(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6598221号
(P6598221)
(45)発行日　令和1年10月30日(2019.10.30)　(24)登録日　令和1年10月11日(2019.10.11)

(51)Int.Cl.　F I
G06F 21/56 (2013.01)　G06F 21/56 360

請求項の数 19 (全 21 頁)

(21)出願番号　特願2017-566782(P2017-566782)
(86)(22)出願日　平成28年5月25日(2016.5.25)
(65)公表番号　特表2018-524716(P2018-524716A)
(43)公表日　平成30年8月30日(2018.8.30)
(86)国際出願番号　PCT/US2016/033978
(87)国際公開番号　WO2017/003588
(87)国際公開日　平成29年1月5日(2017.1.5)
審査請求日　平成30年1月31日(2018.1.31)
(31)優先権主張番号　14/752,893
(32)優先日　平成27年6月27日(2015.6.27)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　517378810
マカフィー，エルエルシー
アメリカ合衆国、９５０５４　カリフォルニア州、サンタ　クララ　ミッション　カレッジ　ブーレバード　２８２１
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　ビーン、ジェイムス
アメリカ合衆国、９５０５４　カリフォルニア州、サンタ　クララ、ミッション　カレッジ　ブールバード　２８２１　マカフィー，　インコーポレイテッド内

最終頁に続く

(54)【発明の名称】マルウェアを特定するための変則検知

(57)【特許請求の範囲】
【請求項１】
プロセッサに、
前記プロセッサによって、システムのメタデータを生成する手順と、
メモリ内に、前記システムの前記メタデータを格納する手順と、
前記システム内の一般性の高いオブジェクトのアクティビティを監視する手順であって、前記一般性の高いオブジェクトは、前記システム内のプロセス、周辺機器、または電子デバイス上のハードウェアである、監視する手順と、
前記監視されたアクティビティを、前記メモリ内に格納された前記システムの前記メタデータと比較する手順と、
潜在的に悪意のあるアクティビティを検知すべく、一般性の低い例外を特定する手順であって、前記一般性の低い例外は、前記一般性の高いオブジェクトのメタデータを模倣し、および、前記一般性の高いオブジェクトの前記メタデータの一部において、変則として現れる、特定する手順と、
前記一般性の高いオブジェクトの前記一般性の低い例外の特定に応答し、前記一般性の高いオブジェクトの前記一般性の低い例外に対し、マルウェアのスキャンをする手順と、
を実行させるための、プログラム。
【請求項２】
前記潜在的に悪意のあるアクティビティを検知すべく、前記一般性の低い例外の期間が少なくとも部分的に用いられる、請求項１に記載のプログラム。

【請求項３】
前記一般性の低い例外によって模倣される前記一般性の高いオブジェクトの前記メタデータは、ファイル名、プロセス名、ファイルプロパティ、フィンガープリント、およびレジストリキーのうちの１または複数を含む、請求項１または２に記載のプログラム。
【請求項４】
前記システムの前記メタデータは、前記システム上で監視された前のアクティビティから生成される、請求項１から３のいずれか一項に記載のプログラム。
【請求項５】
前記システムの前記メタデータは、同様のシステムの他のメタデータに少なくとも部分的に基づく、請求項１から４のいずれか一項に記載のプログラム。
【請求項６】
前記監視されたアクティビティを前記システムの前記メタデータと比較する手順は、ポリモーフィック型の脅威を特定するための、オブジェクトのメタデータの分析、前記オブジェクトが別のオブジェクトのメタデータを再使用しているかどうかを検知するための、前記システムのオブジェクトの再使用の分析、および前記システムのファイル名の分析のうちの少なくとも１つを含む、請求項１から５のいずれか一項に記載のプログラム。
【請求項７】
メモリ要素と、
ハードウェアプロセッサと、を備え、
前記ハードウェアプロセッサは、
システムのメタデータを生成し、
前記メモリ要素内に、前記システムの前記メタデータを格納し、
前記システム内の一般性の高いオブジェクトのアクティビティを監視し、前記一般性の高いオブジェクトは、前記システム内のプロセス、周辺機器、または電子デバイス上のハードウェアであり、
前記監視されたアクティビティを、前記メモリ要素内に格納された前記システムの前記メタデータと比較し、
潜在的に悪意のあるアクティビティを検知すべく、一般性の低い例外を特定し、前記一般性の低い例外は、前記一般性の高いオブジェクトのメタデータを模倣し、および、前記一般性の高いオブジェクトの前記メタデータの一部において、変則として現れ、
前記一般性の高いオブジェクトの前記一般性の低い例外の特定に応答し、前記一般性の高いオブジェクトの前記一般性の低い例外に対し、マルウェアのスキャンをする、ように構成されている、装置。
【請求項８】
前記潜在的に悪意のあるアクティビティを検知すべく、前記一般性の低い例外の期間が少なくとも部分的に用いられる、請求項７に記載の装置。
【請求項９】
前記一般性の低い例外によって模倣される前記一般性の高いオブジェクトの前記メタデータは、ファイル名、プロセス名、ファイルプロパティ、フィンガープリント、およびレジストリキーのうちの１または複数を含む、請求項７または８に記載の装置。
【請求項１０】
前記システムの前記メタデータは、前記システム上で監視された前のアクティビティから生成される、請求項７から９のいずれか一項に記載の装置。
【請求項１１】
前記システムの前記メタデータは、同様のシステムの他のメタデータに少なくとも部分的に基づく、請求項７から１０のいずれか一項に記載の装置。
【請求項１２】
前記監視されたアクティビティを前記システムの前記メタデータと比較することは、ポリモーフィック型の脅威を特定するための、オブジェクトのメタデータの分析、前記オブジェクトが別のオブジェクトのメタデータを再使用しているかどうかを検知するための、

前記システムのオブジェクトの再使用の分析、および前記システムのファイル名の分析のうちの少なくとも１つを含む、請求項７から１１のいずれか一項に記載の装置。
【請求項１３】
システムのメタデータを生成する段階と、
前記システムの前記メタデータを格納する段階と、
前記システム内の一般性の高いオブジェクトのアクティビティを監視する段階であって、前記一般性の高いオブジェクトは、前記システム内のプロセス、周辺機器、または電子デバイス上のハードウェアである、監視する段階と、
前記監視されたアクティビティを、前記システムの前記メタデータと比較する段階と、
潜在的に悪意のあるアクティビティを検知すべく、一般性の低い例外を特定する段階であって、前記一般性の低い例外は、前記一般性の高いオブジェクトのメタデータを模倣し、および、前記一般性の高いオブジェクトの前記メタデータの一部において、変則として現れる、特定する段階と、
前記一般性の高いオブジェクトの前記一般性の低い例外の特定に応答し、前記一般性の高いオブジェクトの前記一般性の低い例外に対し、マルウェアのスキャンをする段階と、
を備える、方法。
【請求項１４】
前記潜在的に悪意のあるアクティビティを検知すべく、前記一般性の低い例外の期間が、少なくとも部分的に用いられる、請求項１３に記載の方法。
【請求項１５】
前記一般性の低い例外によって模倣される前記一般性の高いオブジェクトの前記メタデータは、ファイル名、プロセス名、ファイルプロパティ、フィンガープリント、およびレジスタキーのうちの１または複数を含む、請求項１３または１４に記載の方法。
【請求項１６】
前記システムの前記メタデータは、前記システム上で監視された前のアクティビティから生成される、請求項１３から１５のいずれか一項に記載の方法。
【請求項１７】
前記監視されたアクティビティを前記システムにの前記メタデータと比較する段階は、ポリモーフィック型の脅威を特定するための、オブジェクトのメタデータの分析、前記オブジェクトが別のオブジェクトのメタデータを再使用しているかどうかを検知するための、前記システムのオブジェクトの再使用の分析、および前記システムのファイル名の分析のうちの少なくとも１つを含む、請求項１３から１６のいずれか一項に記載の方法。
【請求項１８】
メモリと、
ハードウェアプロセッサと、を備え、
前記ハードウェアプロセッサは、
システムのメタデータを生成し、
前記メモリ内に前記システムの前記メタデータを格納し、
前記システム内の一般性の高いオブジェクトのアクティビティを監視し、前記一般性の高いオブジェクトは、前記システム内のプロセス、周辺機器、または電子デバイス上のハードウェアであり、
前記監視されたアクティビティを、前記メモリ内に格納された前記システムの前記メタデータと比較し、
潜在的に悪意のあるアクティビティを検知すべく、一般性の低い例外を特定し、前記一般性の低い例外は、前記一般性の高いオブジェクトのメタデータを模倣し、および、前記一般性の高いオブジェクトの前記メタデータの一部において、変則として現れ、
前記一般性の高いオブジェクトの前記一般性の低い例外の特定に応答し、前記一般性の高いオブジェクトの前記一般性の低い例外に対し、マルウェアのスキャンをする、ように構成されている、マルウェアを特定するための変則検知のシステム。
【請求項１９】

前記監視されたアクティビティを前記システムの前記メタデータと比較することは、ポリモーフィック型の脅威を特定するための、オブジェクトのメタデータの分析、前記オブジェクトが別のオブジェクトのメタデータを再使用しているかどうかを検知するための、前記システムのオブジェクトの再使用の分析、および前記システムのファイル名の分析のうちの少なくとも１つを含む、請求項１８に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

