい値を超えると判定することに応答して、プロセスに対して予防措置を実施するための手段とを含む場合もある。

【００１７】

さらなる態様では、非一時的サーバ可読記憶媒体は、複数のモバイルコンピューティングデバイスから構成情報および構成履歴を受信することと、構成情報を分析して悪意のある構成を識別することと、識別された悪意のある構成および構成履歴に基づいて経路構成を識別することと、識別された悪意のある構成および識別された経路構成を含む悪意のある構成および経路構成のデータベースを生成することと、複数のモバイルコンピューティングデバイスに悪意のある構成および経路構成のデータベースを送ることとを含む動作をサーバプロセッサに実行させるように構成された、サーバ実行可能命令を記憶している場合がある。一態様では、記憶されたサーバ実行可能命令は、識別された経路構成の各々について悪意のある構成に遷移する確率を計算することと、悪意のある構成および経路構成のデータベースに計算された確率を含めることとを含む動作をサーバプロセッサに実行させるように構成される場合がある。別の態様では、記憶されたサーバ実行可能命令は、識別された経路構成内にいる間に実行されたとき識別された悪意のある構成につながる、悪意のある経路命令を識別することと、実行されたとき識別された悪意のある構成につながる識別された命令のリストを、悪意のある構成および経路構成のデータベースに含めることとを含む動作をサーバプロセッサに実行させるように構成される場合がある。

【００１８】

さらなる態様では、非一時的プロセッサ可読記憶媒体は、悪意のある構成および経路構成のデータベースを受信することと、現在の構成を決定することと、悪意のある構成および経路構成のデータベースに基づいて、現在の構成が悪意のある構成につながるかどうかを判定することと、現在の構成が悪意のある構成につながると判定することに応答して、予防措置を実施して悪意のある構成を回避することとを含む動作をモバイルコンピューティングデバイスプロセッサに実行させるように構成された、プロセッサ実行可能命令を記憶している場合がある。一態様では、記憶されたプロセッサ実行可能命令は、予防措置を実施して悪意のある構成を回避することが、現在の構成に関連するプロセスを識別することと、プロセスの実行を減速することとを含むような動作をモバイルコンピューティングデバイスプロセッサに実行させるように構成される場合がある。

【００１９】

一態様では、記憶されたプロセッサ実行可能命令は、モバイルコンピューティングデバイス上で起きている他の挙動を検査することと、他の挙動の検査に基づいて、現在の構成が悪意のある構成につながる可能性がかなりあるかどうかを判定することと、現在の構成が悪意のある構成につながる可能性がかなりあると判定することに応答して、プロセスに対して予防措置を実施することとを含む動作をモバイルコンピューティングデバイスプロセッサに実行させるように構成される場合がある。別の態様では、記憶されたプロセッサ実行可能命令は、現在の構成の分類を決定することと、潜在的な将来の構成の分類を決定することと、現在の構成の分類および潜在的な将来の構成の分類に基づいて、現在の構成が悪意のある構成につながる可能性を決定することと、可能性がかなりあるかどうかを判定することと、可能性がかなりあると判定することに応答して、プロセスに対して予防措置を実施することとを含む動作をモバイルコンピューティングデバイスプロセッサに実行させるように構成される場合がある。別の態様では、記憶されたプロセッサ実行可能命令は、現在の構成および構成遷移確率に基づいて、現在の構成が悪意のある構成につながる確率を決定することであって、構成遷移確率が悪意のある構成および経路構成のデータベースに含まれる、決定することと、現在の構成が悪意のある構成につながる確率がリスクしきい値を超えるかどうかを判定することと、現在の構成が悪意のある構成につながる確率がリスクしきい値を超えると判定することに応答して、プロセスに対して予防措置を実施することとを含む動作をモバイルコンピューティングデバイスプロセッサに実行させるように構成される場合がある。

【００２０】

本明細書に組み込まれ、本明細書の一部を構成している添付の図面は、本発明の例示的な態様を示すものであり、上記で与えられた一般的な説明、および下記で与えられる詳細な説明とともに、本発明の特徴を説明する働きをする。

【図面の簡単な説明】
【００２１】
【図１】様々な態様において使用するのに適した例示的な通信システムのネットワーク構成要素を示す通信システムブロック図である。
【図２】特定のモバイルコンピューティングデバイスの挙動、ソフトウェアアプリケーション、またはプロセスが悪意のある挙動につながるかどうかを判定するように構成された、一態様のモバイルコンピューティングデバイスにおける例示的な論理構成要素および情報フローを示すブロック図である。
【図３】悪意のある構成および悪意のある挙動につながる構成を識別し、モバイルコンピューティングデバイス上で悪意のある挙動を回避する際に使用するためにモバイルコンピューティングデバイスにこれらの構成を送るように、クラウドサービス/ネットワーク内で構成されたネットワークサーバを有する一態様のシステムにおける例示的な構成要素および情報フローを示すブロック図である。
【図４】悪意のある構成および経路構成に関する情報を含む悪意のある構成および経路構成のデータベースをモバイルコンピューティングデバイスに送るための一態様の方法を示すプロセスフロー図である。
【図５】モバイルコンピューティングデバイス上で悪意のある挙動を予測し、予防措置を実施して悪意のある挙動を回避するための一態様の方法を示すプロセスフロー図である。
【図６】モバイルコンピューティングデバイス上で起きている他の挙動の検査に部分的に基づいて、近い将来の悪意のある挙動の可能性がかなりあると判定することに応答して、予防措置を実施するための一態様の方法を示すプロセスフロー図である。
【図７Ａ】近い将来の悪意のある挙動の可能性を予測するための有限状態機械分析を示す有限状態機械図である。
【図７Ｂ】近い将来の悪意のある挙動の可能性を予測するときに使用される一実施形態の参照テーブルである。
【図８】現在の構成および潜在的な将来の構成に基づいて、悪意のある構成に入る可能性を決定するための一態様の方法を示すプロセスフロー図である。
【図９】構成間の遷移確率に基づいて、近い将来の悪意のある挙動の可能性を予測するためのマルコフ連鎖分析を示すマルコフ連鎖図である。
【図１０】現在の構成が悪意のある構成につながる確率に基づいて、悪意のある構成に入る確率を決定するための一態様の方法を示すプロセスフロー図である。
【図１１】実行されようとしている命令に基づいて、近い将来の悪意のある挙動の可能性がかなりあると判定することに応答して、予防措置を実施するための一態様の方法を示すプロセスフロー図である。
【図１２】一態様において使用するのに適したモバイルコンピューティングデバイスの構成要素ブロック図である。
【図１３】一態様において使用するのに適した別のモバイルコンピューティングデバイスの構成要素ブロック図である。
【図１４】一態様において使用するのに適したネットワークサーバデバイスの構成要素ブロック図である。
【発明を実施するための形態】
【００２２】
添付の図面を参照して様々な態様が詳細に記載される。可能な場合はいつでも、同じまたは同様の部分を指すために図面全体を通して同じ参照番号が使用される。具体的な例および実装形態への言及は、説明を目的とし、本発明の範囲または本特許請求の範囲を限定するものではない。
【００２３】
いくつかの異なるセルラー通信およびモバイル通信のサービスおよび規格が利用可能であるか、または将来考えられ、それらのすべてが様々な態様を実装し、様々な態様から恩恵を受けることができる。そのようなサービスおよび規格には、たとえば、第3世代パー

トナーシッププロジェクト(3GPP)、ロングタームエボリューション(LTE)システム、第3世代ワイヤレスモバイル通信技術(3G)、第4世代ワイヤレスモバイル通信技術(4G)、モバイル通信用グローバルシステム(GSM（登録商標）)、ユニバーサルモバイルテレコミュニケーションシステム(UMTS)、3GSM（登録商標）、汎用パケット無線サービス(GPRS)、符号分割多元接続(CDMA)システム(たとえば、cdmaOne)、GSM（登録商標）エボリューション用発展型データレート(EDGE:enhanced data rates for GSM（登録商標） evolution)、高度モバイルフォンシステム(AMPS:advanced mobile phone system)、デジタルAMPS(IS-136/TDMA)、エボリューションデータ最適化(EV-DO)、デジタル発展型コードレステレコミュニケーション(DECT:digital enhanced cordless telecommunications)、マイクロ波アクセス用ワールドワイドインターオペラビリティ(WiMAX:Worldwide Interoperability for Microwave Access)、ワイヤレスローカルエリアネットワーク(WLAN)、Wi-Fi保護アクセスIおよびII(WPA、WPA2:Wi-Fi Protected Access I & II)、ならびに統合デジタル発展型ネットワーク(iden:integrated digital enhanced network)が含まれる。これらの技術の各々は、たとえば、音声、データ、シグナリング、および/またはコンテンツメッセージの送信および受信を伴う。個々の電気通信の規格または技術に関係する用語および/または技術的詳細に対するいかなる参照も例示目的にすぎず、請求項の文言に具体的に記載されない限り、特許請求の範囲を特定の通信システムまたは通信技術に限定するものではないことを理解されたい。

【００２４】

本明細書で使用する「モバイルコンピューティングデバイス」という用語は、携帯電話、スマートフォン、パーソナルまたはモバイルのマルチメディアプレーヤ、携帯情報端末(PDA)、ラップトップコンピュータ、タブレットコンピュータ、スマートブック、ウルトラブック、パームトップコンピュータ、ワイヤレス電子メール受信機、マルチメディアインターネット対応携帯電話、ワイヤレスゲームコントローラ、および、性能が重要であるメモリとプログラマブルプロセッサとを含み、節電方法が有益であるようなバッテリ電源で動作する同様のパーソナル電子デバイスのうちの、任意の1つまたはすべてを指す。様々な態様は、限られたリソースを有するスマートフォンなどのモバイルコンピューティングデバイスに対して特に有用であるが、これらの態様は一般に、プロセッサを含みアプリケーションプログラムを実行する、任意の電子デバイスにおいて有用である。

【００２５】

「悪意のある挙動」という用語は、本明細書では、長い処理時間、短いバッテリ寿命、個人データの喪失、悪意のある経済活動(たとえば、無許可のプレミアムSMSメッセージを送ること)、スパイ活動またはボットネット活動などのためにモバイルコンピューティングデバイスを乗っ取ることまたは電話を利用することに関する動作などの、多種多様な望ましくないモバイルコンピューティングデバイスの動作および特性を指すために使用される。

【００２６】

「悪意のある構成」という用語は、本明細書では、悪意のある挙動を表すか、または実行するモバイルコンピューティングデバイス、アプリケーション、プロセスなどの構成を指すために使用される。「不審な構成」という用語は、本明細書では、悪意のある挙動の何らかの証拠があるが、悪意のある挙動に関して明確な結論に到達できる前に、より多くの情報が必要とされる構成を指すために使用される。「良性の構成」という用語は、本明細書では、悪意のある構成でもなく、不審な構成でもない構成を指すために使用される。

【００２７】

「経路構成」という用語は、本明細書では、悪意のある構成につながる中間構成としてネットワークサーバが認識しているベクトルまたは経路を指すために使用される。様々な態様では、経路構成は、悪意のある構成につながる任意の構成(たとえば、良性の構成、不審な構成、または悪意のある構成)であり得る。

【００２８】

不十分に設計されたソフトウェアアプリケーション、マルウェア、ウイルス、断片化さ

れたメモリ、バックグラウンドプロセス、および他の悪意のある挙動を含む、モバイルコンピューティングデバイスの性能および電力利用レベルの経時的な劣化に寄与する場合がある様々な要因が存在する。しかしながら、現代のモバイルコンピューティングデバイスの複雑さに起因して、そのような問題の原因を正確かつ効率的に識別すること、および/または識別された問題に十分な措置を提供することは、ユーザ、オペレーティングシステム、および/またはアプリケーションプログラム(たとえば、アンチウイルスソフトウェアなど)にとってますます困難になっている。

【００２９】

現在、コンピューティングデバイス上で悪意のある挙動を検出するための様々なソリューションが存在する。多くのソリューションは、従来、サーバ上に構築された悪意のあるコード/マルウェアの署名データベースに依拠している。これらのソリューションは、ファイルの名前、関数呼出しの名前、特定のコードセグメントの構造、および、さらにコードの各バイトの署名などの、コードの識別情報(すなわち、署名)に基づいて、コードが悪意があるかどうかを検出するために署名データベースを参照することを必要とする。しかしながら、これらのソリューションは、コードが実行されるまで検出不可能な場合がある、悪意のある挙動を検出するには不十分であり、署名を偽造する新しい技法の結果としてますます効果がなくなる。対象的に、下記に記載される様々な態様は、モバイルコンピューティングデバイスが、いかなる特定の識別情報または署名にもかかわらず、正常動作の間に(すなわち、リアルタイムで)悪意のある挙動を検出し、そのような悪意のある挙動が将来起きないように防止することを可能にする。

【００３０】

他のソリューションは、挙動モデルを使用して、コンピューティングデバイス上の悪意のあるプロセス/プログラムと良性のプロセス/プログラムとの間を差別化する。しかしながら、これらのソリューションは、現在、個々のアプリケーションプログラムまたはプロセスの現在の/進行中の挙動を評価することに限定される。したがって、これらのソリューションは、それらがすでに開始した後の問題を解決することのみに限定される。対照的に、下記に記載される様々な態様は、モバイルコンピューティングデバイスが、そのような悪意のある挙動が起きる前にリアルタイムで将来の悪意のある挙動を予想し防止することを可能にする。

【００３１】

加えて、いくつかのソリューションは、プリエンプティブな走査を開始することによって、それらが実行される前にコード、ファイル、スクリプトなどの中の悪意のある挙動のサインを探す。たとえば、あるソリューションは、ファイルがローカルに実行され得る前にウイルスを探して走査されるように、ファイルがインターネット上のある位置からダウンロードされることを必要とする。他のソリューションは、安全な環境(たとえば仮想マシン)においてプログラムまたはプロセスを実行し、プログラムまたはプロセスのが実行時に悪意をもって挙動するかどうかを発見するように試みることによって、悪意のある挙動を発見するように試みる。しかしながら、これらのソリューションは、各々の疑わしいプログラム、ファイル、プロセスなどが、正常動作の一部として実行することを許可される前に、良性であると判定されなければならないので、相当なコンピュータリソースの投資を必要とする。

【００３２】

従来の手法とは対照的に、下記に記載される様々な態様は、モバイルコンピューティングデバイスが、リアルタイムで悪意のある挙動を検出し防止することを可能にし、それにより、最近の方法の相当な準備コストを回避し、モバイルコンピューティングデバイスが将来の悪意のある挙動の確かなリスクを検出するまで、アプリケーションおよびプロセスが正常に実行することを可能にする。概して、様々な態様は、モバイルコンピューティングデバイスの現在の状態または動作状況、ならびに実行が予定されている動作を考えると、モバイルコンピューティングデバイスが近い将来の悪意のある挙動に遭遇するリスクがあるかどうかを、モバイルコンピューティングデバイスが判定することを可能にする、経

路構成のデータベースをモバイルデバイスに提供することによって、上述されたことなどの最近のソリューションの制限に対処する。このようにして、様々な態様は、悪意のある挙動が発生または開始した後ではなく、悪意のある挙動が開始する前に、モバイルコンピューティングデバイス上の悪意のある挙動を予想するためのシステムを提示する。様々な態様では、ネットワークサーバは、複数のモバイルコンピューティングデバイスから挙動ベクトル情報を受信することができ、受信された挙動ベクトル情報に対して(有限状態機械分析を含む)様々なパターン認識技法を実施して、悪意のある構成、およびそれらの悪意のある構成につながる経路構成を識別することができる。ネットワークサーバは、識別された悪意のある構成および対応する経路構成(すなわち、識別された悪意のある構成の長くはない前に出る構成)をモバイルコンピューティングデバイスに通知することができ、それにより、モバイルコンピューティングデバイスが、悪意のある挙動につながる経路構成に入ったが、または入ろうとするときを認識することによって、リアルタイムで悪意のある挙動を予想し防止することが可能になる。

【００３３】

一態様では、ネットワークサーバは、モバイルコンピューティングデバイスが進行中の悪意のある活動を検出した後、複数のモバイルコンピューティングデバイスから構成情報(たとえば、有限状態機械における状態または挙動ベクトルにおけるベクトル値)を受信することができる。構成情報は、悪意のある挙動が検出されたときのモバイルコンピューティングデバイスの構成または状態、ならびに悪意のある挙動につながるモバイルコンピューティングデバイスの構成および状態の履歴を示すことができる。ネットワークサーバは、(たとえば、パターン認識または有限状態機械分析を利用することによって)集められたモバイルコンピューティングデバイスの構成情報を分析して、悪意のある挙動を示す構成を決定することができる。ネットワークサーバは、モバイルコンピューティングデバイスの構成履歴を利用して、悪意のある構成につながる構成間の構成パターンおよび経路(すなわち、経路構成)を認識するために、悪意のある構成から「逆探知」することができる。サーバは、識別された経路構成をデータベースまたは他の適切なデータ構造に集めることができ、モバイルコンピューティングデバイスがそれら自体の挙動および構成を分析する際に使用することができる、識別された悪意のある構成および経路構成のデータベースまたはデータ構造を提供する、悪意のある構成および経路構成のデータベースをモバイルコンピューティングデバイスに送ることができる。

【００３４】

別の態様では、悪意のある構成および経路構成のデータベースを受信した後、モバイルコンピューティングデバイスは、その現在の構成を決定し、その現在の構成を悪意のある構成および経路構成のデータベースに含まれる構成と比較して、その現在の構成が悪意のある挙動につながるかどうかを判定することができる。言い換えれば、モバイルコンピューティングデバイスは、ネットワークサーバから受信された構成データベースまたはデータ構造を利用して、その現在の構成が経路構成であるかどうかを判定することができる。モバイルコンピューティングデバイスの現在の構成が経路構成であるとき、モバイルコンピューティングデバイスは、様々な予防措置を実施して悪意のある挙動を最初から阻止または防止することができる。

【００３５】

別の態様では、ネットワークサーバはまた、経路構成が悪意のある挙動につながる確率を計算することができる。そのような態様では、ネットワークサーバは、特定の経路構成が悪意のある構成につながる確率を構成データベースまたはデータ構造とともに送ることができ、モバイルコンピューティングデバイスは、構成データベースまたはデータ構造内の経路構成に加えて受信された確率を参照して、その現在の構成が悪意のある構成につながる可能性があるかどうかを判定することができる。

【００３６】

別の態様では、ネットワークサーバは、実行された場合、経路構成を悪意のある構成に変化させる特定の命令を識別することができる。ネットワークサーバは、そのような識別

された命令を構成データベースまたはデータ構造に含めることができ、モバイルコンピューティングデバイスは、構成データベースまたはデータ構造を参照して、デバイスの現在の構成が経路構成であるとき、識別された命令の実行を警戒し防止することができる。

【００３７】

様々な態様は、図1に示された例示的な通信システム100などの様々な通信システム内に実装される場合がある。典型的なセル電話ネットワーク104は、ネットワーク運用センタ108に結合された複数のセル基地局106を含み、ネットワーク運用センタ108は、電話陸上通信線(たとえば、図示されていないPOTSネットワーク)およびインターネット110などを介して、モバイルコンピューティングデバイス102(たとえば、携帯電話、ラップトップ、タブレットなど)と他のネットワーク宛先との間の音声通話およびデータを接続するように動作する。モバイルコンピューティングデバイス102と電話ネットワーク104との間の通信は、4G、3G、CDMA、TDMA、LTE、および/または他の携帯電話通信技術などの双方向ワイヤレス通信リンク112を介して遂行することができる。電話ネットワーク104は、インターネット110への接続を提供するネットワーク運用センタ108に結合されるか、またはネットワーク運用センタ108内の、1つまたは複数のサーバ114を含む場合もある。

【００３８】

通信システム100はさらに、電話ネットワーク104およびインターネット110に接続されたネットワークサーバ116を含む場合がある。ネットワークサーバ116と電話ネットワーク104との間の接続は、インターネット110を介するか、または(破線の矢印で示されたように)プライベートネットワークを介する場合がある。ネットワークサーバ116は、クラウドサービスプロバイダネットワーク118のネットワークインフラストラクチャ内のサーバとして実装される場合もある。ネットワークサーバ116とモバイルコンピューティングデバイス102との間の通信は、電話ネットワーク104、インターネット110、プライベートネットワーク(図示せず)、またはそれらの任意の組合せを介して実現することができる。

【００３９】

モバイルコンピューティングデバイス102は、挙動、状態、分類、モデリング、成功率、および/または統計の情報をモバイルコンピューティングデバイス102内に収集し、収集された情報を分析のために(たとえば、電話ネットワーク104を介して)ネットワークサーバ116に送ることができる。一態様では、モバイルコンピューティングデバイス102は、悪意のある挙動に遭遇した後、それらの現在の構成情報(たとえば、それらの現在の状態を記述するそれらの挙動ベクトル)を送ることができる。モバイルコンピューティングデバイス102はまた、ネットワークサーバ116にそれらの構成履歴を送ることができる。構成履歴は、悪意のある挙動の発見につながるように起きた構成変更の履歴、および場合によってはそれらの構成変更を引き起こした命令を含む場合がある。ネットワークサーバ116は、図4を参照して下記でさらに記載されるように、モバイルコンピューティングデバイス102から受信された情報を使用して、悪意のある構成および悪意のある構成につながる構成(すなわち、経路構成)のリストを決定することができる。

【００４０】

別の態様では、ネットワークサーバ116は、悪意のある構成および経路構成のデータベースをモバイルコンピューティングデバイス102に送ることができ、モバイルコンピューティングデバイス102は、悪意のある構成および経路構成のデータベースを受信し使用して、将来の悪意のある構成をそれが起きる前に予測することができる。ネットワークサーバ116は、モバイルコンピューティングデバイスのデータ/挙動モデルを交換、更新、作成、および/または保持するために、次の悪意のある構成および経路構成のデータベースをモバイルコンピューティングデバイス102に送ることができる。

【００４１】

図2は、特定のモバイルコンピューティングデバイスの挙動、ソフトウェアアプリケーション、またはプロセスが、悪意があるか、不審であるか、または良性であるかを判定するように構成された、一態様のモバイルコンピューティングデバイス102における例示的な論理構成要素および情報フローを示す。図2に示された例では、モバイルコンピューテ

ィングデバイス102は、挙動観測器ユニット202と、挙動分析器ユニット204と、外部コンテキスト情報ユニット206と、分類器ユニット208と、作動器ユニット210とを含む場合がある。一態様では、分類器ユニット208は、挙動分析器ユニット204の一部として実装される場合がある。一態様では、挙動分析器ユニット204は、1つまたは複数の分類器ユニット208を生成するように構成される場合があり、1つまたは複数の分類器ユニット208の各々は、1つまたは複数の分類器を含む場合がある。

【００４２】

ユニット202～210の各々は、ソフトウェア、ハードウェア、またはそれらの任意の組合せに実装される場合がある。様々な態様では、ユニット202～210は、オペレーティングシステムの部分内(たとえば、カーネル内、カーネル空間内、ユーザ空間内など)、個別のプログラムもしくはアプリケーション内、専用のハードウェアバッファもしくはプロセッサ内、またはそれらの任意の組合せに実装される場合がある。一態様では、ユニット202～210のうちの1つまたは複数は、モバイルコンピューティングデバイス102の1つまたは複数のプロセッサ上で実行されるソフトウェア命令として実装される場合がある。

【００４３】

挙動観測器ユニット202は、モバイルコンピューティングデバイスの様々なレベル/モジュールでアプリケーションプログラミングインターフェース(API)を計装するかもしくは連携させ、計装されたAPIを介して様々なレベル/モジュールでモバイルコンピューティングデバイスの動作およびイベント(たとえば、システムイベント、状態変化など)を監視/観測し、観測された動作/イベントに関する情報を収集し、収集された情報を知的にフィルタ処理し、フィルタ処理された情報に基づいて1つもしくは複数の観測値を生成し、生成された観測値をメモリ内(たとえば、ログファイル内など)に記憶し、かつ/または、生成された観測値を挙動分析器ユニット204に(たとえば、メモリ書込み、関数呼出しなどを介して)送るように構成される場合がある。

【００４４】

挙動観測器ユニット202は、アプリケーションフレームワークまたはランタイムライブラリ、システム呼出しAPI、ファイルシステム、およびネットワーキングサブシステムの動作、(センサデバイスを含む)デバイスの状態変化、ならびに他の同様のイベントにおけるライブラリAPI呼出しに関する情報を収集することによって、モバイルコンピューティングデバイスの動作およびイベントを監視/観測することができる。挙動観測器ユニット202はまた、ファイルシステム活動を監視することができ、ファイルシステム活動には、ファイル名、ファイルアクセスのカテゴリ(個人情報または通常のデータファイル)を探索すること、ファイル(たとえば、exe、zipなどのタイプ)を作成または削除すること、ファイル読出し/書込み/シーク動作、ファイルパーミッションを変更することなどが含まれ得る。

【００４５】

挙動観測器ユニット202はまた、データネットワーク活動を監視することができ、データネットワーク活動には、接続のタイプ、プロトコル、ポート番号、デバイスが接続されるサーバ/クライアント、接続数、通信の容量または周波数などが含まれ得る。挙動観測器ユニット202は、送り出された、受信された、または妨害された通話またはメッセージ(たとえば、SMSなど)のタイプおよび数(たとえば、かけられた割増し料金の通話の数)を監視することを含む場合がある、電話ネットワーク活動を監視することができる。

【００４６】

挙動観測器ユニット202はまた、フォークの数、メモリアクセス動作、開かれたファイルの数などを監視することを含む場合がある、システムリソースの使用状況を監視することができる。挙動観測器ユニット202は、ディスプレイがオンかオフか、デバイスがロックされているかアンロックされているか、バッテリの残量、カメラの状態などの様々な要因を監視することを含む場合がある、モバイルコンピューティングデバイスの状態を監視することができる。挙動観測器ユニット202はまた、たとえば、重要なサービス(ブラウザ、コントラクトプロバイダなど)に対する意図、プロセス間通信(IPC)の程度、ポップアッ

プウィンドウなどを監視することによって、プロセス間通信を監視することができる。

【００４７】

挙動観測器ユニット202はまた、1つまたは複数のハードウェア構成要素のドライバの統計データおよび/またはステータスを監視/観測することができ、ハードウェア構成要素には、カメラ、センサ、電子ディスプレイ、WiFi通信構成要素、データコントローラ、メモリコントローラ、システムコントローラ、アクセスポート、タイマ、周辺デバイス、ワイヤレス通信構成要素、外部メモリチップ、電圧レギュレータ、発振器、フェーズロックループ、周辺ブリッジ、ならびに、プロセッサ、およびモバイルコンピューティングデバイス上で動作するクライアントをサポートするために使用される他の同様の構成要素が含まれ得る。

【００４８】

挙動観測器ユニット202はまた、モバイルコンピューティングデバイスおよび/またはモバイルコンピューティングデバイスのサブシステムの状態またはステータスを示す、1つまたは複数のハードウェアカウンタを監視/観測することができる。ハードウェアカウンタは、モバイルコンピューティングデバイス内で発生するハードウェア関連の活動またはイベントのカウントまたは状態を記憶するように構成された、プロセッサ/コアの専用レジスタを含む場合がある。

【００４９】

挙動観測器ユニット202はまた、ソフトウェアアプリケーションの活動または動作、アプリケーションダウンロードサーバ(たとえば、Apple(登録商標)のApp Storeサーバ)からのソフトウェアダウンロード、ソフトウェアアプリケーションによって使用されるモバイルコンピューティングデバイス情報、呼情報、テキストメッセージング情報(たとえば、SendSMS、BlockSMS、ReadSMSなど)、メディアメッセージング情報(たとえば、ReceiveMMS)、ユーザアカウント情報、位置情報、カメラ情報、加速度計情報、ブラウザ情報、ブラウザベース通信のコンテンツ、音声ベース通信のコンテンツ、短距離無線通信(たとえば、Bluetooth（登録商標）、WiFiなど)、テキストベース通信のコンテンツ、記録されたオーディオファイルのコンテンツ、電話帳または連絡先情報、連絡先リストなどを監視/観測することができる。

【００５０】

挙動観測器ユニット202は、ボイスメールを含む通信(VoiceMailComm)、デバイス識別子を含む通信(DeviceIDComm)、ユーザアカウント情報を含む通信(UserAccountComm)、カレンダ情報を含む通信(CalendarComm)、位置情報を含む通信(LocationComm)、記録されたオーディオ情報を含む通信(RecordAudioComm)、加速度計情報を含む通信(AccelerometerComm)などを含む、モバイルコンピューティングデバイスの伝送または通信を監視/観測することができる。

【００５１】

挙動観測器ユニット202は、コンパス情報、モバイルコンピューティングデバイス設定、バッテリ寿命、ジャイロスコープ情報、圧力センサ、磁気センサ、スクリーン活動などの使用、およびそれらに対する更新/変更を監視/観測することができる。挙動観測器ユニット202は、ソフトウェアアプリケーションとの間で通信される通知(AppNotifications)、アプリケーション更新などを監視/観測することができる。挙動観測器ユニット202は、第2のソフトウェアアプリケーションのダウンロードおよび/またはインストールを要求している第1のソフトウェアアプリケーションに関する条件またはイベントを監視/観測することができる。挙動観測器ユニット202は、パスワードのエントリなどのユーザ認証に関する条件またはイベントを監視/観測することができる。

【００５２】

挙動観測器ユニット202はまた、アプリケーションレベル、無線レベル、およびセンサレベルを含むモバイルコンピューティングデバイスの複数のレベルで、条件またはイベントを監視/観測することができる。アプリケーションレベルの観測には、顔認識ソフトウェアを介してユーザを観測すること、ソーシャルストリームを観測すること、ユーザによ

って入力された注釈を観測すること、PassBook/Google Wallet/Paypalの使用に関するイベントを観測することなどが含まれ得る。アプリケーションレベルの観測には、仮想プライベートネットワーク(VPN)の使用に関するイベント、および同期、音声探索、音声制御(たとえば、1語を発することによる電話のロック/アンロック)、言語翻訳機、計算用のデータのオフローディング、ビデオストリーミング、ユーザ活動のないカメラの使用、ユーザ活動のないマイクロフォンの使用などに関するイベントを観測することも含まれ得る。

【００５３】

無線レベルの観測には、無線通信リンクを確立するか、または情報を送信する前のモバイルコンピューティングデバイスとのユーザ対話、二重/多重のSIMカード、インターネットラジオ、モバイル電話テザリング、計算用のデータのオフローディング、デバイス状態通信、ゲームコントローラまたはホームコントローラとしての使用、車両通信、モバイルコンピューティングデバイス同期などのうちのいずれかまたは複数の存在、実在、または量を決定することが含まれ得る。無線レベルの観測には、測位、ピアツーピア(p2p)通信、同期、車両対車両通信、および/または機械対機械(m2m)通信のための、無線(WiFi、WiMax、Bluetooth（登録商標）など)の使用を監視することも含まれ得る。無線レベルの観測には、ネットワークトラフィックの使用、統計データ、またはプロファイルを監視することがさらに含まれ得る。

【００５４】

センサレベルの観測には、モバイルコンピューティングデバイスの使用環境および/または外部環境を決定するために、磁気センサまたは他のセンサを監視することが含まれ得る。たとえば、モバイルコンピューティングデバイスプロセッサは、電話が(たとえば、ホルスタ内の磁石を検知するように構成された磁石センサを介して)ホルスタ内にあるか、または(たとえば、カメラもしくは光センサによって検出される光の量を介して)ユーザのポケット内にあるかを判定するように構成される場合がある。たとえば、モバイルコンピューティングデバイスがホルスタに入れられている間に発生する、ユーザによるアクティブな使用(たとえば、写真またはビデオを撮ること、メッセージを送ること、音声通話を行うこと、音を録音することなど)に関する活動および機能は、(たとえば、ユーザを追跡またはスパイするために)デバイス上で実行されている不正なプロセスのサインである可能性があるので、モバイルコンピューティングデバイスがホルスタ内にあることを検出することは、悪意のある挙動を認識することに関係する場合がある。

【００５５】

使用環境または外部環境に関するセンサレベルの観測の他の例には、近距離場通信(NFC)を検出すること、クレジットカードスキャナ、バーコードスキャナ、またはモバイルタグリーダから情報を収集すること、USB充電源の存在を検出すること、キーボードまたは補助デバイスがモバイルコンピューティングデバイスに結合されていることを検出すること、モバイルコンピューティングデバイスが(たとえば、USBなどを介して)コンピューティングデバイスに結合されていることを検出すること、LED、フラッシュ、フラッシュライト、または光源が修正されているか、または(たとえば、緊急シグナリングアプリケーションなどを悪意をもって無効にして)無効にされていることを判定すること、スピーカまたはマイクロフォンがスイッチオンまたは電源オンにされていることを検出すること、充電イベントまたは電力イベントを検出すること、モバイルコンピューティングデバイスがゲームコントローラとして使用されていることを検出することなどが含まれ得る。センサレベルの観測には、医療もしくはヘルスケアのセンサから、またはユーザの体をスキャンすることから情報を収集すること、USB/オーディオジャックに差し込まれた外部センサから情報を収集すること、(たとえば、振動インターフェースなどを介して)触知センサまたは触覚センサから情報を収集すること、モバイルコンピューティングデバイスの熱状態に関する情報を収集することなども含まれ得る。

【００５６】

監視される要因の数を管理可能レベルまで削減するために、一態様では、挙動観測器ユニット202は、モバイルコンピューティングデバイスの劣化に寄与する可能性があるすべ

ての要因の小さいサブセットである、挙動または要因の初期セットを監視/観測することによって、粗い観測を実行することができる。一態様では、挙動観測器ユニット202は、ネットワークサーバ116および/またはクラウドサービスもしくはネットワーク118内の構成要素から、挙動および/または要因の初期セットを受信することができる。一態様では、挙動/要因の初期セットは、ネットワークサーバ116またはクラウドサービス/ネットワーク118から受信されたデータ/挙動モデル内で指定される場合がある。一態様では、挙動/要因の初期セットは、縮小された特徴モデル(RFM)内で指定される場合がある。

【００５７】

挙動分析器ユニット204および/または分類器ユニット208は、挙動観測器ユニット202から観測値を受信し、受信された情報(すなわち、観測値)を外部コンテキスト情報ユニット206から受信されたコンテキスト情報と比較し、経時的なデバイスの劣化に寄与する(もしくは寄与する可能性がある)か、または場合によってはデバイスに問題を引き起こす可能性がある(たとえば、悪意のある挙動)、受信された観測値に関連するサブシステム、プロセス、および/またはアプリケーションを識別することができる。