［関連出願への相互参照］

本出願は、２０１５年６月２７日に出願された、「マルウェアを特定するための変則検知」と題された米国非仮（実用）特許出願第１４／７５２，８９３号の利益および優先権を主張し、それはその全体において参照によって本明細書に組み込まれる。

【０００２】

本開示は、概して、情報セキュリティの分野に関し、より具体的には、マルウェアを特定するための変則検知に関する。

【背景技術】

【０００３】

今日の社会において、ネットワークセキュリティの分野はますます重要になってきている。インターネットは、世界中の異なるコンピュータネットワークの相互接続を可能にしている。特に、インターネットは、様々なタイプのクライアントデバイスを介して、異なるコンピュータネットワークに接続された異なるユーザの間でデータを交換するための媒体を提供する。インターネットの使用が企業のコミュニケーションおよび個人のコミュニケーションを変えた一方、それは、また、悪意のある操作者がコンピュータおよびコンピュータネットワークへの不正アクセスを得るための、および、機密情報の意図的なまたは不注意による開示のための、手段として使用されている。

【０００４】

ホストコンピュータに感染する、悪意のあるソフトウェア（「マルウェア」）は、ホストコンピュータと関連づけられた企業または個人から機密情報を盗取する、他のホストコンピュータに伝播する、および／または、分散型サービス妨害攻撃を支援する、ホストコンピュータからのスパムまたは悪意のあるｅメールを送信する、などの、任意の数の悪意のある動作を実行することが可能であり得る。従って、コンピュータおよびコンピュータネットワークを、悪意のあるソフトウェアおよびデバイスによる、悪意のある、および不注意なエクスプロイトから保護するための、著しい管理課題が残っている。

【図面の簡単な説明】

【０００５】

本開示、ならびにその特徴および利点のより完全な理解を提供するように、添付の図面と共に用いられる以下の説明が参照される。同様の参照符号は同様の部分を表す。

【０００６】

【図１Ａ】本開示の一実施形態による、マルウェアを特定するための変則検知のための通信システムの簡略ブロック図である。

【０００７】

【図１Ｂ】本開示の一実施形態による、マルウェアを特定するための変則検知のための通信システムの一部分の簡略ブロック図である。

【０００８】

【図２】一実施形態による通信システムに関連づけられ得る、潜在的な操作を示す簡略フローチャートである。

【０００９】

【図３】一実施形態による通信システムに関連づけられ得る、潜在的な操作を示す簡略フローチャートである。

【００１０】

【図４】一実施形態によるポイントツーポイント構成に配置された、例示的なコンピューティングシステムを示すブロック図である。
【００１１】
【図５】本開示の例示的なＡＲＭエコシステム・システムオンチップ（ＳｏＣ）に関連づけられる、簡略ブロック図である。
【００１２】
【図６】一実施形態による例示的なプロセッサコアを示すブロック図である。
【００１３】
図面は、それらの寸法が本開示の範囲から大幅に逸脱することなく変わり得るので、必ずしも縮尺通りに描かれてはいない。
【発明を実施するための形態】
【００１４】
［例示的な実施形態］
図１Ａは、本開示の一実施形態による、マルウェアを特定するための変則検知のための通信システム１００ａの簡略ブロック図である。図１Ａに示されるように、通信システム１００ａは、電子デバイス１０２ａ－１０２ｄ、クラウドサービス１０４、およびサーバ１０６を含み得る。１または複数の電子デバイス１０２ａ－１０２ｄは各々、メモリ１１０、プロセッサ１１２、例外検知モジュール１１４、１または複数のプロセス１１６ａ－１１６ｃ、および複数のハードウェア１１８ａおよび１１８ｂを含み得る。例外検知モジュール１１４は、メタデータデータベース１２０を含み得る。１または複数の周辺機器１２２ａおよび１２２ｂは、１または複数の電子デバイス１０２ａ－１０２ｄと接続し得る。クラウドサービス１０４およびサーバ１０６は各々、ネットワーク例外検知モジュール１２４を含み得る。ネットワーク例外検知モジュール１２４は、メタデータデータベース１２０を含み得る。電子デバイス１０２ａ－１０２ｄと、クラウドサービス１０４と、サーバ１０６とは、ネットワーク１０８を用いて互いに通信し得る。
【００１５】
図１Ｂは、本開示の一実施形態による、マルウェアを特定するための変則検知のための通信システム１００ｂの簡略ブロック図である。図１Ｂに示されるように、通信システム１００ｂは、電子デバイス１０２ｅ－１０２ｇ、クラウドサービス１０４、およびサーバ１０６を含み得る。電子デバイス１０２ｅ－１０２ｇは、ローカルネットワーク１２８を用いて互いに通信し得る。ローカルネットワーク１２８は、電子デバイス１０２ｈを含み得る。電子デバイス１０２ｈは、ローカルネットワーク例外検知モジュール１３０を含み得る。ローカルネットワーク例外検知モジュール１３０は、メタデータデータベース１２０を含み得る。ローカルネットワーク１２８は、ネットワーク１０８を用いて、クラウドサービス１０４およびサーバ１０６と通信し得る。
【００１６】
例示的な実施形態において、通信システム１００ａおよび１００ｂは、本開示の一実施形態によるマルウェアを特定するための変則検知のために構成され得る。例外検知モジュール１１４、ネットワーク例外検知モジュール１２４、およびローカルネットワーク例外検知モジュール１３０は、デバイスの挙動を理解し、ネットワーク上の各デバイスについて、デバイスの評価値を評価するように構成され得る。通信システム１００ａおよび１００ｂは、また、アプリケーションまたはアクティビティに関連づけられたネットワークトラフィックにおけるコンテンツに基づいて、不審なアプリケーションまたはアクティビティを特定するように構成される。例えば、通信システム１００ａおよび１００ｂは、システムのアクティビティを監視し、監視されたアクティビティをシステムのメタデータと比較し、潜在的に悪意のあるオブジェクトを検知すべく、一般性の低い例外（ｌｏｗ　ｐｒｅｖａｌｅｎｃｅ　ｏｕｔｌｉｅｒｓ）を特定するように構成され得る。例えば、例外検知モジュール１１４は、プロセス１１６ａ－１１６ｃ、ハードウェア１１８ａおよび１１８ｂ、および周辺機器１２２ａおよび１２２ｂの挙動を理解し、プロセス１１６ａ－１１６ｃ、ハードウェア１１８ａおよび１１８ｂ、ならびに周辺機器１２２ａおよび１２２ｂ

の一般性の低い例外または変則的な挙動の認識によって、不審なアクティビティを特定するように構成され得る。また、ネットワーク例外検知モジュール１２４は、電子デバイス１０２ａ－１０２ｄの挙動を理解し、電子デバイス１０２ａ－１０２ｄの一般性の低い例外または変則的な挙動の認識によって、不審なアクティビティを特定するように構成され得る。さらに、ローカルネットワーク例外検知モジュール１３０は電子デバイス１０２ｅ－１０２ｇの挙動を理解し、電子デバイス１０２ｅ－１０２ｇの一般性の低い例外または変則的な挙動の認識によって、不審なアクティビティを特定するように構成され得る。メタデータデータベース１２０は、システム上のオブジェクトの挙動の理解を容易にするための、システム内の各オブジェクトに関するメタデータを含み得る。一例において、メタデータデータベース１２０は、通信システム１００ａおよび１００ｂにおいて発見された各例外の普及度および期間、または、通信システム１００ａおよび１００ｂに存在し得る共通に知られた例外の共通の普及度および期間（可能ならば）を含み得る。

【００１７】

例外検知モジュール１１４およびネットワーク例外検知モジュール１２４は、メタデータデータベース１２０を用いて、一般性の低い例外を判断し、および、一般性の低い例外がデバイス、プロセス、またはオブジェクトからの悪意のあるアクティビティをいつ示し得るかを判断し得る。例えば、例外検知モジュール１１４およびネットワーク例外検知モジュール１２４は、通信システム１００ａおよび１００ｂにおけるオブジェクト（例えば、電子デバイス１０２ａ－１０２ｇ、プロセス１１６ａ－１１６ｃ、ハードウェア１１８ａおよび１１８ｂ、周辺機器１２２ａおよび１２２ｂなど）のアクティビティを監視し、監視されたアクティビティをシステムのメタデータと比較し、潜在的に悪意のあるアクティビティを検知すべく、一般性の低い例外を特定するように構成され得る。一例において、監視されるアクティビティは、ポリモーフィック型の脅威を特定するための、システムにおけるオブジェクト（例えば、電子デバイス、プロセス、ハードウェア、周辺機器など）のメタデータの分析を含み得る。より具体的には、ファイル名の再使用、オブジェクトのフィンガープリントは同様だがハッシュが異なりその他の点では同一であるオブジェクトといった、ポリモーフィズム（ｐｏｌｙｍｏｒｐｈｉｓｍ：同種異像）の指標を特定することによって、ポリモーフィック型の脅威の特定を容易にすべく、複数のシステムからのオブジェクトメタデータが比較され得る。ポリモーフィック型のオブジェクトは、別のオブジェクトと似ているが、ファイルジオメトリ、ファイルの暗号ハッシュなどの領域でのみ僅かに異なり、この相違が、オブジェクトが各システム上にどのように示されるかの指標となり得る。監視されるアクティビティは、別のオブジェクトのメタデータを再使用するオブジェクトを検知するための、システムのオブジェクトの再使用の分析をまた含み得る。例えば、一般的なオブジェクトによって用いられるファイル名などのメタデータを再使用するがその他の点では一般性の低いオブジェクトであるといった、一般性の低いオブジェクトは、かなり異なる（例えば、ｓｖｃｈｏｓｔ．ｅｘｅが、悪意のアプリケーションによって再使用される共通のファイル名である）。一般性の低い例外の期間が、潜在的に悪意のあるアクティビティを検知するために、少なくとも部分的に用いられ得る。一例において、各例外の普及度および期間は、例外検知モジュール１１４および／またはネットワーク例外検知モジュール１２４によって判断され得、比較的普及した、新しい例外は、悪意のあるアクティビティの指標となり得る。