【００５８】

一態様では、挙動分析器ユニット204および/または分類器ユニット208は、経時的なデバイスの劣化に寄与する(もしくは寄与する可能性がある)か、または場合によってはデバイスに問題を引き起こす可能性がある、挙動、プロセス、またはプログラムを識別するために、情報の限定されたセット(すなわち、粗い観測値)を利用するための知能を含む場合がある。たとえば、挙動分析器ユニット204は、様々なユニット(たとえば、挙動観測器ユニット202、外部コンテキスト情報ユニット206など)から収集された(たとえば、観測値の形態の)情報を分析し、モバイルコンピューティングデバイスの正常動作の挙動を学習し、比較の結果に基づいて1つまたは複数の挙動ベクトルを生成するように構成される場合がある。挙動分析器ユニット204は、さらなる分析のために、生成された挙動ベクトルを分類器ユニット208に送ることができる。

【００５９】

分類器ユニット208は、挙動ベクトルを受信し、それらを1つまたは複数の挙動モジュールと比較して、特定のモバイルコンピューティングデバイスの挙動、ソフトウェアアプリケーション、またはプロセスが悪意があるか、良性であるか、または不審であるかを判定することができる。

【００６０】

挙動、ソフトウェアアプリケーション、またはプロセスが悪意があると分類器ユニット208が判定すると、分類器ユニット208は作動器ユニット210に通知することができ、作動器ユニット210は、悪意があるか、もしくは性能を劣化させると判定されたモバイルコンピューティングデバイスの挙動を修正するために様々な活動もしくは動作を実行し、かつ/または識別された問題を治癒、回復、隔離、もしくは場合によっては修復する動作を実行することができる。

【００６１】

さらなる態様では、挙動分析器ユニット204および/または分類器ユニット208は、ネットワークサーバ(たとえば、ネットワークサーバ116)から受信された悪意のある構成および経路構成のデータベースを参照して、モバイルコンピューティングデバイス102の現在の構成が経路構成であるかどうかを判定することができる。一態様では、分類器ユニット208(または挙動分析器ユニット204)は、ネットワークサーバから受信された悪意のある構成および経路構成のデータベースに含まれる1つまたは複数の経路構成と、モバイルコンピューティングデバイスの現在の構成を比較して、モバイルコンピューティングデバイス102の現在の構成が悪意のある構成および経路構成のデータベースに含まれる経路構成と一致するかどうかを判定することができる。たとえば、挙動分析器ユニット204は、モバイルコンピューティングデバイス上で現在動作している特定のアプリケーション用の挙動ベクトルを生成することができ、分類器ユニット208は、悪意のある構成および経路構成のデータベースに含まれる経路構成とアプリケーションの挙動ベクトルを比較して、アプ

リケーションの現在の構成がモバイルコンピューティングデバイス上の悪意のある挙動につながるかどうかを判定することができる。

【００６２】

モバイルコンピューティングデバイス102の現在の構成がネットワークサーバから受信された悪意のある構成および経路構成のデータベースに含まれる(すなわち、モバイルコンピューティングデバイス102の現在の構成が悪意のある挙動につながる)と分類器ユニット208が判定すると、分類器ユニット208は作動器ユニット210に通知することができ、作動器ユニット210は、そのような悪意のある挙動が起きる前に、様々なアクションまたは動作を実行して、モバイルコンピューティングデバイス上の悪意のある挙動または他の性能を劣化させる活動を防止することができる。

【００６３】

図3は、クラウドサービス/ネットワーク118とともに動作して、モバイルコンピューティングデバイス102上の悪意のある構成および悪意のある挙動につながる構成を知的かつ効率的に識別するように構成されたネットワークサーバ116を含む、一態様のシステム300における例示的な構成要素および情報フローを示す。図3に示された例では、ネットワークサーバ116は、クラウドユニット302と、悪意のある構成および経路構成のデータベース生成器ユニット304と、トレーニングデータユニット306とを含む。モバイルコンピューティングデバイス102は、挙動観測器ユニット202と、分類器ユニット208と、作動器ユニット210とを含む。一態様では、分類器ユニット208は、(図2に示された)挙動分析器ユニット204の中に、またはその一部として含まれる場合がある。一態様では、モデル生成器304はリアルタイムオンライン分類器であり得る。

【００６４】

クラウドユニット302は、クラウドサービス/ネットワーク118から大量の情報を受信し、悪意のある挙動につながる特徴、データポイント、および/または要因のすべてまたはほとんどを含む、完全またはロバストなデータ/挙動モデルを生成するように構成される場合がある。一態様では、クラウドサービス/ネットワーク118からの情報は、何らかの形態の悪意のある挙動を検出した複数のモバイルコンピューティングデバイスから報告された構成情報および構成履歴を含む場合がある。たとえば、複数のモバイルコンピューティングデバイスは、特定の構成についての悪意のある挙動を報告している場合があり、検出された悪意のある挙動につながるそれらの構成/状態/命令も報告している場合がある。

【００６５】

悪意のある構成および経路構成のデータベース生成器304は、クラウドユニット302において生成された完全な挙動モデルに基づく挙動モデルを含む、悪意のある構成および経路構成のデータベースを生成することができる。一態様では、挙動モデルを生成することは、クラウドユニット302によって生成された完全なモデル内に含まれる特徴およびデータポイントのサブセットを含む、1つまたは複数の縮小された特徴モデル(RFM)を生成することを含む場合がある。一態様では、悪意のある構成および経路構成のデータベース生成器304は、特定のモバイルコンピューティングデバイスの挙動が悪意のある挙動につながるかどうかを分類器ユニット208が最終的に判定することを可能にする最高の確率を有するように決定された情報を含む初期の特徴セット(たとえば、初期の縮小された特徴モデル)を含む、悪意のある構成および経路構成のデータベースを生成することができる。悪意のある構成および経路構成のデータベース生成器304は、生成された悪意のある構成および経路構成のデータベースを分類器ユニット208に送ることができる。

【００６６】

挙動観測器ユニット202は、モバイルコンピューティングデバイス102上でモバイルコンピューティングデバイスの挙動を監視/観測し、観測値を生成し、観測値を分類器ユニット208に送ることができる。分類器ユニット208は、リアルタイム分析動作を実行することができ、リアルタイム分析動作は、悪意のある構成および経路構成のデータベース内の挙動モデルを、挙動観測器ユニット202によって収集された構成情報と比較して、モバイルコンピューティングデバイス102の現在の状態が悪意のある挙動につながるかどうかを判

定することを含む場合がある。モバイルコンピューティングデバイス102の現在の構成が悪意のある構成および経路構成のデータベースに含まれる経路構成と一致すると分類器ユニット208が判定すると、分類器ユニット208は、モバイルコンピューティングデバイスの挙動が悪意のある挙動につながると判定することができる。図2を参照して上記で説明されたように、分類器ユニット208が一致を見つけると、分類器ユニット208は、将来の悪意のある挙動を回避するために対策を講じることを開始するように、作動器ユニット210に警告することができる。

【００６７】

別の態様では、モバイルコンピューティングデバイス102は、その動作の結果、および/またはモデルのアプリケーションに関連する成功率をネットワークサーバ116に送ることができる。たとえば、分類器ユニット208は、悪意のある構成および経路構成のデータベース内の一致を見つけない場合があるが、悪意のある挙動が依然起きる場合があり、それにより、モバイルコンピューティングデバイス102が悪意のある構成および経路構成のデータベースの次の配信に含めるようにネットワークサーバ116に報告する場合がある、以前検出されなかった悪意のある挙動(すなわち、防止におけるギャップ)を示す。ネットワークサーバ116は、モデル発生器304が使用するための結果/成功率に基づいて、(たとえば、トレーニングデータユニット306を介して)トレーニングデータを生成することができる。モデル生成器は、トレーニングデータに基づいて、更新された悪意のある構成および経路構成のデータベースを生成し、モバイルコンピューティングデバイス102および他のモバイルコンピューティングデバイスに更新された悪意のある構成および経路構成のデータベースを周期的に送ることができる。

【００６８】

図4は、悪意のある構成および経路構成を識別する悪意のある構成および経路構成のデータベースをモバイルコンピューティングデバイスに送るための、ネットワークサーバ上で実施され得る一態様の方法400を示す。方法400を実施する際に、ネットワークサーバは、複数のモバイルコンピューティングデバイスから情報を受信し、編集し、分析して、悪意のある挙動を示す構成、およびそれらの悪意のある構成につながる経路構成を識別する、集中型ハブとして機能することができる。サーバはまた、モバイルコンピューティングデバイスが、それらの現在の挙動(またはモバイルコンピューティングデバイス上で動作するアプリケーションもしくはプロセスの挙動)が悪意のある挙動に向かう傾向があるかどうかを検出することを可能にする報告を、複数のモバイルコンピューティングデバイスに提供することができる。

【００６９】

ブロック402において、ネットワークサーバは、複数のモバイルコンピューティングデバイスから構成情報および構成履歴を受信することができる。一態様では、モバイルコンピューティングデバイスが悪意のある挙動(たとえば、ハッキングされること、マルウェア、またはウイルスなど)を検出すると、モバイルコンピューティングデバイスは、モバイルコンピューティングデバイスが悪意のある挙動を発見したときのモバイルコンピューティングデバイスの構成を表す、挙動ベクトルまたは同様の情報をネットワークサーバに送ることができる。加えて、モバイルコンピューティングデバイスはまた、悪意のある挙動が検出されるまでに起きた構成の推移を記述する構成履歴を送ることができる。

【００７０】

一態様では、モバイルコンピューティングデバイスは、スタートアップ構成などの初期の構成から始まる構成変更のリストを保持することができる。たとえば、モバイルコンピューティングデバイスは、その挙動ベクトルが[0,2,1,0,...,4]であるとき、マルウェアの活動を検出することができる。モバイルコンピューティングデバイスは、挙動ベクトル[0,2,1,0,...,4]、および[0,2,1,0,...,4]から初期の構成(たとえば、[0,0,0,0,...,0])などの以前の構成にモバイルコンピューティングデバイスの構成を後退させるための情報をネットワークサーバに送ることができる。別の態様では、モバイルコンピューティングデバイスは、省略された構成履歴のみを保持する(すなわち、モバイルコンピューティン

グデバイスは、悪意のある構成につながるある特定の数の以前の構成のアカウントのみを保持することができる)ことによって、リソースを節約することができる。

【００７１】

ブロック404において、ネットワークサーバは、構成情報を分析して悪意のある構成を識別することができる。一態様では、ネットワークサーバは、悪意のある挙動を表すようにいくつかのモバイルコンピューティングデバイスによって報告された、同一または同様の挙動を整合することによって、悪意のある構成を識別することができる。さらなる態様では、ネットワークサーバは、ある特定の数または割合のモバイルコンピューティングデバイスが悪意があるように構成を識別するときのみ、悪意があるように構成を識別することができる。言い換えれば、ネットワークサーバは、報告するモバイルコンピューティングデバイスの間で何らかの合意があるときのみ、悪意があるように挙動をラベル付けするために、信頼性しきい値を採用することができる。

【００７２】

別の態様では、ネットワークサーバは、同じ能力または構成を共有しない場合がある様々なタイプおよびモデルのモバイルコンピューティングデバイスから構成情報を受信することができ、したがって、モバイルコンピューティングデバイスは、異なる構成情報/挙動ベクトルを有する場合がある。そのような態様では、ネットワークサーバは、様々なパターン照合のアルゴリズムまたは戦略を実施して、悪意のある構成、または複数のモバイルコンピューティングが通常悪意のある挙動を表すように報告する特定の特徴を検出することによって、悪意のある構成を識別することができる。言い換えれば、ネットワークサーバは、様々なモデルのモバイルコンピューティングデバイスからの数千の報告を編集し、モバイルコンピューティングデバイスが悪意のある挙動を検出したときに一貫して存在する構成特性を決定する。たとえば、様々なタイプのモバイルコンピューティングデバイスが、それらの構成が「画面オフ」、「連絡先情報にアクセスすること」、および「データを送信すること」を含んだときは、ほとんど常に悪意のある挙動を報告したと、ネットワークサーバは判定することができる。

【００７３】

ブロック406において、ネットワークサーバは、識別された悪意のある構成に基づいて経路構成を識別することができる。一態様では、経路構成は、悪意のある構成につながる「前兆」構成であり得る。言い換えれば、経路構成は、いくつかの状況下で悪意のある構成に発展するリスクがあり得る。たとえば、経路構成は、悪意のある構成であることから離れた1つまたは2つの構成変更であり得る。

【００７４】

一態様では、多数の構成履歴を受信した後、ネットワークサーバは、パターン認識または(構成履歴が状態間の遷移として提示される場合)状態機械分析を実施して、最終的な悪意のある構成につながる1つまたは複数のパターンまたは構成を発見することができる。言い換えれば、ネットワークサーバは、様々なモバイルコンピューティングデバイスからの構成履歴を使用して、悪意のある構成につながった以前の1つまたは複数の構成を識別するために、悪意のある構成から「逆探知」（つまり、「構成経路」に沿って）することができる。これらの以前の構成は、次の構成が悪意がある確率がかなりあると分析が判定すると、上記で定義されたように、経路構成として識別される場合がある。図7Aを参照して下記で説明されるように、所与の構成または状態は、次に実行される命令または動作に応じて、任意の数の次の構成または状態に発展するか、または変換される場合がある。したがって、悪意のある構成に先行する構成は、他の命令または動作が実行される場合、必ずしも悪意のある構成につながらない場合がある。これに対処するために、サーバ分析は、報告された情報から、所与の構成がどれほど頻繁に悪意のある構成に直接つながるかを判定し、頻繁に悪意のある構成につながる(すなわち、頻度がしきいの値または確率を超える)構成だけを「経路構成」として識別することができる。たとえば、ネットワークサーバは、構成が悪意のある挙動につながる可能性が10%を上回るときのみ、経路構成として構成を分類することができる。サーバ分析はまた、実行されたとき、経路構成を悪意の

ある構成に変換する命令/動作を識別することができる。

【００７５】

一態様では、ネットワークサーバは、ブロック404を参照して上記で説明された悪意のある構成/状態、1つまたは複数の中間構成、および始めの構成を最初に識別することができる。たとえば、ネットワークサーバは、「画面がオフの間に住所録情報を送信すること」が悪意のある構成であると最初に識別することができ、「逆探知」して、「表示画面がオフの間に住所録情報にアクセスすること」が、「画面がオフの間に住所録情報を送信すること」に頻繁につながる経路構成であると発見することができる。

【００７６】

一態様では、将来の悪意のある挙動の早期警戒サインとして経路構成を使用する有効性を増大させるために、ネットワークサーバは、構成が悪意のある構成から離れたしきい値の数の「ステップ」以内であるときのみ、その構成を「経路構成」であると分類することができる。サーバ分析はまた、悪意のある挙動に直接つながる次の経路構成、ならびに、実行されたとき、識別された経路構成から悪意のある構成への一連のステップをモバイルコンピューティングデバイスに通らせる命令/動作を識別することができる。

【００７７】

ブロック408において、ネットワークサーバは、識別された悪意のある構成および識別された経路構成を含む悪意のある構成および経路構成のデータベースを生成することができる。一態様では、悪意のある構成および経路構成のデータベースは、図5、図6、図8、図10、および図11を参照して下記で説明されるように、モバイルコンピューティングデバイスが悪意のある構成に入るリスクがあるかどうかをモバイルコンピューティングデバイスが評価することを可能にすることができる情報を含む場合がある。

【００７８】

上記で説明されたように、オプションのブロック410において、ネットワークサーバは、識別された経路構成ごとに悪意のある構成に遷移する確率を計算することができる。確率を計算するために、ネットワークサーバは、数千のモバイルコンピューティングデバイスの構成履歴を分析して、経路構成から悪意のある構成への遷移がどれほどの頻度で起きるかを判定することができる。たとえば、100,000個のモバイルコンピューティングデバイスからの報告を分析した後、ネットワークサーバは、70,000個のモバイルコンピューティングデバイスがある特定の経路構成から良性の構成に遷移し(すなわち、70%または0.7)、30,000個がその特定の経路構成から悪意のある構成に遷移した(すなわち、30%または0.3)と判定することができる。一態様では、ネットワークサーバは、下記図9に示されるように、各構成(すなわち、状態)および1つの構成から別の構成に遷移することについての確率を含むこの情報を、マルコフ連鎖分析において表すことができる。ネットワークサーバはまた、オプションのブロック412において、悪意のある構成および経路構成のデータベースに計算された確率を含めることができる。

【００７９】

同様に上記で説明されたように、オプションのブロック414において、ネットワークサーバは、識別された経路構成内にいる間に実行されたとき、悪意のある構成に導く悪意のある経路命令または経路動作を識別することができる。この動作では、ネットワークサーバは、挙動ベクトル情報および構成履歴を分析して、経路構成を悪意のある構成に変化させるコード、パラメータ、または他の命令を識別することができる。ネットワークサーバは、特定の経路構成との関連でそのような命令を識別することができる。したがって、ネットワークサーバは、実行されたとき、経路構成を悪意があるようにさせる命令を決定することができ、それにより、モバイルコンピューティングデバイスが悪意のある構成に発展するリスクがあるかどうかをより良く判定することが可能になる。言い換えれば、ネットワークサーバは、特定の経路構成内のモバイルコンピューティングデバイスが、本明細書において「悪意のある経路命令」と呼ばれるいくつかの命令を実行した後、悪意があるようになると判定することができる。悪意のある経路命令は、モバイルコンピューティングデバイスが経路構成内にいる間に実行されたときのみ、悪意のある挙動または悪意のあ

る構成をもたらす場合があることに留意されたい。このようにして、様々な態様は、ほとんどの状況では安全であり、悪意のある挙動とは関連しない命令/動作を認識し、それらに反応することを可能にするので、従来のマルウェア検出システムとは異なる。

【００８０】

ネットワークサーバは、オプションのブロック416において、悪意のある構成および経路構成のデータベースに、実行されたとき識別された悪意のある構成につながる識別された命令のリストを含めることができる。さらなる態様では、ネットワークサーバはまた、経路構成と、経路構成を悪意があるようにさせる悪意のある1つまたは複数の経路命令と間の関連付けを含めることができる。モバイルコンピューティングデバイスは、図11を参照して下記でさらに記載されるように、悪意のある挙動につながる命令のリストを含む悪意のある構成および経路構成のデータベースを利用して、そのような悪意のある挙動を回避することができる。

【００８１】

ブロック418において、ネットワークサーバは、複数のモバイルコンピューティングデバイスに悪意のある構成および経路構成のデータベースを送ることができる。様々な態様では、モバイルコンピューティングデバイスは、悪意のある挙動につながる可能性がある経路構成をプリエンプティブに識別する際に使用するために、悪意のある構成および経路構成のデータベースを使用することができる。一態様では、悪意のある構成および経路構成のデータベースは、モバイルコンピューティングデバイス上で動作する挙動分析器ユニット204および/または分類器ユニット208が利用することができる、有限状態機械における状態、経路、または挙動ベクトル値として、悪意のある構成および経路構成を提示することができる。

【００８２】

オプションの態様では、ネットワークサーバは、ブロック402においてモバイルコンピューティングデバイスから挙動ベクトル情報および構成履歴を継続的に受信するようなループにおいてプロセスを実行することができる。そのような態様では、ネットワークサーバは、回転ベースで挙動ベクトル情報および構成履歴を受信することができる。言い換えれば、ネットワークサーバは、モバイルコンピューティングデバイスから悪意のある挙動の情報をそれらが起きるにつれて継続的に受信することができ、より多くの挙動ベクトル情報および構成履歴が受信されるにつれて、悪意のある構成および経路構成を継続的に分析し識別することができる。そのため、ネットワークサーバは、受信された新しい情報に基づいて、モバイルコンピューティングデバイスに更新された悪意のある構成および経路構成のデータベースを継続的に送出するために、プロセスを繰り返すことができる。

【００８３】

図5は、悪意のある構成をプリエンプティブに識別するための、モバイルコンピューティングデバイスによって実施され得る一態様の方法500を示す。一態様では、モバイルコンピューティングデバイスは、悪意のある構成および経路構成を識別する悪意のある構成および経路構成のデータベースを利用して、モバイルコンピューティングデバイスの状態(またはモバイルコンピューティングデバイスのアプリケーション、プロセス、または構成要素の現在の構成)がいつ悪意のある挙動につながるかを判定することができる。その判定に基づいて、モバイルコンピューティングデバイスは、様々な手段を実施して、そのような悪意のある活動を回避または防止することができる。

【００８４】

ブロック502において、モバイルコンピューティングデバイスは、悪意のある構成および経路構成のデータベースを受信することができる。上記で説明されたように、図4を参照して記載された方法400のブロック418において、ネットワークサーバは、クラウドソーシングされた構成情報および/または構成履歴を使用して、他のモバイルコンピューティングデバイスによって報告された何らかの形態の悪意のある挙動につながるリスクを有するいくつかの構成を識別することができる。ネットワークサーバは、悪意のある構成および経路構成に関する情報を悪意のある構成および経路構成のデータベース内に編集するこ

とができ、モバイルコンピューティングデバイスに1つまたは複数の悪意のある構成および経路構成のデータベースを送ることができる。さらなる態様では、モバイルコンピューティングデバイスは、ネットワークサーバが管理する周期的なサービスの一部として、悪意のある構成および経路構成のデータベースを定期的に受信することができる(たとえば、モバイルコンピューティングデバイスは、悪意のある構成および経路構成のデータベースを受信するようにネットワークサーバに登録することができる)。

【００８５】

ブロック504において、モバイルコンピューティングデバイスは、その現在の構成を決定することができる。図2を参照して上述されたように、一態様では、挙動観測器ユニット202は、モバイルコンピューティングデバイスの現在の動作/ステータス/状態(すなわち、「挙動観測値」)、ならびにモバイルコンピューティングデバイスが経験した構成または状態の変更に関する様々なタイプの情報を収集することができる。

【００８６】

一態様では、モバイルコンピューティングデバイスは、挙動ベクトルを参照してモバイルコンピューティングデバイスの現在の構成を確認することができる。別の態様では、挙動分析器ユニット204は、挙動観測器ユニット202から挙動観測値を受信することができ、挙動分析器ユニット204は、挙動観測値を使用して、挙動ベクトルまたはモバイルコンピューティングデバイスの現在の構成の別の指示を生成することができる。たとえば、挙動分析器ユニット204は、データが送信されていて、画面がオフであることをモバイルコンピューティングデバイスの現在の構成が示すと判定することができる。挙動分析器ユニット204は、挙動観測値を使用して有限状態分析を行うことができ、それにより、挙動分析器ユニット204は、現在の状態(すなわち、現在の構成)への一連の状態遷移を追跡することによって、モバイルコンピューティングデバイスの現在の構成を決定することができる。有限状態機械分析を使用して現在の構成を決定することは、図7Aを参照して説明される下記でさらに詳細に記載される。

【００８７】

判定ブロック506において、モバイルコンピューティングデバイスは、悪意のある構成および経路構成のデータベースに基づいて、現在の構成が悪意のある構成につながるかどうかを判定することができる。言い換えれば、モバイルコンピューティングデバイスは、その現在の構成が経路構成であるかどうかを判定することができる。一態様では、挙動分析器ユニット204および/または分類器ユニット208は、ネットワークサーバから受信された悪意のある構成および経路構成のデータベースに含まれる経路構成および悪意のある構成と、モバイルコンピューティングデバイスの現在の構成(たとえば、モバイルコンピューティングデバイスの現在の構成を表す挙動ベクトル)を比較して、現在の構成が悪意のある構成および経路構成のデータベースに含まれる経路構成と一致するかどうかを判定することができる。

【００８８】

悪意のある構成および経路構成のデータベースに基づいて現在の構成が悪意のある構成につながらないとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック506=「No」)、モバイルコンピューティングデバイスは、ブロック510において正常に実行を続行することができる。モバイルコンピューティングデバイスがブロック504においてモバイルコンピューティングデバイスの現在の構成を決定することによって続行することができるようなループにおいて、プロセスは続行することができる。したがって、一態様では、モバイルコンピューティングデバイスは、その現在の構成を継続的にチェックして、将来の悪意のある挙動のリスクがないことを確認することができる。

【００８９】

悪意のある構成および経路構成のデータベースに基づいて現在の構成が悪意のある構成につながるとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック506=「Yes」)、モバイルコンピューティングデバイスは、オプションの判定ブロック507において、予防措置を実施して悪意のある構成を回避するべきかどうかを判定すること

ができる。

【００９０】

場合によっては、モバイルコンピューティングデバイスは、デバイスまたはデバイス上の構成要素の現在の構成が悪意のある構成につながると判定されるたびに予防措置を実施することによって、不十分な、または許容できない性能に遭遇する可能性がある。現在の構成が悪意のある構成に実際に発展するとは限らないので、モバイルコンピューティングデバイスは、セキュリティと性能の効果的なバランスを実現するために、あらかじめ定義されたしきい値を超える近い将来の悪意のある挙動の特定のリスクが存在するときのみ、予防措置を選択的に実施することができる。たとえば、モバイルコンピューティングデバイスは、図8を参照して下記でさらに記載されるように、現在の構成が悪意のある構成につながる可能性をかなり有するときのみ、予防措置を実施することができる。同様に、別の例では、モバイルコンピューティングデバイスは、図10を参照して下記でさらに記載されるように、現在の構成から悪意のある構成に入る計算されたリスクがあらかじめ定義された確率/リスクのしきい値を超えるときのみ、予防措置を実施することができる。

【００９１】

さらなる態様では、あらかじめ定義されたしきい値は、モバイルコンピューティングデバイス上のユーザインターフェース構成要素から受信されたユーザ入力に基づいて設定される場合があり、あらかじめ定義されたしきい値は、ユーザのセキュリティ対性能の優先度を反映する場合がある。たとえば、情報機関にいるユーザは、すべての悪意のあるアプリケーションが捕らえられたことを保証するために、より高いセキュリティ(すなわち、モバイルコンピューティングデバイスが予防措置を実施して将来の悪意のある構成を回避するより多くのインスタンス)を必要とする場合があり、そのようなユーザは、予防措置がほとんどまたはすべての時間で取られるように、低いしきい値を使用するようにモバイルコンピューティングデバイスを構成することができる。別の例では、別のユーザは、あらゆる悪意のある挙動を停止させることが性能への影響に値しないと決定する場合があり、悪意のある構成に入るリスクが高いしきい値を超えるときのみ、予防措置を実施するようにモバイルコンピューティングデバイスを構成することができる。

【００９２】

予防措置を実施して悪意のある構成を回避することは行わないとモバイルコンピューティングデバイスが判定すると(すなわち、オプションの判定ブロック507=「No」)、モバイルコンピューティングデバイスは、ブロック510において正常に実行を続行することができる。モバイルコンピューティングデバイスがブロック504においてモバイルコンピューティングデバイスの現在の構成を決定することによって続行することができるようなループにおいて、プロセスは続行することができる。したがって、一態様では、モバイルコンピューティングは、その現在の構成を継続的にチェックして、将来の悪意のある挙動のリスクがないことを確認することができる。

【００９３】

予防措置を実施して悪意のある構成を回避するとモバイルコンピューティングデバイスが判定すると(すなわち、オプションの判定ブロック507=「Yes」)、デバイスは、ブロック508において、予防措置を実施して悪意のある構成を回避することができる。一態様では、モバイルコンピューティングデバイスは、将来の悪意のある構成に関連するアプリケーション/プロセスを決定し、それらのアプリケーション/プロセスを終了、隔離、および/または治癒することなどの、様々な動作を実行して将来の悪意のある構成を回避することができる。予防措置を実施することは、図6を参照してより詳細に下記に記載される。

【００９４】

予防措置を実施した後、モバイルコンピューティングデバイスは、ブロック510において正常に実行を続行することができる。分析エンジンがブロック504においてモバイルコンピューティングデバイスの現在の構成を決定することによって続行することができるようなループにおいて、プロセスは続行することができる。

【００９５】

上記の説明はモバイルコンピューティングデバイスの現在の構成が悪意のある構成につながるかどうかを判定することに関係するが、さらなる態様では、モバイルコンピューティングデバイスまたはモバイルコンピューティングデバイス上で動作する構成要素は、代わりに、モバイルコンピューティングデバイス上で動作する個々のハードウェアまたはソフトウェアの構成要素の現在の構成が悪意のある構成につながるかどうかを判定することができる。たとえば、モバイルコンピューティングデバイスは、アプリケーションの現在の構成が悪意のある構成につながる経路構成であると判定することができる。これらの代替的な態様では、ネットワークサーバから受信された悪意のある構成および経路構成のデータベースは、個々のアプリケーションまたはハードウェア構成要素が近い将来に悪意のある構成のリスクがあるかどうかを判定するために、モバイルコンピューティングデバイス(またはモバイルコンピューティングデバイス上で動作する構成要素)のために必要な悪意のある構成および経路構成に関する情報を含む場合がある。

【００９６】

図6は、モバイルコンピューティングデバイスが現在経路構成内にいるときに、予防措置を実施して近い将来の悪意のある構成を回避するための、モバイルコンピューティングデバイス上で実施され得る一態様の方法600を示す。一態様では、モバイルコンピューティングデバイスが現在経路構成内にいると判定した後、モバイルコンピューティングデバイスは、現在の経路構成に関連する1つまたは複数のプロセスを減速または休止して、モバイルコンピューティングデバイスに、モバイルコンピューティングデバイス上で起きている他の挙動を検査して、それが近い将来の悪意のある挙動の危険が実際にあるかどうかを評価するのに十分な時間を提供することができる。

【００９７】

方法600の動作は、図5を参照して上述された方法500のブロック508の動作の一態様を実施する。したがって、モバイルコンピューティングデバイスは、モバイルコンピューティングデバイスが、現在、悪意のある挙動につながる経路構成内にいると判定した後(すなわち、判定ブロック506=「Yes」)、方法600の実施を開始することができる。

【００９８】

ブロック602において、モバイルコンピューティングデバイスは、現在の構成に関連する1つまたは複数のプロセスを識別することができる。一態様では、1つまたは複数のプロセスは、モバイルコンピューティングデバイス上で動作するアプリケーション、プログラム、スクリプト、ハードウェア構成要素、または他の構成要素であり得る。たとえば、現在の構成は「カメラオン」および「画面オフ」を含む場合があり、モバイルコンピューティングデバイスは、それらの特性をモバイルコンピューティングデバイス上で現在実行中のカメラアプリケーションと関連付けることができる。

【００９９】

別の態様では、モバイルコンピューティングデバイスは、モバイルコンピューティングデバイスの現在の経路構成に関連する1つまたは複数のプロセスを識別する、悪意のある構成および経路構成のデータベースに含まれる情報を受信することができ、モバイルコンピューティングデバイスは、この情報を活用して現在の構成に関係する1つまたは複数のプロセスを識別することができる。たとえば、モバイルコンピューティングデバイスが経路構成内にいると判定した後、モバイルコンピューティングデバイスは、悪意のある構成および経路構成のデータベースを参照して、モバイルコンピューティングデバイス上で動作しているソーシャルメディアアプリケーションが経路構成に関連し、モバイルコンピューティングデバイスを悪意のある挙動に導くことに関与しそうであることを発見することができる。さらなる態様では、悪意のある構成および経路構成のデータベースは、経路構成にリンクされた2つ以上のプロセスまたは構成要素の識別情報を含む場合がある。

【０１００】

ブロック604において、モバイルコンピューティングデバイスは、1つまたは複数のプロセスの実行を減速することができる。一態様では、1つまたは複数のプロセスを減速することは、図5を参照して記載された方法500の判定ブロック506において上述されたように

、現在の構成が経路構成であることを最初に発見した後すぐに起きる場合がある、悪意のある挙動の進行中の発展を阻止する最初の予防措置であり得る。別の態様では、モバイルコンピューティングデバイスは、代わりに、1つまたは複数のプロセスの実行を完全に停止することができる。

【０１０１】

1つまたは複数のプロセスの実行を減速または休止することは、モバイルコンピューティングデバイスの機能性および性能を一時的に低下させる可能性があり、そのようなコストは、近い将来の悪意のある挙動を回避することの潜在的な恩恵が上回る可能性がある。モバイルコンピューティングデバイスは、モバイルコンピューティングデバイスが現在経路構成内にいると判定した後のみ、プロセスの動作に賢明に介入することができるので、様々な態様はこれらのコストをさらに低減する。したがって、将来の悪意のある挙動の検出されたリスクが存在するとき(すなわち、モバイルコンピューティングデバイスが現在経路構成内にいるとき)のみアクションを取ることによって、モバイルコンピューティングデバイスは、モバイルコンピューティングデバイス上で動作している1つまたは複数のプロセスまたは構成要素に対して最小限の影響をもたらしながら、それ自体を保護することができる。

【０１０２】

図6に戻ると、ブロック606において、モバイルコンピューティングデバイスは、モバイルコンピューティングデバイス上で現在起きている他の挙動を検査することができる。一態様では、1つまたは複数のプロセスが減速または停止している間、モバイルコンピューティングデバイスは、現在の構成が悪意のある挙動に向かう傾向があるかどうかをより良く予測する試みにおいて、他の進行中の活動を調査することができる。たとえば、モバイルコンピューティングデバイスは、他の異例または不審な挙動を発見する試みにおいて、1つまたは複数のプロセスに関係するか、またはそれらによって使用されるアプリケーションまたはハードウェア構成要素を走査することができる。別の態様では、他の挙動の検査は、包括的かつ完全な走査および分析を含む場合があり、1つまたは複数のプロセスを減速すると、現在の構成が悪意のある構成に発展する前に、モバイルコンピューティングデバイスがこれらの包括的な走査を完了することが可能になり得る。

【０１０３】

オプションの判定ブロック608において、モバイルコンピューティングデバイスは、現在の構成が悪意があるようになっているかどうかの最終的な判定を行う前に、より多くの検査が必要とされるかどうかを判定することができる。より多くの検査が必要とされるとモバイルコンピューティングデバイスが判定すると(すなわち、オプションの判定ブロック608=「Yes」)、モバイルコンピューティングデバイスは、オプションのブロック610において、モバイルコンピューティングデバイス上で現在起きている他の挙動の検査を続行することができる。モバイルコンピューティングデバイスは、現在の構成が悪意があるようになっているかどうか、および/または何がモバイルコンピューティングデバイスを悪意のある挙動に向かう傾向にさせている可能性があるかの最終的な判定を行うことが適度に可能になるまで、他の挙動の検査を続行することができる。