【００１８】

図１の複数の要素は、任意の好適な（有線または無線）接続を採用する１または複数のインタフェースを通じて互いに結合され得、それはネットワーク（例えば、ネットワーク１０８、ローカルネットワーク１２８など）通信のための実行可能な経路を提供する。加えて、図１のそれらの要素の任意の１または複数は、特定の構成の必要性に基づいて、組み合わされ得、または、アーキテクチャから取り除かれ得る。通信システム１００ａおよび１００ｂは、ネットワークにおけるパケットの送信または受信のための、伝送制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）通信が可能な構成を含み得る。通信システム１００ａおよび１００ｂは、必要に応じて、および特定の必要性に基づいて、ユ

ーザデータグラムプロトコル／ＩＰ（ＵＤＰ／ＩＰ）または任意の他の好適なプロトコルと共に、また動作し得る。

【００１９】

通信システム１００ａおよび１００ｂの特定の例の技術を示す目的で、ネットワーク環境をトラバースし得る通信を理解することが重要である。以下の基礎的情報は、本開示が適切に説明され得る根拠とみなされ得る。

【００２０】

現在、マルウェアはしばしば、マルウェアが動作する環境に、存在することが予期されるオブジェクトを模倣することによって、マルウェア自体を隠すことを試みる。マルウェアが模倣し得るオブジェクトは、様々なメタデータ、ファイル名、プロセス名、ファイルプロパティ、レジストリキーなどであり得る。この技術は、しばしば、ユーザおよび管理者からマルウェアを隠すためにうまく動作する。マルウェアが用いる模倣のプロセスを利用して、マルウェアを検知および特定できる方法が必要である。

【００２１】

図１Ａおよび図１Ｂに概説されるような、マルウェアを特定するための変則検知のための通信システムが、これらの（および他の）課題を解決し得る。通信システム１００ａおよび１００ｂは、集中化されたデータストア（例えば、メタデータデータベース１２０）を用いて、共通のアプリケーションおよびプロセスのメタデータを特定して、例外を特定するように構成され得る。検知アルゴリズムは、集中化されたデータストア（例えば、メタデータデータベース１２０）と共に動作して、環境内の一般性の高い、一様なオブジェクトを発見し、および、一般性の低い例外を探して、潜在的に悪意のあるオブジェクトを特定し得る。このプロセスは、人間の調査員が、システム上で異常な挙動を検査する場合に行うことと同様であり、通信システム１００ａおよび１００ｂが、調査員および管理者が実現不可能な規模で、このタイプのロジックを自動化することを可能にし得る。

【００２２】

例外検知モジュール１１４およびローカルネットワーク例外検知モジュール１３０は、メタデータの例外を特定すべく、集中化されたデータストア（例えば、メタデータデータベース１２０）を用いると、通信システム１００ａおよび１００ｂにおける一般性の高い、一様なオブジェクトを特定し、且つ、一般性の低い例外を探して、潜在的に悪意のオブジェクトを特定することができる。通信システム１００ａおよび１００ｂ、または通信システム１００ａおよび１００ｂの一部分の分析は、スケジュールされたプロセスであってよく、一般性が高く、且つ、過去に例外があったとしてもわずかであるようなオブジェクトに対する例外を探す。（例えば、ＭＳＩＥｘｅｃは常に署名される。署名されていないＭＳＩＥｘｅｃの１つの独特のインスタンスが、最新の分析で出現した場合、それは、悪意のあるアクティビティを示し得る）。これを拡張していくと、文脈の中で、新しい例外の上位集合を検査することになる。例えば、最新の分析の最中に、単一のシステムがＶＳＥまたはＨＩＰＳの脅威イベントを有し、例外検知モジュール１１４が、１７個の非常に珍しい例外を特定したならば、そのシステムは、悪意のあるアクティビティに遭遇している可能性が非常に高い。分析はまた、電子デバイスからのクエリへの応答などの、オンデマンドであり得る。クエリは、デバイスまたはネットワーク上の潜在的に悪意のある挙動に応答して行われるものであってよく、クエリは、通信システム１００ａおよび１００ｂ内の潜在的に悪意のある挙動、または一般的な挙動の位置を確認するために用いられ得る。例えば、ネットワーク例外検知モジュール１２４が、ローカルネットワークから、異常な量の例外アクティビティを検知している場合、ローカルネットワーク例外検知モジュール１３０は、その異常な量の例外アクティビティの出所が電子デバイス１０２ｅであるとトレースすることが可能であり得る。電子デバイス１０２ｅは、例外検知モジュール１１４を含み得、その異常な量の例外アクティビティのソースが、プロセス、周辺機器またはハードウェアであるとトレースし得る。

【００２３】

例外検知モジュール１１４およびローカルネットワーク例外検知モジュール１３０によ

る分析は、環境内の１つのバイナリを除き、他のあらゆるバイナリインスタンスには有効な署名があるというような、ポリモーフィック型であり得る。分析はまた、オートランレジストリキーが環境内の他のものと合致しない、独特の値であるというような、オブジェクトの再使用を探してもよい。例えば、オートランレジストリキーのターゲットファイル群は、Ａｄｏｂｅによって署名されているが、問題になっているターゲットバイナリは、唯一署名されていない。分析はまた、ファイル名を含み得る。例えば、一般に用いられるファイル（例えば、ｍｓｉｅｘｅｃ．ｅｘｅ）が、独特の位置にあり、独特のバイナリプロパティ（例えば、パック／アンパック、３２／６４ビットなど）を有する。一例において、ロジックの組み合わせは、例外検知モジュール１１４およびローカルネットワーク例外検知モジュール１３０によって成され得る。いくつかのプロパティ（例えば、ファイルバージョン情報）は、ダイナミックでありユビキタスではないように意図されている。他の点では同一のバイナリが、ネイティブＷｉｎ３２から．ＮＥＴファイル構造に変更されることはありそうにない。一例において、ロジックエンジンは、メタデータの変化に異なる重みづけをするように構成され得る。

【００２４】

一実施形態において、ネットワーク例外検知モジュール１２４およびローカルネットワーク例外検知モジュール１３０は、ネットワークトラフィックを受動的にリッスンして、各電子デバイスとの間を行き来するネットワークトラフィックを監視するように構成され得る。一例において、ネットワークにおける１または複数の電子デバイス（例えば、電子デバイス１０２ａ－１０２ｄ）は、ネットワークトラフィックを監視して、各々の電子デバイスとの間を行き来するネットワークトラフィックに基づいてアラートを提供するための例外検知モジュール１１４を各々含み得る。別の例において、中央ネットワークゲートウェイデバイス（例えば、電子デバイス１０２ｈ）は、ローカルネットワーク例外検知モジュール１３０を用いて、トラフィックを監視し、情報アラートの提供に加えて、不審な挙動に自動的に対処することができる。

【００２５】

図１Ａおよび図１Ｂのインフラストラクチャに移ると、例示的な実施形態による通信システム１００ａおよび１００ｂが示される。概して、通信システム１００ａおよび１００ｂは、任意の種類またはトポロジのネットワークにおいて実装され得る。ネットワーク１０８は、通信システム１００ａおよび１００ｂを通じて伝播する情報のパケットを受信および送信する、相互接続された通信経路の一連のポイントまたはノードを示す。ネットワーク１０８は、ノード間の通信インタフェースを提供し、任意のローカルエリアネットワーク（ＬＡＮ）、仮想ローカルエリアネットワーク（ＶＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）、無線ローカルエリアネットワーク（ＷＬＡＮ）、メトロポリタンエリアネットワーク（ＭＡＮ）、イントラネット、エクストラネット、仮想プライベートネットワーク（ＶＰＮ）、および、ネットワーク環境において通信を容易にする任意の他の適切なアーキテクチャまたはシステム、または、それらの任意の好適な組み合わせとして、有線および／または無線通信を含んで構成され得る。ローカルネットワーク１２８は、電子デバイス１０２ｅ－１０２ｇを通じて伝播する情報のパケットを受信および送信する、相互接続された通信経路の一連のポイントまたはノードを示す。ローカルネットワーク１２８は、ノード間の通信インタフェースを提供し、任意のローカルエリアネットワーク（ＬＡＮ）、仮想ローカルエリアネットワーク（ＶＬＡＮ）、および、ネットワーク環境において通信を容易にする任意の他の適切なアーキテクチャまたはシステム、または、それらの任意の好適な組み合わせとして、有線および／または無線通信を含んで構成され得る。