【０１０４】

したがって、より多くの検査が必要とされないとモバイルコンピューティングデバイスが判定すると(すなわち、オプションの判定ブロック608=「No」)、モバイルコンピューティングデバイスは、判定ブロック612において、他の挙動の検査に基づいて、現在の構成が悪意のある構成につながる可能性がかなりあるかどうかを判定することができる。1つまたは複数のプロセスが、画面がオフである間に写真を撮るカメラアプリケーションである(すなわち、現在の構成が「カメラオン」および「画面オフ」である)例では、ユーザの入力に応答して画面がオンになろうとしていることをモバイルコンピューティングデバイス上の他の活動が示すので、モバイルコンピューティングデバイスは、現在の構成が悪意のある状態(たとえば、「画面オフ」、「カメラオン」、および「カメラデータの送信オン」)に入っていないと結論づけることができる。この例では、現在の構成は、悪意のあ

る構成ではない可能性がある「カメラオン」および「画面オン」に遷移すると予想される。

【０１０５】

現在の構成が悪意のある構成につながる可能性がかなりあることはないとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック612=「No」)、モバイルコンピューティングデバイスは、ブロック618において、1つまたは複数のプロセスを正常動作に戻すことができる。一態様では、1つまたは複数のプロセスは、正常な速度で動作を続行することができる。

【０１０６】

現在の構成が悪意があるようになっているとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック612=「Yes」)、モバイルコンピューティングデバイスは、オプションのブロック614において、1つまたは複数のプロセスを中断することができる。一態様では、1つまたは複数のプロセスを中断することは、1つまたは複数のプロセスの実行を完全に停止すること、またはそれらを終了することを含む場合がある。

【０１０７】

ブロック616において、モバイルコンピューティングデバイスは、1つまたは複数のプロセスに対して予防措置を実施することができる。一態様では、モバイルコンピューティングデバイスは、1つまたは複数のプロセスをモバイルコンピューティングデバイス上の他のアプリケーションまたは構成要素と対話することから切り離すこと、および最初の良性の構成から1つまたは複数のプロセスをリセット/リスタートすることを含む、様々な技法を実施して悪意のある挙動を回避することができる。他の技法には、良性であると知られている以前の処理ポイントに1つまたは複数のプロセスを復元すること(たとえば、アプリケーションを以前のバージョンに戻すこと)が含まれ得る。モバイルコンピューティングデバイスはまた、ブロック618において、1つまたは複数のプロセスを正常動作に戻すことができる。

【０１０８】

モバイルコンピューティングデバイスは、図5を参照して上述された方法500のブロック504において、現在の構成を決定することによって、続行することができる。

【０１０９】

図7Aは、有限状態機械(「FSM」)700として表された一態様のモバイルコンピューティングデバイス上の構成および構成間の遷移の状態図を示す。

【０１１０】

一態様では、FSM700は、モバイルコンピューティングデバイスの可能な構成(「画面オン」、「画面オフ」、「データを送ること」など)の各々についての状態(すなわち、構成)を含む場合がある。FSM700はまた、モバイルコンピューティングデバイスの構成が、1つの状態/構成から別の状態/構成への遷移とともに、経時的にどのように変化するかを表すことができる。たとえば、FSM700は、特定の構成A702(たとえば、「画面オン」および「音声オフ」)が別の構成B'704(たとえば、「画面オン」および「音声オン」)に遷移する場合があることを示すことができる。

【０１１１】

一態様では、ネットワークサーバは、複数のモバイルデバイスから取得された構成情報および/または構成履歴に基づいて、FSM700を生成することができる。たとえば、ネットワークサーバは、複数のモバイルコンピューティングデバイスから構成情報を受信することができ、この情報を編集して、モバイルコンピューティングデバイスの構成/状態およびそれらの構成間の遷移を表すFSMを生成することができる。一例では、ネットワークサーバは、数千のモバイルコンピューティングデバイスから構成履歴を受信することができ、最初の構成(たとえば、「電源オン」状態)から様々な中間構成および最終構成への構成遷移を表すFSMを生成することができる。別の態様では、様々なモバイルコンピューティングデバイスが様々な特徴または機能を有する場合があるので、ネットワークサーバは、同様の特性(たとえば、同じモデル番号、製造業者など)を共有するモバイルコンピューテ

ィングデバイス用の専用FSMを生成することができる。

【０１１２】

別の態様では、ネットワークサーバは、FSM700内の各構成/状態を、良性の構成、不審な構成、または悪意のある構成として分類することができる。一態様では、ネットワークサーバは、複数のモバイルコンピューティングデバイスから受信された構成情報に基づいて、挙動分析を実行することができる。たとえば、ネットワークサーバは、悪意のある挙動の報告に一貫してリンクされた構成(すなわち、悪意のある構成)と、それらが悪意があるかどうかを判定するためにより多くの検査を必要とする構成(すなわち、不審な構成)と、悪意のある挙動を示さない構成(すなわち、良性の構成)とを識別することができる。したがって、さらなる態様では、ネットワークサーバは、構成およびそれらの構成間の遷移、ならびに各構成の分類を記述するFSMを生成することができる。

【０１１３】

加えて、別の態様では、FSM700において構成を分類した後、ネットワークサーバは、図4を参照して上述されたように、悪意のある構成から「逆探知」して、それらの悪意のある構成につながるリスクをかなり有する構成(すなわち、経路構成)を識別することができる。たとえば、ネットワークサーバは、複数のモバイルデバイスから受信された構成情報および構成履歴を使用して、悪意のある挙動に向かう傾向の始まりを一貫して示す特定の構成を決定することができる。

【０１１４】

別の態様では、FSM700を生成し、FSM700において構成を分類し、FSM700において悪意のある構成につながる経路構成を識別した後、ネットワークサーバは、図4を参照して上述された悪意のある構成および経路構成のデータベース内などで、FSM700に関するこの情報をモバイルコンピューティングデバイスに送ることができる。

【０１１５】

一態様では、モバイルコンピューティングデバイスは、FSM700を利用してその構成をリアルタイムで追跡することができる。たとえば、正常動作の間、モバイルコンピューティングデバイスは、FSM700内の構成遷移を追跡して、その現在の構成を記録することができる。別の態様では、モバイルコンピューティングデバイスは、その現在の構成が(たとえば、ネットワークサーバから受信された悪意のある構成および経路構成のデータベース内で示されるような)経路構成であるかどうかを判定することができる。モバイルコンピューティングデバイスが現在経路構成内にいるとモバイルコンピューティングデバイスが判定すると、モバイルコンピューティングデバイスは、FSM700を分析して、モバイルコンピューティングデバイスが近い将来遷移する可能性がある潜在的な構成を決定することができる。言い換えれば、モバイルコンピューティングデバイスは、有限状態機械分析を実行し、モバイルコンピューティングデバイスの現在の構成から「前方探知」して、次に起きる可能性がある構成(すなわち、潜在的な将来の構成)を決定することができる。

【０１１６】

一態様では、潜在的な将来の構成は、モバイルコンピューティングデバイスが特定の数の遷移の後到達する可能性がある構成であり得る。たとえば、モバイルコンピューティングデバイスの現在の構成は、「画面オフおよび音声オフ」であり得る。したがって、モバイルコンピューティングデバイスは、「画面オンおよび音声オフ」ならびに「画面オフおよび音声オン」などの、1回の遷移/構成変更で到達可能であり得る、2つの潜在的な将来の構成を有する場合がある。さらなる例では、モバイルコンピューティングデバイスは、2回の遷移で到達可能な別の潜在的な将来の構成(たとえば、「画面オンおよび音声オン」)に遷移する場合がある。

【０１１７】

一態様では、潜在的な将来の構成を識別した後、モバイルコンピューティングデバイスは、それらの分類を決定することができ、それらの潜在的な将来の構成の分類に基づいて、将来悪意のある構成に入ることを防止または回避するために必要な対策を講じることができる。一例では、モバイルコンピューティングデバイスは、現在、良性であり経路構成

ではない(すなわち、現在の構成を考えると将来の悪意のある挙動の識別されたリスクがない)構成A702内にいる場合がある。この場合、モバイルコンピューティングデバイスは、正常に動作を続行することができる。言い換えれば、モバイルコンピューティングデバイスは、相当なコンピュータリソースを消費する必要なしに、その現在の状態が悪意のある挙動につながるかどうかを、リアルタイムで(すなわち、実際の正常な動作中に)迅速にチェックすることができる。

【０１１８】

上記の例の構成では、モバイルコンピューティングデバイスは、モバイルコンピューティングデバイスを構成A702から構成B704に遷移させる可能性がある、経時的な1つまたは複数の構成変更を経験する場合がある。構成B704に入ると、モバイルコンピューティングデバイスは、その現在の構成が経路構成であると判定することができる。このようにして、モバイルコンピューティングデバイスは、近い将来悪意のある構成に遷移するリスクがあると判定することができる。この時点で、モバイルコンピューティングデバイスは、構成B704に関係する1つまたは複数のプロセスを減速または停止して、悪意のある挙動が近い将来に起きる可能性を評価する追加の時間を可能にすることができる。このようにして、将来の悪意のある挙動の識別されたリスクが存在するまで予防措置の開始を待つことによって、モバイルコンピューティングデバイスは、不必要な計算を回避することができる。

【０１１９】

一態様では、経路構成に入った後、モバイルコンピューティングデバイスは、図7Bを参照して記載されるテーブル725に示されたように、その現在の構成の分類および潜在的な将来の構成の分類に基づいて、近い将来の悪意のある挙動の可能性がかなりあるかどうかを判定することができる。図9を参照して下記でさらに記載される別の態様では、モバイルコンピューティングデバイスは、ネットワークサーバから受信された情報を利用して、近い将来に起きる悪意のある挙動の確率(たとえば、0.0から1.0までの値)を決定することができ、デバイスは、悪意のある挙動の確率がある特定のしきい値の確率(たとえば、25%)を超えると、悪意のある挙動の可能性がかなりあると判定することができる。

【０１２０】

一例では、構成B704が経路構成であるとモバイルコンピューティングデバイスが判定した後、モバイルコンピューティングデバイスは、構成B704が良性であり、1回のステップで到達可能な潜在的な将来の構成(すなわち、構成C706および構成D708)が、それぞれ良性および悪意があると判定することができる。一態様では、モバイルコンピューティングデバイスは、テーブル725を参照し、テーブル参照に基づいて、構成B704が悪意のある構成に直接つながるので、将来の悪意のある挙動の可能性がかなりあると結論づけることできる。

【０１２１】

別の例では、モバイルコンピューティングデバイスの現在の構成が構成E710であるとき、モバイルコンピューティングデバイスは、唯一の潜在的な将来の構成(すなわち、構成F712)が良性なので、悪意のある挙動に最終的につながる可能性はごくわずかであると判定することができる。しかしながら、モバイルコンピューティングデバイスが構成F712に遷移した場合、モバイルコンピューティングデバイスは、潜在的な将来の構成がすべて悪意があるので、将来の悪意のある挙動のリスクがかなりあると判定することができる。

【０１２２】

モバイルコンピューティングデバイスの現在の構成が構成G714である別の例では、モバイルコンピューティングデバイスは、構成G714が不審なので、現在の構成が悪意のある挙動につながる可能性がかなりあると判定することができる。一態様では、モバイルコンピューティングデバイス(またはネットワークサーバ)は、構成が良性か悪意があるかを判定するためにより多くの情報が必要とされるとき、構成を不審として分類することができる。

【０１２３】

一態様では、将来の悪意のある挙動の可能性を決定した後、モバイルコンピューティングデバイスは、判定された可能性に基づいて、様々な予防措置を実施して将来の悪意のある挙動を回避するべきかどうかを判定することができる。判定された可能性に基づいて取るべき適切な手段を決定するプロセスは、図8を参照して下記に記載される。

【０１２４】

図8は、現在の構成が悪意のある挙動につながる可能性がかなりあるときに予防措置を実施するための、モバイルコンピューティングデバイス上で実施され得る一態様の方法800を示す。一態様では、モバイルコンピューティングデバイスが現在経路構成内にいる(すなわち、近い将来の悪意のある挙動のリスクがある)と判定した後、モバイルコンピューティングデバイスは、モバイルコンピューティングデバイスの現在の構成およびモバイルコンピューティングデバイスがその現在の構成から遷移する可能性がある構成に基づいて、近い将来に悪意のある挙動に遭遇する可能性がかなりあるかどうかを判定することができる。

【０１２５】

方法800の動作は、図5を参照して上述された方法500のブロック508の動作の一態様を実施する。したがって、モバイルコンピューティングデバイスは、図5を参照して上述されたように、現在の構成が経路構成であると判定した後(判定ブロック506=「Yes」)、方法800の実施を開始することができる。

【０１２６】

ブロック602において、モバイルコンピューティングデバイスは、図6を参照して上述されたように、現在の構成に関連する1つまたは複数のプロセスを識別することができる。モバイルコンピューティングデバイスはまた、ブロック604において、1つまたは複数のプロセスの実行を減速することができる。一態様では、1つまたは複数のプロセスの実行を減速することによって、モバイルコンピューティングデバイスは、近い将来の悪意のある挙動を回避するために、予防措置が必要であるかどうかを判定する追加の時間を有することができる。

【０１２７】

ブロック802において、モバイルコンピューティングデバイスは、現在の構成の分類を決定することができる。一態様では、モバイルコンピューティングデバイスは、現在の構成が良性であるか、悪意があるか、または不審であるかを判定することができる。一態様では、ネットワークサーバは、図7A～図7Bを参照して(たとえば、モバイルコンピューティングデバイスの構成およびそれらの構成間の遷移を記述するFSMの一部として)記載されたように、モバイルコンピューティングデバイスの様々な構成の分類を決定している可能性があり、モバイルコンピューティングデバイスによって受信された悪意のある構成および経路構成のデータベースの一部として分類を送っている可能性がある。

【０１２８】

別の態様では、悪意のある構成および経路構成のデータベースの一部としてネットワークサーバからモバイルコンピューティングデバイスの現在の構成の分類を受信するのではなく、モバイルコンピューティングデバイス上で動作する挙動分析器ユニット204および/または分類器ユニット208は、代わりに、図2を参照して上記で説明されたように、モバイルコンピューティングデバイスの現在の構成の分類をローカルに決定することができる。たとえば、挙動分析器ユニット204は、挙動観測器ユニットから現在の挙動観測値を受信することができ、モバイルコンピューティングデバイスの現在の構成を表す挙動ベクトルを生成することができる。分類器ユニット208は、次いで、モバイルコンピューティングデバイスの現在の構成が良性であるか、不審であるか、または悪意があるかを生成された挙動ベクトルが示すかどうかを判定することができる。

【０１２９】

オプションの判定ブロック804において、モバイルコンピューティングデバイスは、現在の構成が悪意があるかどうかを判定することができる。現在の構成が悪意があるとモバイルコンピューティングデバイスが判定すると(すなわち、オプションの判定ブロック804

=「Yes」)、モバイルコンピューティングデバイスは、オプションのブロック808において、現在の構成に関連する1つまたは複数のプロセスに対して治療手段を実施して、現在の悪意のある構成を解消することができる。一態様では、モバイルコンピューティングデバイスの現在の構成が悪意があるとき、悪意のある挙動を防止することは遅すぎる場合があり、したがって、モバイルコンピューティングデバイスは、治療手段を実施して続行中の悪意のある挙動を停止する必要があり得る。たとえば、モバイルコンピューティングデバイスは、マルウェア、ウイルス、破損ファイルなどについて走査し、それらを削除することができる。モバイルコンピューティングデバイスはまた、ブロック618において、1つまたは複数のプロセスを正常動作に戻すことができる。モバイルコンピューティングデバイスはまた、図5を参照して上述された方法500のブロック504において、現在の構成を決定することによって、実行を続行することができる。

【０１３０】

現在の構成が悪意がないとモバイルコンピューティングデバイスが判定すると(すなわち、オプションの判定ブロック804=「No」)、モバイルコンピューティングデバイスは、ブロック806において、潜在的な将来の構成の分類を決定することができる。一態様では、モバイルコンピューティングデバイスは、ブロック802において現在の構成の分類を決定することを参照して上記で説明されたように、潜在的な将来の構成の分類を決定することができる。たとえば、モバイルコンピューティングデバイスは、ネットワークサーバから送られた悪意のある構成および経路構成のデータベースの一部として、潜在的な将来の構成の分類を受信している可能性がある。別の例では、モバイルコンピューティングデバイス(またはモバイルコンピューティングデバイス上で動作している1つまたは複数の構成要素)は、潜在的な将来の構成に基づいて挙動ベクトルを生成し、それらの挙動ベクトルを分類することができる。

【０１３１】

ブロック810において、モバイルコンピューティングデバイスは、現在の構成および潜在的な将来の構成の分類に基づいて、現在の構成が悪意のある構成につながる可能性を決定することができる。一態様では、モバイルコンピューティングデバイスは、図7Bを参照して上述されたテーブル725のような参照テーブルを参照して、現在の構成が悪意のある挙動につながる可能性を決定することができる。

【０１３２】

判定ブロック812において、モバイルコンピューティングデバイスは、現在の構成が悪意のある構成につながる可能性をかなり有しているかどうかを判定することができる。たとえば、モバイルコンピューティングデバイスは、現在の構成および潜在的な将来の構成のすべてが良性であるとき、近い将来の悪意のある挙動のリスクがごくわずかであると判定することができる。別の例では、モバイルコンピューティングデバイスは、現在の構成が良性である場合でも、潜在的な将来の構成のうちの1つまたは複数が悪意があるとき、悪意のある挙動のリスクがかなりあると判定することができる。

【０１３３】

悪意のある構成につながる可能性がごくわずかであるとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック812=「No」)、モバイルコンピューティングデバイスは、ブロック618において、1つまたは複数のプロセスを正常動作に戻すことができる。モバイルコンピューティングデバイスは、図5を参照して上述された方法500のブロック504において、現在の構成を決定することによって、実行を続行することができる。

【０１３４】

現在の構成が悪意のある挙動につながる可能性がかなりあるとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック812=「Yes」)、モバイルコンピューティングデバイスは、オプションのブロック614において、1つまたは複数のプロセスの実行を場合によっては中断することができる。一態様では、モバイルコンピューティングデバイスは、1つまたは複数のプロセスの実行を停止して、任意の将来の悪意のある挙動を回避するのに十分な時間をモバイルコンピューティングデバイスに提供することができる

。

【０１３５】

ブロック616において、モバイルコンピューティングデバイスは、図6に示された方法600のブロック616において上述されたように、1つまたは複数のプロセスに対して予防措置を実施することができる。一態様では、予防措置を実施することは、1つまたは複数のプロセスの性能または構成を調整して、予想される悪意のある挙動を回避することを含む場合がある。たとえば、1つまたは複数のプロセスは、良性であると知られている以前の構成に戻される場合がある。

【０１３６】

ブロック618において、モバイルコンピューティングデバイスは、1つまたは複数のプロセスを正常動作に戻すことができる。(図示されていない)一態様では、近い将来の悪意のある挙動の可能性がかなりあることはもはやないとモバイルコンピューティングデバイスが判定すると、モバイルコンピューティングデバイスは、1つまたは複数のプロセスの正常実行を再開することができる。モバイルコンピューティングデバイスは、図5を参照して上述された方法500のブロック504において、現在の構成を決定することによって、実行を続行することができる。

【０１３７】

図9は、モバイルコンピューティングデバイス上で悪意のある挙動を予測することで使用するためのマルコフ連鎖分析を示す。一態様では、図7Aを参照して上述されたFSM分析のように、マルコフ連鎖分析は、モバイルコンピューティングデバイスの様々な構成およびそれらの構成間の遷移を記述することができる。さらに、マルコフ連鎖分析は、1つの構成から次の構成への遷移の確率を含む場合もある。

【０１３８】

一態様では、ネットワークサーバは、図7Aに示されたFSM700を参照して上述されたように、複数のモバイルコンピューティングデバイスから受信された構成情報/構成履歴からFSM900を生成することができる。したがって、FSM900は、様々な構成/状態およびそれらの構成の間の遷移を含む場合がある。ネットワークサーバはまた、FSM900内の構成ごとに分類(すなわち、良性である、悪意がある、または不審である)を決定し、悪意のある挙動につながる1つまたは複数の構成(すなわち、経路構成)を決定することができる。

【０１３９】

加えて、別の態様では、ネットワークサーバは、経路構成が特定の潜在的な将来の構成に(たとえば、「画面オフ」から「画面オン」に)直接遷移する確率を計算することができる。たとえば、ネットワークサーバは、複数のモバイルコンピューティングデバイスから報告を受信することができ、報告された遷移の総数のうちの各経路構成が潜在的な将来の構成に遷移した回数を決定することができる。たとえば、図9に示されたように、ネットワークサーバは、構成B904内のモバイルコンピューティングデバイスが、10%の時間、構成C906に遷移し、90%の時間、構成D908に遷移したと計算している可能性がある。

【０１４０】

さらなる態様では、現在の構成が経路構成であると判定した後、モバイルコンピューティングデバイスは、潜在的な将来の構成の分類および現在の構成が潜在的な将来の構成の各々に遷移する確率を決定することができる。悪意のある潜在的な将来の構成に直接遷移する確率がある特定のしきい値を超える場合、モバイルコンピューティングデバイスは、予防措置を実施して予想される悪意のある挙動を回避することができる。たとえば、構成E910内のモバイルコンピューティングデバイスは、悪意のある構成に直接遷移する0%の可能性を有する場合がある。この状況では、モバイルコンピューティングデバイスは、悪意のある構成に直接遷移する確率がしきい値の確率を下回るので、予防措置を実施しない可能性がある。しかしながら、構成F912内のモバイルコンピューティングデバイスは、悪意のある状態に直接遷移する100%(0.7+0.3=1.0=100%)の可能性を有する場合があり、したがって、モバイルコンピューティングデバイスは、予防措置を実施して、現在の構成が悪意のある挙動につながる非常に高い確率を回避することができる。

【０１４１】
別の態様では、ネットワークサーバは、図4のオプションのブロック410を参照して上述されたように、経路構成ごとに悪意のある構成に最終的に遷移する確率を計算することができる。一例では、構成H916内のモバイルコンピューティングデバイスは、2つの悪意のある構成(すなわち、構成D908および構成I918)に最終的に遷移する可能性がある。構成H916から構成Dに遷移する確率は9%(構成B904に遷移する10%の確率と、次いで構成B904から構成D908に遷移する90%の確率)である。構成H916から構成I918に遷移する確率は2.5%(構成H916から構成G914に遷移する5%の確率と、構成G914から構成I918に遷移する50%の確率)であり得る。したがって、構成H内のモバイルコンピューティングデバイスは、悪意のある構成に最終的につながる全体で11.5%(9%+2.5%=11.5%)の可能性を有する場合がある。
【０１４２】
ネットワークサーバは、経路構成が悪意のある挙動に最終的につながる確率をモバイルコンピューティングデバイスが決定することを可能にすることができる確率情報を、モバイルコンピューティングデバイスに送ることができる。別の態様では、モバイルコンピューティングデバイスは、経路構成から潜在的な将来の構成に遷移する確率(すなわち、現在の構成から次の構成に直接遷移する確率)を受信することができ、現在の経路構成が悪意のある挙動に最終的につながる確率をローカルに計算することができる。
【０１４３】
図10は、現在の構成が悪意のある構成につながる確率に基づいて、予防措置を実施して悪意のある挙動を回避するための、モバイルコンピューティングデバイス上で実施され得る一態様の方法1000を示す。方法1000の動作は、図5を参照して上述された方法500の動作の一態様を実施する。一態様では、モバイルコンピューティングデバイスが現在経路構成内にいると判定した後、モバイルコンピューティングデバイスは、モバイルコンピューティングデバイスの現在の構成から悪意のある構成に遷移する確率がある特定のしきい値を超えたとき、予防措置を実施して悪意のある挙動を回避することができる。
【０１４４】
ブロック1002において、モバイルコンピューティングデバイスは、構成遷移確率を含む悪意のある構成および経路構成のデータベースをネットワークサーバから受信することができる。図9を参照して説明されたように、構成遷移確率は、経路構成が悪意のある構成に遷移する確率を含む、モバイルコンピューティングデバイスが1つの構成から別の構成に遷移する可能性を記述することができる。一態様では、構成遷移確率は、経路構成から悪意のある構成に直接遷移する確率(すなわち、1回だけの遷移で悪意のある構成に入る確率)を記述することができる。別の態様では、構成遷移確率は、経路構成から悪意のある構成に最終的に遷移する全体的な確率(すなわち、1回以上の遷移で悪意のある構成に入る確率)を示すことができる。
【０１４５】
ブロック504において、モバイルコンピューティングデバイスは、図5を参照して上述された方法500のブロック504を参照して説明されたように、その現在の構成を決定することができる。たとえば、挙動分析器ユニットは、挙動観測値に基づいて、モバイルコンピューティングデバイスの現在の構成を記述する挙動ベクトルを生成することができる。
【０１４６】
判定ブロック506において、モバイルコンピューティングデバイスは、悪意のある構成および経路構成のデータベースに基づいて、現在の構成が悪意のある構成につながるかどうかを判定することができる。言い換えれば、モバイルコンピューティングデバイスは、ネットワークサーバから受信された悪意のある構成および経路構成のデータベースに含まれる経路構成のリストと、モバイルコンピューティングデバイスの現在の構成を比較することによって、モバイルコンピューティングデバイスが経路構成であるかどうかを判定することができる。現在の構成が経路構成ではないとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック506=「No」)、その現在の構成が経路構成である(すなわち、将来の悪意のある挙動のリスクがある)とモバイルコンピューティングデバイ

スが判定するまで、プロセスはループで続行することができる。

【０１４７】

現在の構成が経路構成であるとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック506=「Yes」)、モバイルコンピューティングデバイスは、ブロック602において、現在の構成に関連する1つまたは複数のプロセスを識別することができる。モバイルコンピューティングデバイスはまた、ブロック604において、1つまたは複数のプロセスの実行を減速することができる。一態様では、モバイルコンピューティングデバイスは、図6を参照して上述された方式と同様の方式で、1つまたは複数のプロセスを識別し、それらの実行を減速することができる。

【０１４８】

オプションの態様では、モバイルコンピューティングデバイスは、オプションの判定ブロック804において、現在の構成が悪意があるかどうかを判定することができる。たとえば、モバイルコンピューティングデバイスがネットワークサーバから悪意のある構成および経路構成のデータベースを受信するときまで、モバイルコンピューティングデバイスの現在の構成は、すでに悪意のある構成であり得る。現在の構成が悪意があるとモバイルコンピューティングデバイスが判定すると(すなわち、オプションの判定ブロック804=「Yes」)、モバイルコンピューティングデバイスは、オプションのブロック808において、1つまたは複数のプロセスに対して治療手段を実施して、現在の悪意のある構成を解消することができる。たとえば、モバイルコンピューティングデバイスは、マルウェアについて走査しそれを削除する従来の方法を採用することができる。モバイルコンピューティングデバイスは、ブロック618において、1つまたは複数のプロセスを正常動作に戻すことができる。ブロック504において、モバイルコンピューティングデバイスが経路構成の始まりに入るときをモバイルコンピューティングデバイスが認識することを続行することができるようなループにおいて、プロセスは続行することができる。

【０１４９】

現在の構成が悪意がないとモバイルコンピューティングデバイスが判定すると(すなわち、オプションの判定ブロック804=「No」)、モバイルコンピューティングデバイスは、ブロック1004において、現在の構成および構成遷移確率に基づいて、現在の構成が悪意のある構成につながる確率を決定することができる。一態様では、モバイルコンピューティングデバイスは、ネットワークサーバから受信された構成遷移確率を参照し、モバイルコンピューティングデバイスがその現在の構成から悪意のある構成に直接遷移する確率を決定することができる。

【０１５０】

別の態様では、モバイルコンピューティングデバイスは、現在の構成から1つまたは複数の悪意のある構成への遷移を追跡することができる。モバイルコンピューティングデバイスは、ネットワークサーバから受信された構成遷移確率を利用して、モバイルコンピューティングデバイスが、1つまたは複数の遷移の後、その現在の構成から悪意のある構成に遷移する確率を計算することができる。たとえば、モバイルコンピューティングデバイスは、その現在の構成から中間構成に遷移する75%の可能性と、中間構成から悪意のある構成に遷移する50%の可能性とを有する場合がある。したがって、現在の構成が悪意のある構成に最終的につながる37.5%(75%*50%=37.5%)の可能性があり得る。

【０１５１】

判定ブロック1006において、モバイルコンピューティングデバイスは、現在の構成が悪意のある構成につながる確率がリスクしきい値を超えるかどうかを判定することができる。一態様では、リスクしきい値は、予防措置を実施するコストが悪意のある挙動を回避する利益を超える場合があるポイントを表すことができる。たとえば、現在の構成に関連する1つまたは複数のプロセスを以前の状態またはバージョンに戻すコストは、現在の構成が悪意のある構成に実際に発展する可能性が5%しかないとき、コスト効率が良くない場合がある。予防措置を実施するコストは、一般に、現在の構成が悪意のある挙動につながる可能性が95%あるとき、モバイルコンピューティングデバイスの全体的な性能を大きく利

する場合がある。図5を参照して上述されたように、リスクしきい値は、ユーザインターフェースデバイスから受信されたユーザ入力に基づいて設定される場合があり、それにより、ユーザが所望のレベルのセキュリティを指定することが可能になる。

【０１５２】

現在の構成が悪意のある構成につながる確率がリスクしきい値を超えないとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック1006=「No」)、モバイルコンピューティングデバイスは、図6を参照して上述されたブロック618において、1つまたは複数のプロセスを正常動作に戻すことができる。ブロック504において現在の構成を決定することによってモバイルデバイスが続行することができるようなループにおいて、プロセスは続行することができる。

【０１５３】

現在の構成が悪意のある構成につながる確率がリスクしきい値を超えるとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック1006=「Yes」)、モバイルコンピューティングデバイスは、オプションのブロック614において、1つまたは複数のプロセスの実行を場合によっては中断することができる。モバイルコンピューティングデバイスはまた、図6を参照して上述されたブロック616において、1つまたは複数のプロセスに対して予防措置を実施することができる。モバイルコンピューティングデバイスはまた、ブロック618において、1つまたは複数のプロセスを正常動作に戻すことができる。

【０１５４】

ブロック504において、モバイルコンピューティングデバイスが経路構成の始まりに入るときをモバイルコンピューティングデバイスが認識することを続行することができるようなループにおいて、プロセスは続行することができる。

【０１５５】

図11は、悪意のある挙動をもたらすと判定された命令の実行を防止するための、モバイルコンピューティングデバイス上で実施され得る一態様の方法1100を示す。方法1100の動作は、図5を参照して上述された方法500の動作の一態様を実施する。

【０１５６】

ブロック1102において、モバイルコンピューティングデバイスは、悪意のある経路命令のリストを含む悪意のある構成および経路構成のデータベースをネットワークサーバから受信することができる。図4のオプションのブロック414を参照して上述されたように、ネットワークサーバは、複数のモバイルデバイスから受信された構成情報および構成履歴から、悪意のある挙動をもたらすことに関連する命令のリストを編集することができる。たとえば、モバイルコンピューティングデバイスは、それらが悪意のある挙動を発見した時点におけるそれらの構成、ならびに悪意のある挙動につながる、モバイルコンピューティングデバイスが実行した命令のリストの両方を報告することができる。このようにして、一態様では、ネットワークサーバは、これらの潜在的に悪意のある経路命令を含む悪意のある構成および経路構成のデータベースを生成することができ、それにより、モバイルコンピューティングデバイスが下記に記載されるようにこれらの命令の実行について監視し、それを防止することが可能になる。

【０１５７】

ブロック504において、モバイルコンピューティングデバイスは、図5を参照して上述された方法500のブロック504を参照して説明されたように、現在の構成を決定することができる。たとえば、挙動分析器ユニットは、挙動観測値に基づいて、モバイルコンピューティングデバイスの現在の構成を記述する挙動ベクトルを生成することができる。

【０１５８】

判定ブロック506において、モバイルコンピューティングデバイスは、悪意のある構成および経路構成のデータベースに基づいて、現在の構成が悪意のある構成につながるかどうかを判定することができる。言い換えれば、モバイルコンピューティングデバイスは、ネットワークサーバから受信された悪意のある構成および経路構成のデータベースに含まれる経路構成のリストと、モバイルコンピューティングデバイスの現在の構成を比較する

ことによって、モバイルコンピューティングデバイスが経路構成であるかどうかを判定することができる。現在の構成が経路構成ではないとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック506=「No」)、その現在の構成が経路構成である(すなわち、将来の悪意のある挙動のリスクがある)とモバイルコンピューティングデバイスが判定するまで、プロセスはループで続行することができる。

【０１５９】

現在の構成が経路構成であるとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック506=「Yes」)、モバイルコンピューティングデバイスは、ブロック602において、現在の構成に関連する1つまたは複数のプロセスを識別することができる。モバイルコンピューティングデバイスはまた、ブロック604において、1つまたは複数のプロセスの実行を減速することができる。一態様では、モバイルコンピューティングデバイスは、図6を参照して上述された方式と同様の方式で、1つまたは複数のプロセスを識別し、それらの実行を減速することができる。

【０１６０】

ブロック1104において、モバイルコンピューティングデバイスは、1つまたは複数のプロセスによって実行されようとしている1つまたは複数の命令を決定することができる。一態様では、モバイルコンピューティングデバイスは、1つまたは複数のプロセスが実行しようとしている命令をプレビューすることができ、ネットワークサーバから受信された悪意のある構成および経路構成のデータベースに含まれる悪意のある経路命令のリストと、それらの命令を比較することができる。

【０１６１】

判定ブロック1106において、モバイルコンピューティングデバイスは、実行されようとしている1つまたは複数の命令が悪意のある経路命令のリスト内にあるかどうかを判定することができる。たとえば、モバイルコンピューティングデバイスは、1つまたは複数のプロセスが起動しようとしている関数呼出しの名前を発見することができ、モバイルコンピューティングデバイスは、悪意のある構成および経路構成のデータベースをチェックして、それらの関数呼出しの名前が悪意のある経路命令のリストに含まれるかどうかを判定する。

【０１６２】

実行されようとしている1つまたは複数の命令が悪意のある経路命令のリスト内にないとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック1106=「No」)、モバイルコンピューティングデバイスは、図6を参照して上述されたブロック618において、1つまたは複数のプロセスを正常動作に戻すことができる。ブロック504において現在の構成を決定することによってモバイルコンピューティングデバイスが続行することができるようなループにおいて、プロセスは続行することができる。