【００２６】

通信システム１００ａおよび１００ｂにおいて、パケット、フレーム、信号、データなどを含むネットワークトラフィックは、任意の好適な通信メッセージングプロトコルによって送信され得、および受信され得る。好適な通信メッセージングプロトコルは、開放型システム間相互接続（ＯＳＩ）モデル、または、それらの任意の派生または変形（例えば、伝送制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）、ユーザデータグラ

ムプロトコル／ＩＰ（ＵＤＰ／ＩＰ））、などの多層スキームを含み得る。加えて、セルラネットワークにわたる無線信号通信もまた、通信システム１００ａおよび１００ｂにおいて、提供されてよい。好適なインタフェースおよびインフラストラクチャが、セルラネットワークとの通信を可能にするように提供されてよい。

【００２７】

本明細書で用いられる用語「パケット」は、パケット交換ネットワーク上のソースノードと宛先ノードとの間でルーティングされ得るデータの単位を指す。パケットは、ソースネットワークアドレスおよび宛先ネットワークアドレスを含む。これらのネットワークアドレスは、ＴＣＰ／ＩＰメッセージングプロトコルにおけるインターネットプロトコル（ＩＰ）アドレスであり得る。本明細書で用いられる用語「データ」は、電子デバイスおよび／またはネットワークにおいて、１つのポイントから別のポイントへ通信され得る任意の適切なフォーマットの、任意の種類のバイナリ、数値、音声、ビデオ、テキスト、もしくはスクリプトデータ、もしくは、任意の種類のソースもしくはオブジェクトコード、または、任意の他の好適な情報を指す。加えて、メッセージ、要求、応答、およびクエリはネットワークトラフィックの形態であり、従って、パケット、フレーム、信号、データなどを備え得る。

【００２８】

例示的な実装において、電子デバイス１０２ａ－１０２ｈ、クラウドサービス１０４、およびサーバ１０６はネットワーク要素であり、それらは、ネットワーク環境において情報を交換するように操作可能な、ネットワーク機器、サーバ、ルータ、スイッチ、ゲートウェイ、ブリッジ、ロードバランサ、プロセッサ、モジュール、または、任意の他の好適なデバイス、コンポーネント、要素、もしくはオブジェクトを包含することが意図される。ネットワーク要素は、それらの操作を容易にする、任意の好適なハードウェア、ソフトウェア、コンポーネント、モジュール、または、オブジェクト、ならびに、ネットワーク環境においてデータまたは情報を受信、送信、および／または別の方法で通信するために好適なインタフェースを含み得る。これは、データまたは情報の効果的な交換を可能にする適切なアルゴリズムおよび通信プロトコルを含み得る。

【００２９】

通信システム１００ａおよび１００ｂに関連づけられた内部構造に関して、電子デバイス１０２ａ－１０２ｈ、クラウドサービス１０４、およびサーバ１０６の各々は、本明細書に概説される操作において用いられる情報を格納するための複数のメモリ要素を含み得る。電子デバイス１０２ａ－１０２ｈ、クラウドサービス１０４、およびサーバ１０６の各々は、任意の好適なメモリ要素（例えば、ランダムアクセスメモリ（ＲＡＭ）、リードオンリメモリ（ＲＯＭ）、消去可能プログラマブルＲＯＭ（ＥＰＲＯＭ）、電気的消去可能プログラマブルＲＯＭ（ＥＥＰＲＯＭ）、特定用途向け集積回路（ＡＳＩＣ）など）、ソフトウェア、ハードウェア、ファームウェア、または、必要に応じて、および特定の必要性に基づいて、任意の他の好適なコンポーネント、デバイス、要素、もしくはオブジェクトに、情報を保持し得る。本明細書で説明された任意のメモリアイテムは、広義の用語「メモリ要素」の中に包含されると解釈されるべきである。さらに、通信システム１００ａおよび１００ｂにおいて用いられ、トラッキングされ、送信され、または受信される情報は、任意のデータベース、レジスタ、キュー、テーブル、キャッシュ、制御リスト、または他のストレージ構造において提供され得、それらの全ては、任意の好適な時間枠で参照され得る。任意のそのようなストレージの選択肢が、本明細書で用いられる広義の用語「メモリ要素」の中に、また含まれ得る。

【００３０】

特定の例示的な実装において、本明細書に概説される機能は、非一時的コンピュータ読み取り可能媒体を含み得る１または複数の有形媒体において符号化されるロジック（例えば、ＡＳＩＣに提供される組み込みロジック、デジタル信号プロセッサ（ＤＳＰ）命令、プロセッサまたは他の同様の機械によって実行されるソフトウェア（オブジェクトコードおよびソースコードを潜在的に含む）、など）によって実装され得る。これらの例のいく

つかにおいて、メモリ要素は、本明細書に説明された操作のために用いられるデータを格納し得る。これは、本明細書に説明されたアクティビティを遂行するように実行される、ソフトウェア、ロジック、コード、またはプロセッサ命令を格納可能なメモリ要素を含む。

【００３１】

例示的な実装において、電子デバイス１０２ａ－１０２ｈ、クラウドサービス１０４、およびサーバ１０６などの通信システム１００ａおよび１００ｂのネットワーク要素は、本明細書に概説される操作を実現または促進する、ソフトウェアモジュール（例えば、例外検知モジュール１１４およびネットワーク例外検知モジュール１２４）を含み得る。これらのモジュールは、特定の構成および／またはプロビジョニングの必要性に基づき得る、任意の適切な態様で好適に組み合わされ得る。例示的な実施形態において、そのような操作は、ハードウェアによって遂行され得、それらの要素の外部に実装され得、または、意図される機能を実現する何らかの他のネットワークデバイスに含まれ得る。さらに、モジュールは、ソフトウェア、ハードウェア、ファームウェア、またはそれらの任意の好適な組み合わせとして実装され得る。これらの要素は、本明細書に概説されるような動作を実現させるように、他のネットワーク要素と連携し得るソフトウェア（またはレシプロケーティングソフトウェア（ｒｅｃｉｐｒｏｃａｔｉｎｇ　ｓｏｆｔｗａｒｅ））をまた含み得る。

【００３２】

加えて、電子デバイス１０２ａ－１０２ｈ、クラウドサービス１０４、およびサーバ１０６の各々は、本明細書に説明されたようなアクティビティを実行するソフトウェアまたはアルゴリズムを実行可能なプロセッサを含み得る。プロセッサは、本明細書で詳述された操作を実現するように、データと関連づけられた任意の種類の命令を実行し得る。一例において、プロセッサは、要素または物品（例えば、データ）を、１つの状態または物から、別の状態または物に変換し得る。別の例において、本明細書に概説されるアクティビティは、固定されたロジックまたはプログラム可能なロジック（例えば、プロセッサによって実行されるソフトウェア／コンピュータ命令）によって実装され得、本明細書において特定される要素は、デジタルロジック、ソフトウェア、コード、電子命令、またはそれらの任意の好適な組み合わせを含む、何らかのタイプのプログラム可能なプロセッサ、プログラム可能なデジタルロジック（例えば、フィールドプログラマブルゲートアレー（ＦＰＧＡ）、ＥＰＲＯＭ、ＥＥＰＲＯＭ）、またはＡＳＩＣであり得る。本明細書で説明される、任意の潜在的な処理要素、モジュールおよび機械は、広義の用語「プロセッサ」の中に包含されると解釈されるべきである。

【００３３】

電子デバイス１０２ａ－１０２ｈは各々、ネットワーク要素であり得、例えば、デスクトップコンピュータ、ラップトップコンピュータ、モバイルデバイス、パーソナルデジタルアシスタント、スマートフォン、タブレット、または他の同様のデバイスを含む。クラウドサービス１０４は、クラウドサービスを電子デバイス１０２ａ－ｈに提供するように構成される。クラウドサービス１０４は、インターネットなどのネットワークにわたるサービスとして供給されるコンピューティングリソースの使用として、概して定義され得る。通常、計算、ストレージ、およびネットワークリソースがクラウドインフラストラクチャにおいて提供され、ワークロードをローカルネットワークからクラウドネットワークへ効果的にシフトする。サーバ１０６は、サーバまたは仮想サーバなどのネットワーク要素であり得、何らかのネットワーク（例えば、ネットワーク１０８）を介して通信システム１００ａおよび１００ｂにおいて通信を開始することを所望しているクライアント、顧客、エンドポイント、またはエンドユーザに関連づけられ得る。用語「サーバ」は、通信システム１００ａおよび１００ｂの中のクライアントの要求を果たす、および／または、クライアントの代わりにいくらかの計算のタスクを実行するように用いられるデバイスを含む。例外検知モジュール１１４が電子デバイス１０２ａに位置するものとして図１Ａに表されているが、これは例示目的のみである。例外検知モジュール１１４は、任意の好適な

構成において組み合わされ、または分離され得る。さらに、ローカルネットワーク例外検知モジュール１３０が電子デバイス１０２ｈに位置するものとして図１Ｂに表されているが、これは例示のみの目的である。ローカルネットワーク例外検知モジュール１３０は、任意の好適な構成において組み合わされ、または分離され得る。さらに、例外検知モジュール１１４およびローカルネットワーク例外検知モジュール１３０は各々、クラウドサービス１０４またはサーバ１０６などの電子デバイス１０２ａ－ｆによってアクセス可能な別のネットワークと統合され得、または、別のネットワーク内に分散され得る。

【００３４】

図２に移ると、図２は、一実施形態による、マルウェアを特定するための変則検知に関連づけられ得るフロー２００の可能な工程を示す、例示的なフローチャートである。一実施形態において、フロー２００の１または複数の工程は、例外検知モジュール１１４、ローカルネットワーク例外検知モジュール１３０、およびネットワーク例外検知モジュール１２４によって実行され得る。２０２において、デバイスがネットワークに接続される。２０４において、システムは、当該デバイスのメタデータが、ネットワークの外部で利用可能かどうか判断する。例えば、システムは、当該デバイスの普及度、期間、および他のメタデータが、ネットワークの外部で利用可能かどうか判断し得る。当該デバイスのメタデータがネットワークの外部で利用可能でない場合、２０８に示されるように、システムは、同様のタイプのデバイスがネットワークに接続されているかどうか判断する。当該デバイスのメタデータがネットワークの外部で利用可能である場合、２０６に示されるように、当該デバイスのメタデータがネットワークの外部から取得される。２０８において、システムは、同様のタイプのデバイスがネットワークに接続されているかどうか判断する。

【００３５】

同様のタイプのデバイスがネットワークに接続されていない場合、２１２に示されるように、当該デバイスのアクティビティがネットワーク上で観測される。同様のタイプのデバイスがネットワークに接続されている場合、同様のタイプのデバイスのメタデータが、当該デバイスのメタデータに追加される。２１２において、当該デバイスのアクティビティがネットワーク上で観測される。

【００３６】

２１４において、当該デバイスからのメタデータが生成される。２１６において、システムは、当該デバイスの生成されたメタデータが変更される必要があるかどうか判断する。当該デバイスの生成されたメタデータが変更される必要がある場合、２１８に示されるように、当該デバイスのメタデータは必要に応じて変更される。当該デバイスの生成されたメタデータが変更される必要がない場合、フローは終了し、当該デバイスのメタデータは変更されない。

【００３７】

図３に移ると、図３は、一実施形態による、マルウェアを特定するための変則検知に関連づけられ得るフロー３００の可能な工程を示す、例示的なフローチャートである。一実施形態において、フロー３００の１または複数の工程は、例外検知モジュール１１４、ローカルネットワーク例外検知モジュール１３０、およびネットワーク例外検知モジュール１２４によって実行され得る。３０２において、システムのメタデータが判断される。３０４において、システムのアクティビティが監視される。３０６において、システムは、システムのアクティビティが、システムの判断されたメタデータの範囲内にあるかどうか判断する。システムのアクティビティが、システムの判断されたメタデータの範囲内にある（例えば、例外がない）場合、３０４に示されるように、システムのアクティビティは監視され続ける。システムのアクティビティが、システムの判断されたメタデータの範囲内にない（例えば、例外が存在する）場合、３０８に示されるように、是正措置がとられる。例えば、是正措置は、マルウェアがないか、システムをスキャンすること、または、システムのアクティビティがシステムの判断されたメタデータの範囲内にないことに関するソース若しくは原因をトレースすることであり得る。

【００３８】
図４は、一実施形態による、ポイントツーポイント（ＰｔＰ）構成に配置された、コンピューティングシステム４００を示す。特に、図４は、プロセッサ、メモリ、および入力／出力デバイスが、複数のポイントツーポイントインタフェースによって相互結合されるシステムを示す。概して、通信システム１００ａおよび１００ｂのネットワーク要素の１または複数は、コンピューティングシステム４００と同じ、または同様の態様で構成され得る。
【００３９】
図４に示されるように、システム４００は、いくつかのプロセッサを含み得、明確さのために、それらのうちプロセッサ４７０および４８０の２つのみが示される。２つのプロセッサ４７０および４８０が示される一方、システム４００の実施形態は、また、そのようなプロセッサを１つのみ含み得ることが、理解されるべきである。プログラムの複数のスレッドを実行するように、プロセッサ４７０および４８０は各々、一組のコア（すなわち、プロセッサコア４７４Ａおよび４７４Ｂ、ならびにプロセッサコア４８４Ａおよび４８４Ｂ）を含み得る。コアは、図１－図３を参照して上に説明されたものと同様の態様で、命令コードを実行するように構成され得る。各プロセッサ４７０、４８０は、少なくとも１つの共有キャッシュ４７１、４８１を含み得る。共有キャッシュ４７１、４８１は、プロセッサコア４７４および４８４などの、プロセッサ４７０、４８０の１または複数のコンポーネントによって利用されるデータ（例えば、命令）を格納し得る。
【００４０】
プロセッサ４７０および４８０は各々、メモリ要素４３２および４３４と通信するための、統合されたメモリコントローラロジック（ＭＣ）４７２および４８２をまた含み得る。メモリ要素４３２および／または４３４は、プロセッサ４７０および４８０によって用いられる様々なデータを格納し得る。代替的な実施形態において、メモリコントローラロジック４７２および４８２は、プロセッサ４７０および４８０から独立した、個別のロジックであり得る。
【００４１】
プロセッサ４７０および４８０は、任意の種類のプロセッサであり得、ポイントツーポイントインタフェース回路４７８および４８８をそれぞれ用いて、ポイントツーポイント（ＰｔＰ）インタフェース４５０を介してデータを交換し得る。プロセッサ４７０および４８０は各々、ポイントツーポイントインタフェース回路４７６、４８６、４９４および４９８を用いて、個別のポイントツーポイントインタフェース４５２および４５４を介して、チップセット４９０とデータを交換し得る。チップセット４９０は、ＰｔＰインタフェース回路であり得るインタフェース回路４９２を用いて、高性能グラフィックインタフェース４３９を介して、高性能グラフィック回路４３８とデータをまた交換し得る。代替的な実施形態において、図４に示されたＰｔＰリンクのいずれかまたは全ては、ＰｔＰリンクではなくマルチドロップバスとして実装され得る。
【００４２】
チップセット４９０は、インタフェース回路４９６を介してバス４２０と通信し得る。バス４２０は、バスブリッジ４１８およびＩ／Ｏデバイス４１６などの、それを介して通信する１または複数のデバイスを有し得る。バス４１０を介して、バスブリッジ４１８は、キーボード／マウス４１２（または、タッチスクリーン、トラックボールなどの他の入力デバイス）、通信デバイス４２６（モデム、ネットワークインタフェースデバイス、または、コンピュータネットワーク４６０を通じて通信し得る他のタイプの通信デバイスなど）、オーディオＩ／Ｏデバイス４１４、および／またはデータストレージデバイス４２８などの、他のデバイスと通信し得る。データストレージデバイス４２８は、プロセッサ４７０および／または４８０によって実行され得る、コード４３０を格納し得る。代替的な実施形態において、バスアーキテクチャの任意の部分は、１または複数のＰｔＰリンクで実装され得る。
【００４３】

図４に図示されたコンピュータシステムは、本明細書に説明された様々な実施形態を実装するように利用され得るコンピューティングシステムの実施形態の、概略的な例示である。図４に図示されたシステムの様々なコンポーネントは、システムオンチップ（ＳｏＣ）アーキテクチャ、または任意の他の好適な構成で組み合わされ得ることが、理解されるであろう。例えば、本明細書に開示された実施形態は、スマートセルラ電話、タブレットコンピュータ、パーソナルデジタルアシスタント、携帯可能ゲームデバイスなどの、モバイルデバイスを含むシステム内に組み込まれ得る。これらのモバイルデバイスは、少なくともいくつかの実施形態において、ＳｏＣアーキテクチャを備え得ることが理解されるであろう。

【００４４】

図５に移ると、図５は、本開示の例示的なＡＲＭエコシステムＳｏＣ５００と関連づけられた簡略ブロック図である。本開示の少なくとも１つの例示的な実装は、本明細書で説明された変則検知機能、およびＡＲＭコンポーネントを含み得る。例えば、図５の例は、任意のＡＲＭコア（例えば、Ａ－７、Ａ－１５など）に関連づけられ得る。さらに、アーキテクチャは、任意の種類のタブレット、スマートフォン（Ａｎｄｒｏｉｄ（登録商標）ｐｈｏｎｅ、ｉＰｈｏｎｅ（登録商標）を含む）、ｉＰａｄ（登録商標）、Ｇｏｏｇｌｅ　Ｎｅｘｕｓ（登録商標）、Ｍｉｃｒｏｓｏｆｔ　Ｓｕｒｆａｃｅ（登録商標）、パーソナルコンピュータ、サーバ、ビデオ処理コンポーネント、ラップトップコンピュータ（任意の種類のノートブックを含む）、Ｕｌｔｒａｂｏｏｋ（登録商標）システム、任意の種類のタッチ対応入力デバイスなどの一部であり得る。