【０１６３】

実行されようとしている1つまたは複数の命令が悪意のある経路命令のリスト内にあるとモバイルコンピューティングデバイスが判定すると(すなわち、判定ブロック1106=「Yes」)、モバイルコンピューティングデバイスは、オプションのブロック614において、1つまたは複数のプロセスの実行を場合によっては中断することができる。

【０１６４】

ブロック1108において、モバイルコンピューティングデバイスは、実行されようとしている1つまたは複数の命令の実行を防止することができる。一態様では、モバイルコンピューティングデバイスは、1つもしくは複数のプロセスをリセット/リスタートするか、または1つもしくは複数のプロセスを以前の良性の構成に戻すことができる。別の態様では、モバイルコンピューティングデバイスは、悪意があると判定された1つまたは複数の命令を実行しないように1つまたは複数のプロセスを防止することができるにすぎず、そうでない場合、モバイルコンピューティングデバイスは、ブロック618において、1つまたは複数のプロセスが正常に動作することを可能にすることができる。

【０１６５】

モバイルコンピューティングデバイスは、モバイルコンピューティングデバイスが経路構成に入ったかどうかを常に監視するように、ブロック504に戻る連続ループにおいて、その態様のプロセスを実行することができる。

【０１６６】

様々な態様は、様々なモバイルコンピューティングデバイスのいずれかに実装される場合があり、その一例が図12に示される。モバイルコンピューティングデバイス1200は、内部メモリ1206に結合されたプロセッサ1202を含む場合がある。プロセッサ1202は、汎用または特定の処理タスクに指定された1つまたは複数のマルチコア集積回路であり得る。内部メモリ1206は、揮発性メモリまたは不揮発性メモリであり得るし、セキュアなメモリおよび/もしくは暗号化されたメモリ、またはセキュアでないメモリおよび/もしくは暗号化されていないメモリ、またはそれらの任意の組合せでもあり得る。プロセッサ1202は、抵抗感知タッチスクリーン、容量感知タッチスクリーン、赤外線感知タッチスクリーンなどの、タッチスクリーンパネル1212に結合される場合もある。加えて、モバイルコンピューティングデバイス1200のディスプレイは、タッチスクリーン機能を有する必要はない。

【０１６７】

モバイルコンピューティングデバイス1200は、互いに結合され、かつ/またはプロセッサ1202に結合された、通信を送信および受信するための1つまたは複数の無線信号トランシーバ1208(たとえば、Peanut(登録商標)、Bluetooth(登録商標)、Zigbee(登録商標)、Wi-Fi、RF無線)、およびアンテナ1210を有する場合がある。トランシーバ1208およびアンテナ1210は、様々なワイヤレス送信のプロトコルスタックおよびインターフェースを実装するために、上述の回路とともに使用される場合がある。モバイルコンピューティングデバイス1200は、セルラーネットワークを介する通信を可能にし、プロセッサに結合されたセルラーネットワークワイヤレスモデムチップ1216を含む場合がある。

【０１６８】

モバイルコンピューティングデバイス1200は、プロセッサ1202に結合された周辺デバイス接続インターフェース1218を含む場合がある。周辺デバイス接続インターフェース1218は、1つのタイプの接続を受け入れるように単独で構成される場合があるか、または、USB、FireWire、Thunderbolt、もしくはPCIeなどの様々なタイプの物理接続および通信接続を共通もしくはプロプライエタリに受け入れるように、構成される場合がある。周辺デバイス接続インターフェース1218は、同様に構成された周辺デバイス接続ポート(図示せず)に結合される場合もある。

【０１６９】

モバイルコンピューティングデバイス1200は、オーディオ出力を提供するためのスピーカ1214を含む場合もある。モバイルコンピューティングデバイス1200は、本明細書で説明された構成要素のすべてまたはいくつかを収容するための、プラスチック、金属、または材料の組合せから構築された筐体1220を含む場合もある。モバイルコンピューティングデバイス1200は、使い捨てまたは充電可能なバッテリなどの、プロセッサ1202に結合された電源1222を含む場合もある。充電可能なバッテリは、モバイルコンピューティングデバイス1200の外部にある電源から充電電流を受けるために、周辺デバイス接続ポートに結合される場合もある。モバイルコンピューティングデバイス1200は、ユーザ入力を受け取るための物理ボタン1224を含む場合もある。モバイルコンピューティングデバイス1200は、モバイルコンピューティングデバイス1200をオンオフするための電源ボタン1226を含む場合もある。

【０１７０】

上述された様々な態様はまた、図13に示されたラップトップコンピュータ1300などの様々なモバイルコンピューティングデバイス内に実装される場合がある。多くのラップトップコンピュータは、コンピュータのポインティングデバイスとして働くタッチパッドのタッチ面1317を含み、したがって、タッチスクリーンディスプレイを装備した上述のモバイルコンピューティングデバイス上で実施されるものと同様のドラッグジェスチャ、スクロールジェスチャ、およびフリックジェスチャを受け取ることができる。ラップトップコン

ピュータ1300は、通常、揮発性メモリ1312、およびフラッシュメモリのディスクドライブ1313などの大容量不揮発性メモリに結合されたプロセッサ1311を含む。加えて、コンピュータ1300は、プロセッサ1311に結合されたワイヤレスデータリンクおよび/または携帯電話トランシーバ1316に接続され得る、電磁放射を送受信するための1つまたは複数のアンテナ1308を有する場合がある。コンピュータ1300は、プロセッサ1311に結合されたフロッピー（登録商標）ディスクドライブ1314およびコンパクトディスク(CD)ドライブ1315を含む場合もある。ノートブック構成では、コンピュータの筐体は、すべてがプロセッサ1311に結合された、タッチパッド1317、キーボード1318、およびディスプレイ1319を含む。コンピューティングデバイスの他の構成には、よく知られているように、(たとえば、USB入力を介して)プロセッサに結合されたコンピュータマウスまたはトラックボールが含まれ得るし、それらは様々な態様と連携して使用される場合もある。

【０１７１】

態様の方法の一部は、態様の方法を実行している間にモバイルコンピューティングデバイスプロセッサによってアクセスされ得る、正常動作の挙動のデータベースを保持することなどの、処理のいくつかがサーバ内で発生する、クライアントサーバアーキテクチャにおいて遂行される場合がある。そのような態様は、図14に示されたサーバ1400などの、様々な市販のサーバデバイスのいずれかに実装される場合がある。そのようなサーバ1400は、通常、揮発性メモリ1402、およびディスクドライブ1403などの大容量の不揮発性メモリに結合された、プロセッサ1401を含む。サーバ1400は、プロセッサ1401に結合されたフロッピー（登録商標）ディスクドライブ、コンパクトディスク(CD)またはDVDのディスクドライブ1404を含む場合もある。サーバ1400は、他のブロードキャストシステムのコンピュータおよびサーバに結合されたローカルエリアネットワークなどの、ネットワーク1406とデータ接続を確立するための、プロセッサ1401に結合されたネットワークアクセスポート1405を含む場合もある。プロセッサ1401は、上述された様々な態様の機能を含む、様々な機能を実行するようにソフトウェア命令(アプリケーション)によって構成され得る、任意のプログラマブルマイクロプロセッサ、マイクロコンピュータ、または1つもしくは複数の多重プロセッサチップであり得る。通常、ソフトウェアアプリケーションは、それらがアクセスされ、プロセッサ1401にロードされる前に、内部メモリ1402、1403に記憶される場合がある。プロセッサ1401は、アプリケーションソフトウェア命令を記憶するのに十分な内部メモリを含む場合がある。

【０１７２】

上記の方法の説明およびプロセスフロー図は、単に説明のための例として提供され、様々な態様のステップが提示された順序で実行されなければならないことを要求または意味するものではない。当業者によって諒解されるように、上記の態様におけるステップの順序は、いかなる順序でも実施することができる。「したがって」、「次いで」、「次に」などの単語は、ステップの順序を限定するものではなく、これらの単語は、単に、方法の説明を通して読者を導くために使用される。さらに、たとえば、冠詞「a」、「an」、または「the」を使用する、単数形での請求項の要素へのいかなる言及も、要素を単数形に限定するものとして解釈されるべきではない。

【０１７３】

本出願で使用する「構成要素」、「モジュール」、「システム」、「エンジン」、「ジェネレータ」、「マネージャ」などの用語は、限定はしないが、特定の動作または機能を実施するように構成された、ハードウェア、ファームウェア、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などのコンピュータ関連エンティティを含むものとする。たとえば、構成要素は、限定はしないが、プロセッサ上で動作しているプロセス、プロセッサ、オブジェクト、実行ファイル、実行スレッド、プログラム、および/またはコンピュータであり得る。実例として、コンピューティングデバイス上で動作しているアプリケーションとコンピューティングデバイスの両方は、構成要素と呼ばれる場合がある。1つまたは複数の構成要素は、プロセスおよび/または実行スレッドの中に存在する場合があり、1つの構成要素は、1つのプロセッサもしくはコアに局在する

場合があり、かつ/または2つ以上のプロセッサもしくはコアの間に分散する場合がある。加えて、これらの構成要素は、様々な命令および/またはデータ構造を記憶している様々な非一時的コンピュータ可読媒体から実行することができる。構成要素は、ローカルプロセスおよび/またはリモートプロセス、関数呼出しまたはプロシージャ呼出し、電子信号、データパケット、メモリ読出し/書込み、ならびに他の知られているネットワーク、コンピュータ、プロセッサ、および/またはプロセス関連の通信方法によって通信することができる。

【０１７４】

本明細書で開示された態様に関して記載された様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装される場合がある。ハードウェアおよびソフトウェアのこの互換性を明確に示すために、様々な例示的な構成要素、ブロック、モジュール、回路、およびステップが、全般にそれらの機能に関して上述されている。そのような機能がハードウェアとして実装されるか、またはソフトウェアとして実装されるかは、特定の適用例および全体的なシステムに課された設計制約に依存する。当業者は、記載された機能を特定の適用例ごとに様々な方法で実施することができるが、そのような実施の決定は、本発明の範囲からの逸脱を引き起こすものとして解釈されるべきではない。

【０１７５】

本明細書で開示された態様に関して記載された様々な例示的な論理、論理ブロック、モジュール、および回路を実装するために使用されるハードウェアは、本明細書に記載された機能を実施するように設計された、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、またはそれらの任意の組合せを用いて実装または実施される場合がある。汎用プロセッサはマルチプロセッサであり得るが、代替として、プロセッサは任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械であり得る。プロセッサは、コンピューティングデバイスの組合せ、たとえば、DSPとマルチプロセッサとの組合せ、複数のマルチプロセッサ、DSPコアと連携する1つもしくは複数のマルチプロセッサ、または任意の他のそのような構成として実装される場合もある。代替として、いくつかのステップまたは方法は、所与の機能に特有の回路によって実施される場合がある。

【０１７６】

1つまたは複数の例示的な態様では、記載された機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せに実装される場合がある。ソフトウェアに実装される場合、機能は、非一時的コンピュータ可読媒体または非一時的プロセッサ可読媒体に、1つまたは複数の命令またはコードとして記憶される場合がある。本明細書で開示された方法またはアルゴリズムのステップは、非一時的なコンピュータ可読記憶媒体またはプロセッサ可読記憶媒体に存在する場合があるプロセッサ実行可能ソフトウェアモジュールにおいて具現化される場合がある。非一時的なコンピュータ可読またはプロセッサ可読の記憶媒体は、コンピュータまたはプロセッサによってアクセスされ得る任意の記憶媒体であり得る。限定ではなく例として、そのような非一時的なコンピュータ可読またはプロセッサ可読の媒体は、RAM、ROM、EEPROM、FLASHメモリ、CD-ROMもしくは他の光ディスクストレージ、磁気ディスクストレージもしくは他の磁気記憶デバイス、または命令もしくはデータ構造の形態で所望のプログラムコードを記憶するために使用され得るし、コンピュータによってアクセスされ得る任意の他の媒体を含む場合がある。本明細書で使用するディスク(disk)およびディスク(disc)は、コンパクトディスク(disc)(CD)、レーザディスク(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(DVD)、フロッピー（登録商標）ディスク(disk)、およびブルーレイディスク(disc)を含み、ディスク(disk)は、通常、データを磁気的に再生し、ディスク(disc)は、データをレーザで光学的に再生する。上記の組合せも、非一時的なコンピュータ可読およびプロセッサ可読の媒体の範囲内に含まれる。加えて、方法またはアルゴリズムの動作は、コンピュータプログラム製品

に組み込まれる場合がある、非一時的なプロセッサ可読媒体および/またはコンピュータ可読媒体上のコードおよび/または命令の1つまたは任意の組合せまたはセットとして存在する場合がある。

【０１７７】

開示された態様の上記の説明は、任意の当業者が本発明を作成または使用することができるように提供される。これらの態様に対する様々な修正は、当業者には容易に明らかであり、本明細書で定義された一般的な原理は、本発明の要旨または範囲から逸脱することなく、他の態様に適用される場合がある。したがって、本発明は、本明細書に示された態様に限定されるものではなく、以下の特許請求の範囲、ならびに、本明細書で開示された原理および新規の特徴と一致する最も広い範囲を与えられるべきである。

【符号の説明】

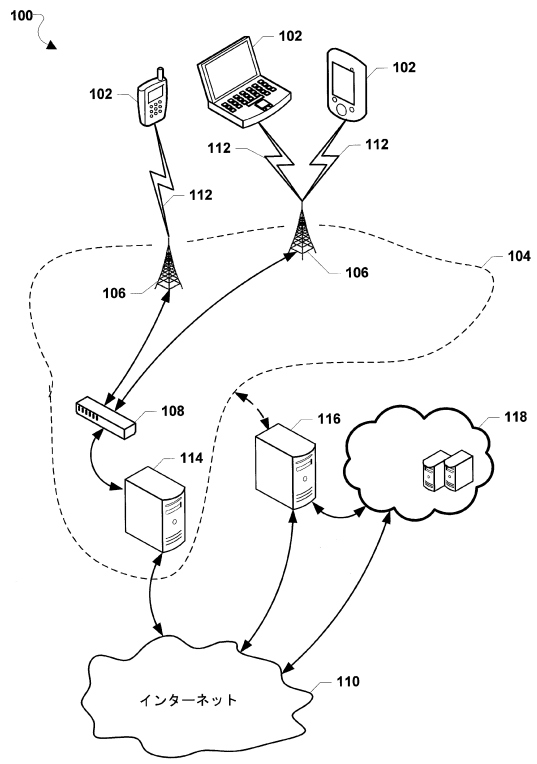
【０１７８】

100 通信システム
102 モバイルコンピューティングデバイス
104 セル電話ネットワーク
106 セル基地局
108 ネットワーク運用センタ
110 インターネット
112 双方向ワイヤレス通信リンク
114 サーバ
116 ネットワークサーバ
118 クラウドサービスプロバイダネットワーク
202 挙動観測器ユニット
204 挙動分析器ユニット
206 外部コンテキスト情報ユニット
208 分類器ユニット
210 作動器ユニット
300 システム
302 クラウドユニット
304 悪意のある構成および経路構成のデータベース生成器ユニット
306 トレーニングデータユニット
400 方法
402 ブロック
404 ブロック
406 ブロック
408 ブロック
410 オプションのブロック
412 オプションのブロック
414 オプションのブロック
416 オプションのブロック
418 ブロック
500 方法
502 ブロック
504 ブロック
506 判定ブロック
507 オプションの判定ブロック
508 ブロック
510 ブロック
600 方法
602 ブロック

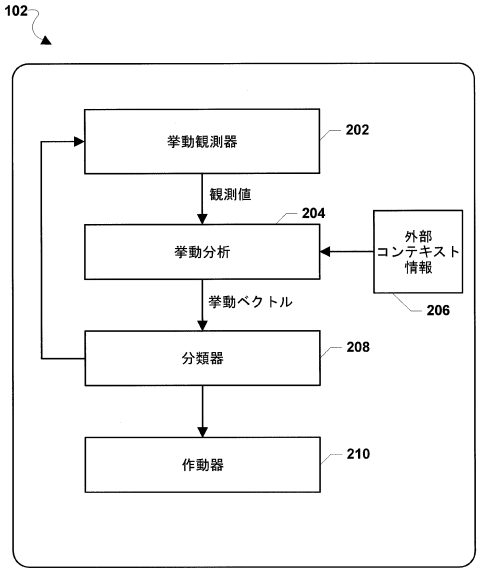
604 ブロック
606 ブロック
608 オプションの判定ブロック
610 オプションのブロック
612 判定ブロック
614 オプションのブロック
616 ブロック
618 ブロック
700 有限状態機械(「FSM」)
702 構成A
704 構成B
706 構成C
708 構成D
710 構成E
712 構成F
714 構成G
725 テーブル
800 方法
802 ブロック
804 オプションの判定ブロック
806 ブロック
808 オプションのブロック
810 ブロック
812 判定ブロック
900 FSM
904 構成B
906 構成C
908 構成D
910 構成E
912 構成F
914 構成G
916 構成H
918 構成I
1000 方法
1002 ブロック
1004 ブロック
1006 判定ブロック
1100 方法
1102 ブロック
1104 ブロック
1106 判定ブロック
1108 ブロック
1200 モバイルコンピューティングデバイス
1202 プロセッサ
1206 内部メモリ
1208 無線信号トランシーバ
1210 アンテナ
1212 タッチスクリーンパネル
1214 スピーカ
1216 セルラーネットワークワイヤレスモデムチップ