【００４５】

図５のこの例において、ＡＲＭエコシステムＳＯＣ５００は、液晶ディスプレイ（ＬＣＤ）に結合するモバイルインダストリープロセッサインタフェース（ＭＩＰＩ）／高精細度マルチメディアインタフェース（ＨＤＭＩ（登録商標））リンクと関連づけられ得る、複数のコア５０６－５０７、Ｌ２キャッシュ制御５０８、バスインタフェースユニット５０９、Ｌ２キャッシュ５１０、グラフィック処理ユニット（ＧＰＵ）５１５、インターコネクト５０２、ビデオコーデック５２０、およびＬＣＤ　Ｉ／Ｆ５２５を含み得る。

【００４６】

ＡＲＭエコシステムＳＯＣ５００は、加入者識別モジュール（ＳＩＭ）Ｉ／Ｆ５３０、ブートリードオンリメモリ（ＲＯＭ）５３５、シンクロナスダイナミックランダムアクセスメモリ（ＳＤＲＡＭ）コントローラ５４０、フラッシュメモリコントローラ５４５、シリアル周辺機器インタフェース（ＳＰＩ）マスター５５０、好適な電力制御５５５、ダイナミックＲＡＭ（ＤＲＡＭ）５６０、およびフラッシュメモリ５６５を、また含み得る。加えて、１または複数の例示的な実施形態は、１または複数の通信機能、インタフェース、ならびに、Ｂｌｕｅｔｏｏｔｈ（登録商標）５７０、３Ｇモデム５７５、全地球測位システム（ＧＰＳ）５８０、および８０２．１１Ｗｉ－Ｆｉ５８５という例などの機能を含み得る。

【００４７】

操作において、図５の例は、様々なタイプのコンピューティング（例えば、モバイルコンピューティング、ハイエンドデジタルホーム、サーバ、無線インフラストラクチャなど）を可能にする比較的低い電力消費と共に、処理機能を提供し得る。さらに、そのようなアーキテクチャは、任意の数のソフトウェアアプリケーション（例えば、Ａｎｄｒｏｉｄ（登録商標）、Ａｄｏｂｅ（Ｒ）　Ｆｌａｓｈ（Ｒ）プレーヤ、Ｊａｖａ（登録商標）プラットフォームスタンダードエディション（Ｊａｖａ（登録商標）ＳＥ）、Ｊａｖａ（登録商標）ＦＸ、Ｌｉｎｕｘ（登録商標）、Ｍｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）　Ｅｍｂｅｄｄｅｄ、ＳｙｍｂｉａｎおよびＵｂｕｎｔｕなど）を可能にし得る。少なくとも１つの例示的な実施形態において、コアプロセッサは、結合された低レイテンシのレベル２キャッシュを有するアウトオブオーダー・スーパースカラー・パイプラインを実装し得る。

【００４８】

図６は、一実施形態によるプロセッサコア６００を示す。プロセッサコア６００は、マイクロプロセッサ、組み込まれたプロセッサ、デジタル信号プロセッサ（ＤＳＰ）、ネットワークプロセッサ、またはコードを実行する他のデバイスなど、任意の種類のプロセッサのためのコアであり得る。１つのみのプロセッサコア６００が図６に示されているが、プロセッサは、図６に示されたプロセッサコア６００のうちの１つより多くを、代替的に含み得る。例えば、プロセッサコア６００は、図４のプロセッサ４７０および４８０を参照して示されおよび説明された、プロセッサコア４７４ａ、４７４ｂ、４８４ａおよび４８４ｂの１つの例示的な実施形態を示す。プロセッサコア６００は、シングルスレッドコアであり得、または、少なくとも１つの実施形態に関して、プロセッサコア６００は、コア毎に１つより多いハードウェアスレッドコンテキスト（または「論理プロセッサ」）を含み得るという点で、マルチスレッドであり得る。

【００４９】

図６は、一実施形態によるプロセッサコア６００に結合されるメモリ６０２を、また示す。メモリ６０２は、知られているような、そうでなければ当業者に利用可能なような、任意の多種多様なメモリ（メモリ階層の様々な層を含む）であり得る。メモリ６０２は、プロセッサコア６００によって実行される、１または複数の命令であり得るコード６０４を含み得る。プロセッサコア６００は、コード６０４によって示される命令のプログラムシーケンスに従ってよい。各命令はフロントエンドロジック６０６に入り、１または複数のデコーダ６０８によって処理される。デコーダは、その出力として、予め定義されたフォーマットの固定幅マイクロオペレーションなどの、マイクロオペレーションを生成し得、または、オリジナルのコード命令を反映する他の命令、マイクロ命令、または制御信号を生成し得る。フロントエンドロジック６０６は、レジスタリネーミングロジック６１０およびスケジューリングロジック６１２をまた含み、それは概して、リソースを割り当て、実行のための命令に対応する操作をキューに登録する。

【００５０】

プロセッサコア６００は、一組の実行ユニット６１６－１から６１６－Ｎを有する実行ロジック６１４を、また含み得る。いくつかの実施形態は、特定の機能または機能の組に専用の、複数の実行ユニットを含み得る。他の実施形態は、１つの実行ユニットのみ、または、特定の機能を実行し得る１つの実行ユニットを含み得る。実行ロジック６１４は、コード命令によって指定される動作を実行する。

【００５１】

コード命令によって指定される動作の実行の完了後、バックエンドロジック６１８は、コード６０４の命令をリタイアし得る。一実施形態において、プロセッサコア６００は、アウトオブオーダー実行を可能にするが、命令のインオーダーリタイアメントを必要とする。リタイアメントロジック６２０は、様々な知られている形態（例えば、リオーダーバッファまたは同様のもの）を取り得る。本態様において、プロセッサコア６００は、少なくとも、デコーダによって生成される出力、レジスタリネーミングロジック６１０によって利用されるハードウェアレジスタおよびテーブル、および実行ロジック６１４によって書き換えられた任意のレジスタ（示されない）の観点から、コード６０４の実行の最中に変換される。

【００５２】

図６には示されないが、プロセッサは、プロセッサコア６００を有するチップ上の他の要素を含み得、その少なくともいくらかが図６を参照して本明細書で示されて説明される。例えば、図６に示されるように、プロセッサは、プロセッサコア６００と共にメモリ制御ロジックを含み得る。プロセッサは、Ｉ／Ｏ制御ロジックを含み得、および／または、メモリ制御ロジックと統合されたＩ／Ｏ制御ロジックを含み得る。

【００５３】

本明細書に提供された例と共に、相互作用は、２つ、３つ、またはより多くのネットワーク要素の観点から説明され得ることに留意する。しかしながら、これは、明確さおよび例示のみの目的で成されている。特定の場合には、限られた数のネットワーク要素を参照

するのみによって、所与の組のフローの機能の１または複数の説明がより容易になり得る。通信システム１００ａおよび１００ｂおよびそれらの教示は、容易に拡張可能であり、多数のコンポーネント、ならびに、より複雑な／洗練された配置及び構成に対応し得ることが、理解されるべきである。従って、提供された例は、無数の他のアーキテクチャに潜在的に適用されるものとしての通信システム１００ａおよび１００ｂの、範囲を制限すべきではなく、または、広い教示を阻むべきではない。

【００５４】

前述のフロー図（すなわち、図２および図３）における操作は、通信システム１００ａおよび１００ｂによって、または通信システム１００ａおよび１００ｂの中で実行され得る、起こり得る相関するシナリオおよびパターンのいくつかのみを示すことに留意することが、また重要である。これらの操作のいくつかは、必要に応じて削除され得、または取り除かれ得、または、これらの操作は、本開示の範囲から逸脱することなく、大幅に書き換えられ得、または変更され得る。加えて、これらの操作の多数は、１または複数の追加の動作と同時に、またはそれと並行して実行されるものとして、説明されてきた。しかしながら、これらの操作のタイミングは大幅に変更され得る。前述の操作フローは、例示および説明の目的で提供されている。任意の好適な配置、時系列、構成、およびタイミング機構が、本開示の教示から逸脱することなく提供され得るという点で、かなりの柔軟性が、通信システム１００ａおよび１００ｂによって提供される。

【００５５】

本開示は特定の配置及び構成を参照して詳細に説明されているが、これらの例示的な構成および配置は、本開示の範囲から逸脱することなく、大幅に変更され得る。さらに、特定のコンポーネントが、特定の必要性および実装に基づいて、組み合わされ、分離され、除去され、または追加され得る。加えて、通信システム１００ａおよび１００ｂは、通信処理を容易にする特定の要素及び動作を参照して示されるが、これらの要素及び動作は、通信システム１００ａおよび１００ｂの意図される機能を実現する任意の好適なアーキテクチャ、プロトコル、および／またはプロセスによって置換され得る。

【００５６】

数多くの他の変化、代替、変形、変更、および修正が、本分野の当業者に確認され得、本開示は、添付の特許請求の範囲の中に属するそのような変化、代替、変形、変更、および修正を、全て包含することが意図されている。米国特許商標庁（ＵＳＰＴＯ）、および加えて、本出願に関して発行される任意の特許の任意の読者の助力となるように、本明細書に添付の特許請求の範囲の解釈において、出願人は、以下に留意することを望む。（ａ）出願人は、添付のいかなる請求項も、文言「ための手段」または「ための段階」が特定の請求項において具体的に用いられない限り、本明細書の出願の日において存在する米国特許法第１１２条第６パラグラフを発動させる意図はない。（ｂ）出願人は、添付の特許請求の範囲に反映されない限り、本明細書におけるいかなる発言によっても、いかなる方法でも、本開示を限定する意図はない。