1218 周辺デバイス接続インターフェース
1220 筐体
1222 電源
1224 物理ボタン
1226 電源ボタン
1300 ラップトップコンピュータ
1308 アンテナ
1311 プロセッサ
1312 揮発性メモリ
1313 ディスクドライブ
1314 フロッピー（登録商標）ディスクドライブ
1315 コンパクトディスク(CD)ドライブ
1316 ワイヤレスデータリンクおよび/または携帯電話トランシーバ
1317 タッチパッド
1318 キーボード
1319 ディスプレイ
1400 サーバ
1401 プロセッサ
1402 揮発性メモリ
1403 ディスク(disk)ドライブ
1404 ディスク(disc)ドライブ
1405 ネットワークアクセスポート
1406 ネットワーク

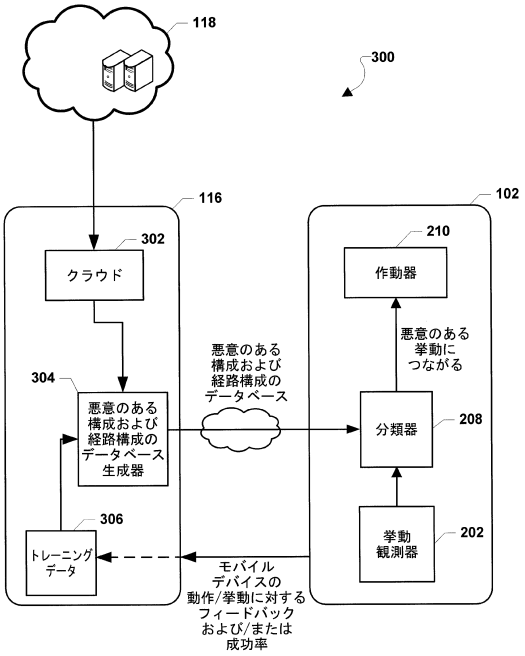
【図１】



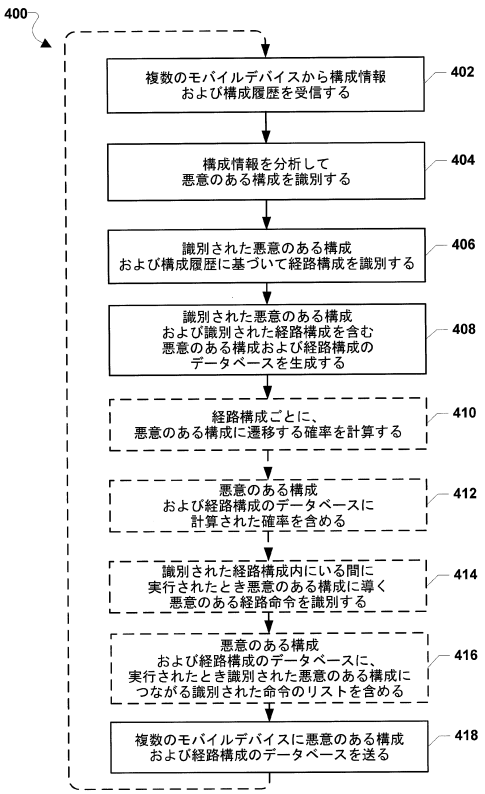
【図２】



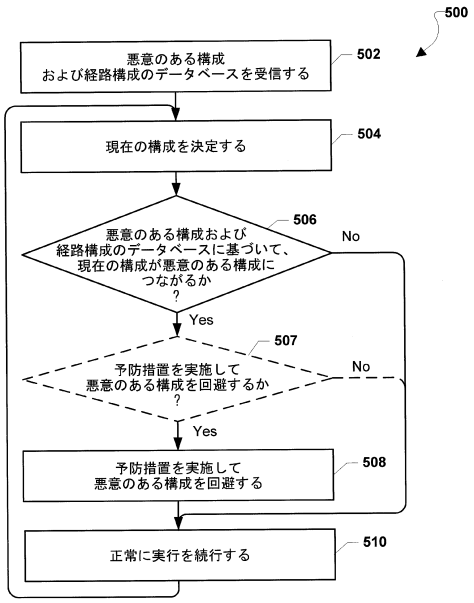
【図３】


118
300
116
102
302
クラウド
210
作動器
悪意のある
挙動に
つながる
悪意のある
構成および
経路構成の
データベース
304
悪意のある
構成および
経路構成の
データベース
生成器
分類器
208
306
トレーニング
データ
挙動
観測器
202
モバイル
デバイスの
動作/挙動に対する
フィードバック
および/または
成功率

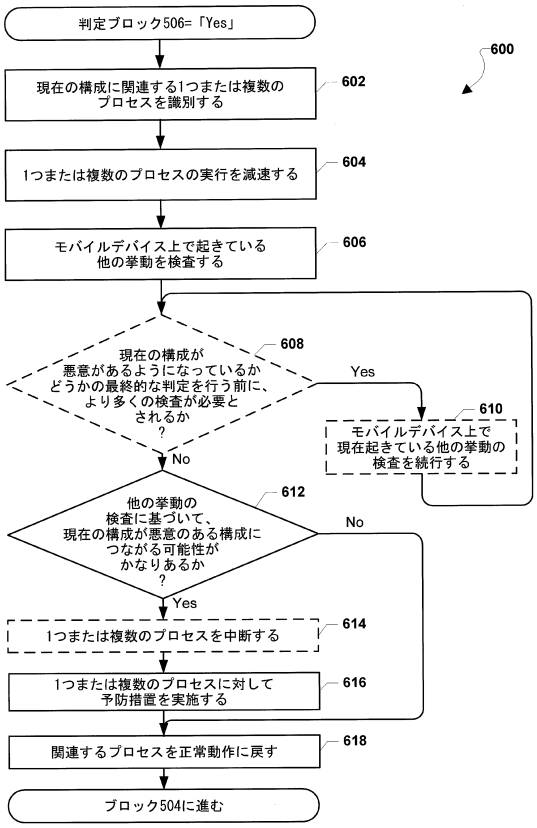
【図４】


400
複数のモバイルデバイスから構成情報
および構成履歴を受信する
402
構成情報を分析して
悪意のある構成を識別する
404
識別された悪意のある構成
および構成履歴に基づいて経路構成を識別する
406
識別された悪意のある構成
および識別された経路構成を含む
悪意のある構成および経路構成の
データベースを生成する
408
経路構成ごとに、
悪意のある構成に遷移する確率を計算する
410
悪意のある構成
および経路構成のデータベースに
計算された確率を含める
412
識別された経路構成内にいる間に
実行されたとき悪意のある構成に導く
悪意のある経路命令を識別する
414
悪意のある構成
および経路構成のデータベースに、
実行されたとき識別された悪意のある構成に
つながる識別された命令のリストを含める
416
複数のモバイルデバイスに悪意のある構成
および経路構成のデータベースを送る
418

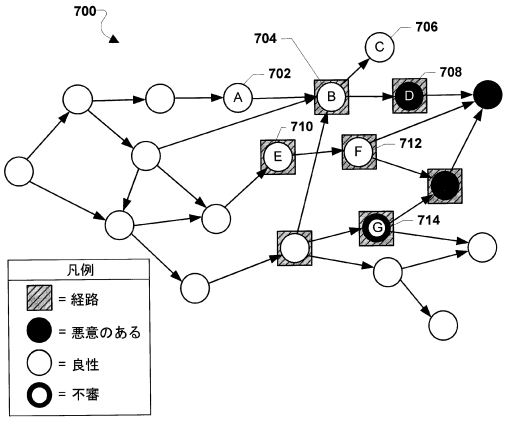
【図５】


500
悪意のある構成
および経路構成のデータベースを受信する
502
現在の構成を決定する
504
悪意のある構成および
経路構成のデータベースに基づいて、
現在の構成が悪意のある構成に
つながるか
?
506
No
Yes
予防措置を実施して
悪意のある構成を回避するか
?
507
No
Yes
予防措置を実施して
悪意のある構成を回避する
508
正常に実行を続行する
510

【図６】


判定ブロック506=「Yes」
600
現在の構成に関連する1つまたは複数の
プロセスを識別する
602
1つまたは複数のプロセスの実行を減速する
604
モバイルデバイス上で起きている
他の挙動を検査する
606
現在の構成が
悪意があるようになっているか
どうかの最終的な判定を行う前に、
より多くの検査が必要と
されるか
?
608
Yes
モバイルデバイス上で
現在起きている他の挙動の
検査を続行する
610
No
他の挙動の
検査に基づいて、
現在の構成が悪意のある構成に
つながる可能性が
かなりあるか
?
612
No
Yes
1つまたは複数のプロセスを中断する
614
1つまたは複数のプロセスに対して
予防措置を実施する
616
関連するプロセスを正常動作に戻す
618
ブロック504に進む

【図７Ａ】

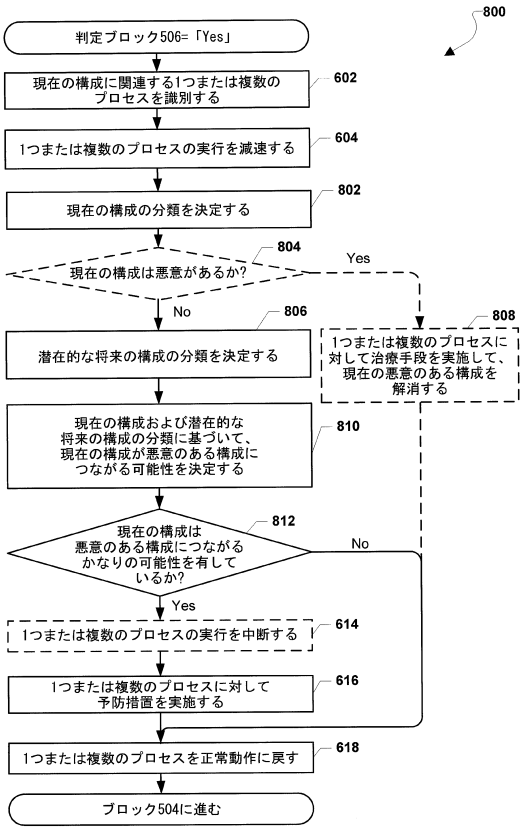


【図７Ｂ】

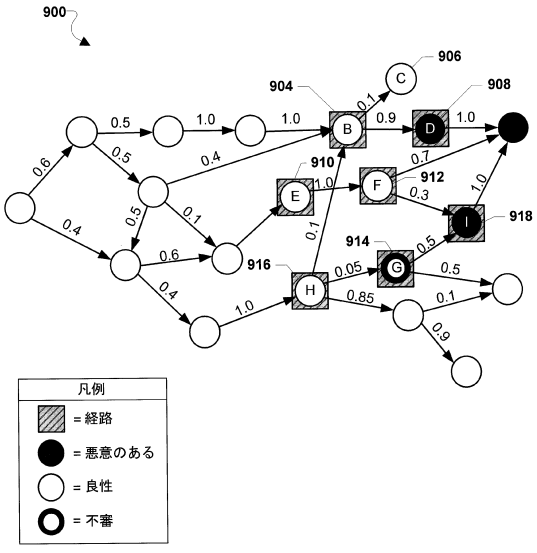
725

現在の構成の分類	潜在的な将来の構成の分類	近い将来の悪意のある構成のかなりの可能性
良性	悪意のある構成がない	なし
不審	任意の構成	あり
良性	1つ以上の悪意のある構成および1つ以上の悪意のない構成	あり
悪意のある	任意の構成	あり
良性	すべて悪意のある構成	あり
不審	すべて悪意のある構成	あり

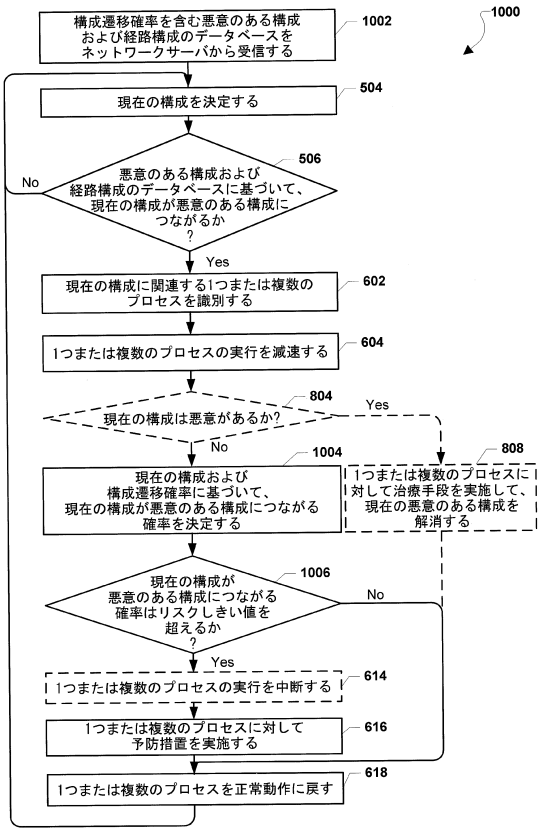
【図８】



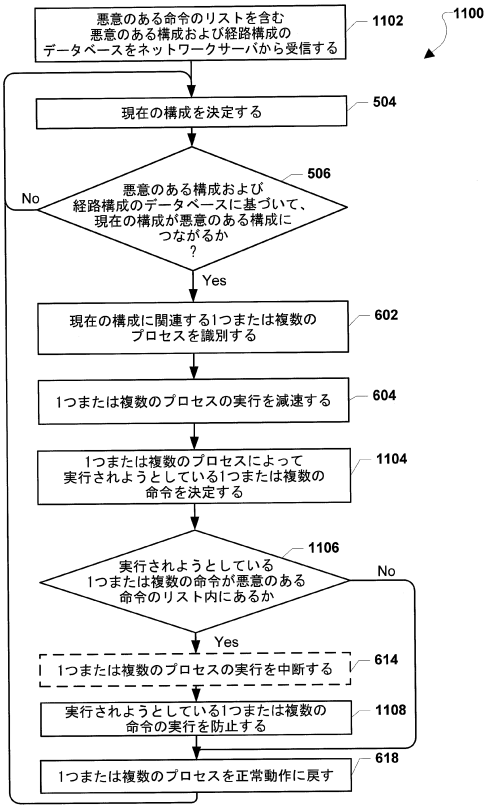
【図９】



【図１０】



【図１１】



【図１２】

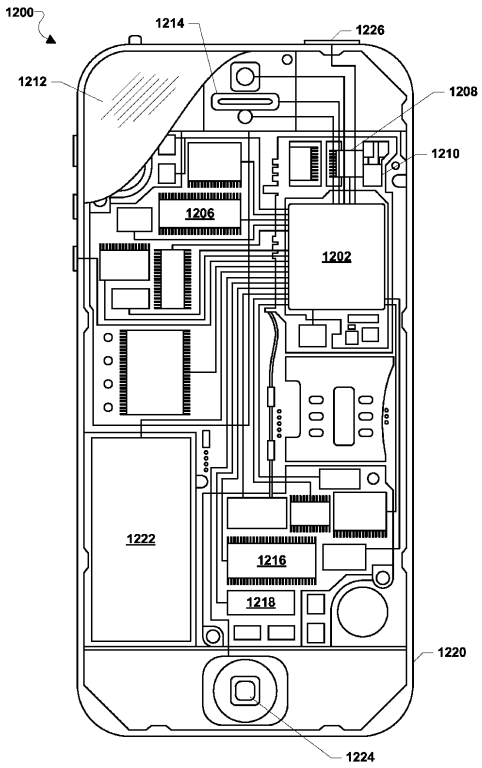


FIG. 12

【図１３】

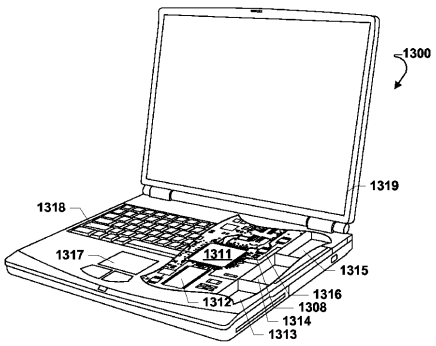


FIG. 13

【図１４】

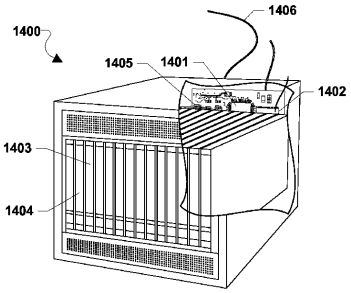


FIG. 14

フロントページの続き

(72)発明者　サティヤジト・プラバカール・パトネ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　ラジャルシ・グプタ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　岸野　徹

(56)参考文献　特開２００７－０１８０４４（ＪＰ，Ａ）
特開２００５－１３６５２６（ＪＰ，Ａ）
特開２００２－２５１３７４（ＪＰ，Ａ）
特開２００５－３４１２１７（ＪＰ，Ａ）
米国特許出願公開第２０１３／００９７６６０（ＵＳ，Ａ１）
特開２００１－０３４５９６（ＪＰ，Ａ）
米国特許出願公開第２０１２／０１３７３６９（ＵＳ，Ａ１）
米国特許出願公開第２０１１／０２１４１６１（ＵＳ，Ａ１）
米国特許出願公開第２００５／００１５６６７（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５６