［他の注記および例］

【００５７】

例Ｃ１は、少なくとも１つのプロセッサによって実行された場合、少なくとも１つのプロセッサに、システムにおけるオブジェクトのアクティビティを監視させ、監視されたアクティビティをシステムのメタデータと比較させ、潜在的に悪意のあるアクティビティを検知すべく、一般性の低い例外を特定させる、１または複数の命令を有する少なくとも１つの機械可読媒体である。

【００５８】

例Ｃ２において、例Ｃ１の主題は、監視されたアクティビティをシステムのメタデータと比較することが、ポリモーフィック型の脅威を特定するための、システムにおけるオブジェクトのメタデータの分析を含むことを、随意に含み得る。

【００５９】

例Ｃ３において、例Ｃ１－Ｃ２のうちの任意の１つの主題は、監視されたアクティビテ

ィをシステムのメタデータと比較することが、オブジェクトが別のオブジェクトからのメタデータを再使用することを検知するための、システムのオブジェクトの再使用の分析を含むことを、随意に含み得る。

【００６０】

例Ｃ４において、例Ｃ１－Ｃ３のうちの任意の１つの主題は、潜在的に悪意のあるアクティビティを検知すべく、一般性の低い例外の期間が、少なくとも部分的に用いられることを、随意に含み得る。

【００６１】

例Ｃ５において、例Ｃ１－Ｃ４のうちの任意の１つの主題は、監視されたアクティビティがシステムのファイル名の分析を含むことを、随意に含み得る。

【００６２】

例Ｃ６において、例Ｃ１－Ｃ５のうちの任意の１つの主題は、潜在的に悪意のあるアクティビティがオブジェクトと関連づけられ、オブジェクトがマルウェアスキャンされることを、随意に含み得る。

【００６３】

例Ｃ７において、例Ｃ１－Ｃ６のうちの任意の１つの主題は、システムのメタデータが、システム上で監視された、前のアクティビティから生成されることを、随意に含み得る。

【００６４】

例Ｃ８において、例Ｃ１－Ｃ７のうちの任意の１つの主題は、システムのメタデータが、同様のシステムの他のメタデータに少なくとも部分的に基づくことを、随意に含み得る。

【００６５】

例Ａ１において、電子デバイスは例外検知モジュールを含み得、例外検知モジュールは、システムにおけるオブジェクトのアクティビティを監視し、監視されたアクティビティをシステムのメタデータと比較し、潜在的に悪意のあるアクティビティを検知すべく、一般性の低い例外を特定するように構成される。

【００６６】

例Ａ２において、例Ａ１の主題は、監視されたアクティビティをシステムのメタデータと比較することが、ポリモーフィック型の脅威を特定するための、システムにおけるオブジェクトのメタデータの分析を含むことを、随意に含み得る。

【００６７】

例Ａ３において、例Ａ１－Ａ２のうちの任意の１つの主題は、監視されたアクティビティをシステムのメタデータと比較することが、オブジェクトが別のオブジェクトからのメタデータを再使用することを検知するための、システムのオブジェクトの再使用の分析を含むことを、随意に含み得る。

【００６８】

例Ａ４において、例Ａ１－Ａ３のうちの任意の１つの主題は、悪意のあるアクティビティを検知すべく、一般性の低い例外の期間が、少なくとも部分的に用いられることを、随意に含み得る。

【００６９】

例Ａ５において、例Ａ１－Ａ４のうちの任意の１つの主題は、監視されたアクティビティがシステムのファイル名の分析を含むことを、随意に含み得る。

【００７０】

例Ａ６において、例Ａ１－Ａ５のうちの任意の１つの主題は、潜在的に悪意のあるアクティビティがオブジェクトと関連づけられ、オブジェクトがマルウェアスキャンされることを、随意に含み得る。

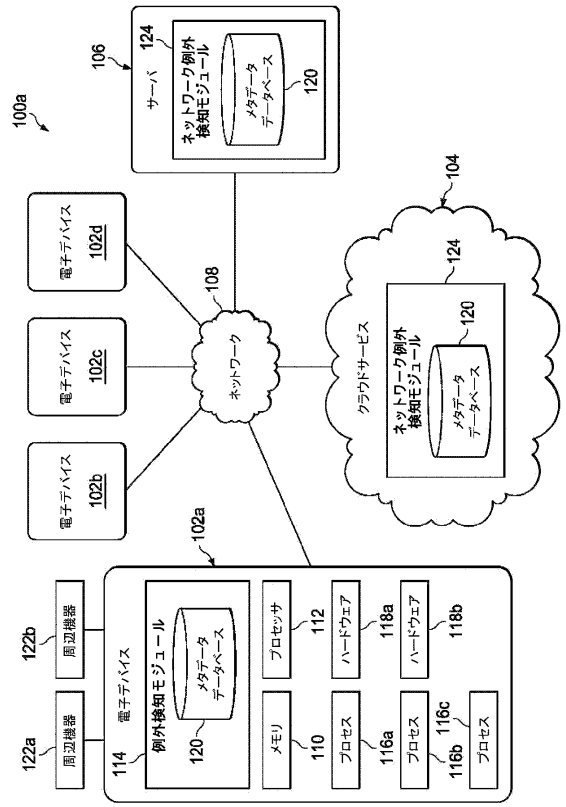
【００７１】

例Ａ７において、例Ａ１－Ａ６のうちの任意の１つの主題は、システムのメタデータが、システム上で監視された、前のアクティビティから生成されることを、随意に含み得る

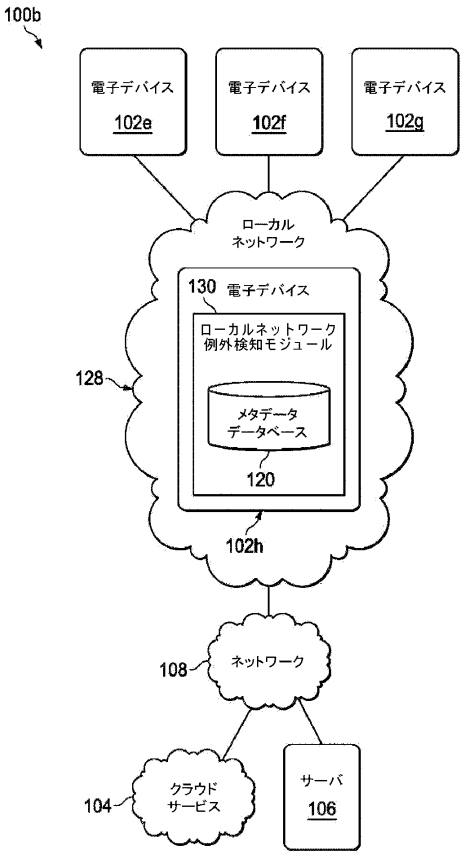
。
【００７２】
例Ａ８において、例Ａ１－Ａ７のうちの任意の１つの主題は、システムのメタデータが、同様のシステムの他のメタデータに少なくとも部分的に基づくことを、随意に含み得る。
【００７３】
例Ｍ１は、システムにおけるオブジェクトのアクティビティを監視することと、監視されたアクティビティをシステムのメタデータと比較することと、潜在的に悪意のあるアクティビティを検知すべく、一般性の低い例外を特定することと、を含む方法である。
【００７４】
例Ｍ２において、例Ｍ１の主題は、監視されたアクティビティをシステムのメタデータと比較することが、ポリモーフィック型の脅威を特定するための、システム上のオブジェクトのメタデータの分析を含むことを、随意に含み得る。
【００７５】
例Ｍ３において、例Ｍ１－Ｍ２のうちの任意の１つの主題は、監視されたアクティビティをシステムのメタデータと比較することが、オブジェクトが別のオブジェクトからのメタデータを再使用することを検知するための、システムのオブジェクトの再使用の分析を含むことを、随意に含み得る。
【００７６】
例Ｍ４において、例Ｍ１－Ｍ３のうちの任意の１つの主題は、潜在的に悪意のあるアクティビティを検知すべく、一般性の低い例外の期間が、少なくとも部分的に用いられることを、随意に含み得る。
【００７７】
例Ｍ５において、例Ｍ１－Ｍ４のうちの任意の１つの主題は、監視されたアクティビティがシステムのファイル名の分析を含むことを、随意に含み得る。
【００７８】
例Ｍ６において、例Ｍ１－Ｍ５のうちの任意の１つの主題は、潜在的に悪意のあるアクティビティをオブジェクトと関連づけることと、潜在的に悪意のあるオブジェクトに対しマルウェアのスキャンをすることとを、随意に含み得る。
【００７９】
例Ｍ７において、例Ｍ１－Ｍ６のうちの任意の１つの主題は、システムのメタデータが、システム上で監視された、前のアクティビティから生成されることを、随意に含み得る。
【００８０】
例Ｓ１は、マルウェアを特定するための変則検知のためのシステムであり、システムは、システムにおけるオブジェクトのアクティビティを監視し、監視されたアクティビティをシステムのメタデータと比較し、潜在的に悪意のあるアクティビティを検知すべく、一般性の低い例外を特定するように構成された、例外検知モジュールを含む。
【００８１】
例Ｓ２において、例Ｓ１の主題は、監視されたアクティビティをシステムのメタデータと比較することが、ポリモーフィック型の脅威を特定するための、システムにおけるオブジェクトのメタデータの分析、オブジェクトが別のオブジェクトからのメタデータを再使用することを検知するための、システムのオブジェクトの再使用の分析、およびシステムのファイル名の分析を随意に含み得る。
【００８２】
例Ｘ１は、例Ａ１－Ａ８、またはＭ１－Ｍ７のうちの任意の１つに示されるような方法を実装するための、または装置を実現するための、機械可読命令を含む機械可読記憶媒体である。例Ｙ１は、例の方法Ｍ１－Ｍ７のうちのいずれかを実行するための手段を含む装置である。例Ｙ２において、例Ｙ１の主題は、方法を実行するための、プロセッサおよびメモリを含む手段を随意に含み得る。例Ｙ３において、例Ｙ２の主題は、機械可読命令を

含むメモリを随意に含み得る。

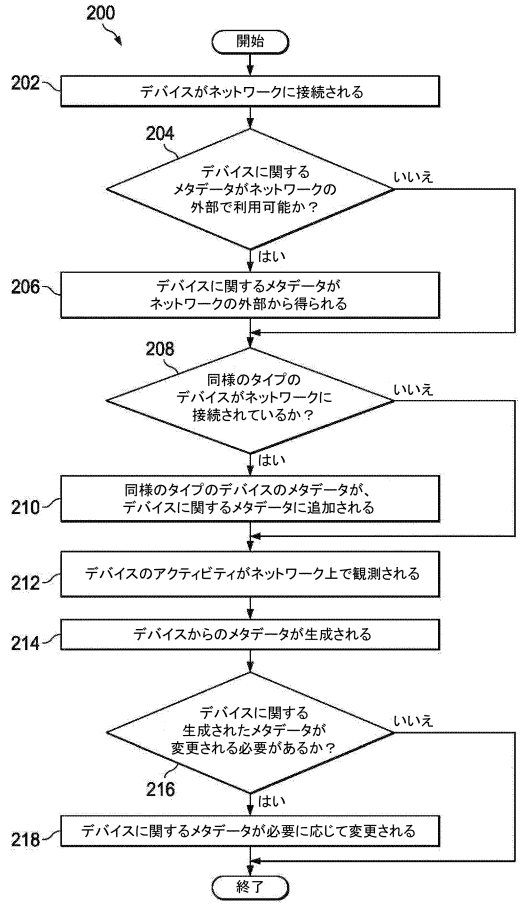
【図１Ａ】



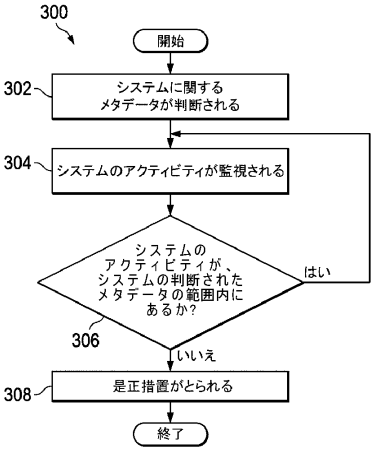
【図１Ｂ】



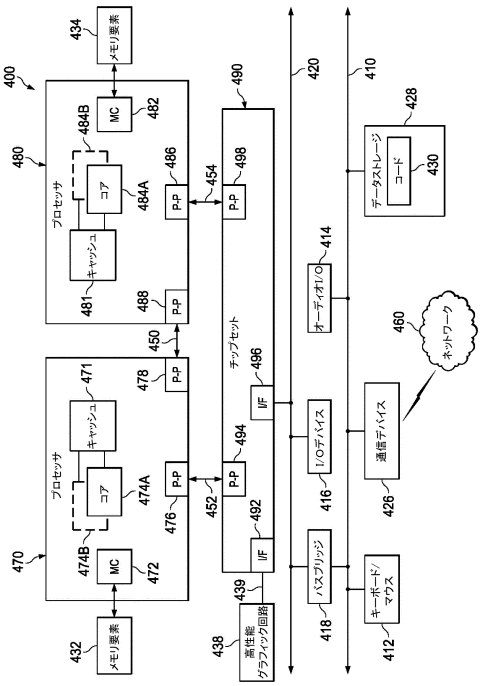
【図２】


200
開始
202
デバイスがネットワークに接続される
204
デバイスに関する
メタデータがネットワークの
外部で利用可能か？
いいえ
はい
206
デバイスに関するメタデータが
ネットワークの外部から得られる
208
同様のタイプの
デバイスがネットワークに
接続されているか？
いいえ
はい
210
同様のタイプのデバイスのメタデータが、
デバイスに関するメタデータに追加される
212
デバイスのアクティビティがネットワーク上で観測される
214
デバイスからのメタデータが生成される
デバイスに関する
生成されたメタデータが
変更される必要があるか？
いいえ
216
はい
218
デバイスに関するメタデータが必要に応じて変更される
終了

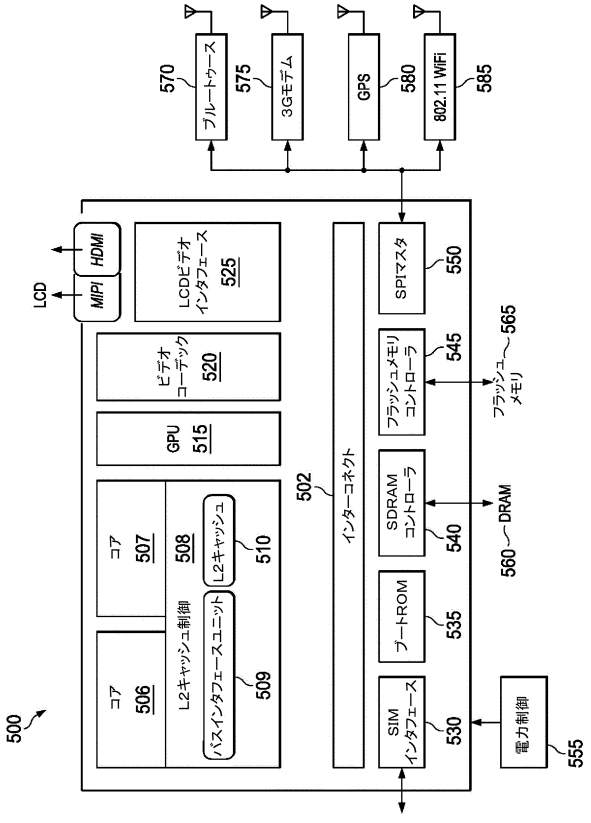
【図３】


300
開始
302
システムに関する
メタデータが判断される
304
システムのアクティビティが監視される
システムの
アクティビティが、
システムの判断された
メタデータの範囲内に
あるか？
はい
306
いいえ
308
是正措置がとられる
終了

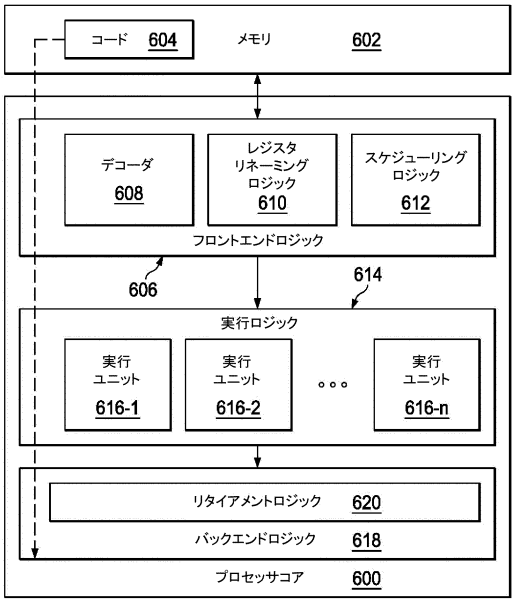
【図４】


400
480
プロセッサ
コア
484A
484B
キャッシュ
481
MC
482
メモリ要素
434
P-P
486
488
454
450
470
プロセッサ
コア
474A
474B
キャッシュ
471
MC
472
メモリ要素
432
P-P
478
476
452
490
チップセット
P-P
498
P-P
494
IF
496
IF
492
高性能
グラフィック回路
438
439
420
410
データストレージ
コード
428
430
オーディオI/O
414
I/Oデバイス
416
バスブリッジ
418
通信デバイス
426
キーボード/
マウス
412
ネットワーク
460

【図５】


500
570
ブルートゥース
575
3Gモデム
580
GPS
585
802.11 WiFi
LCD
HDMI
MIPI
LCDビデオ
インタフェース
525
ビデオ
コーデック
520
GPU
515
コア
507
L2キャッシュ
510
L2キャッシュ制御
508
バスインタフェースユニット
509
コア
506
502
インターコネクト
SPIマスタ
550
フラッシュメモリ
コントローラ
545
フラッシュ
メモリ
565
SDRAM
コントローラ
540
DRAM
560
ブートROM
535
SIM
インタフェース
530
電力制御
555

【図６】


コード 604
メモリ 602
デコーダ 608
レジスタリネーミングロジック 610
スケジューリングロジック 612
フロントエンドロジック
606
614
実行ロジック
実行ユニット 616-1
実行ユニット 616-2
実行ユニット 616-n
リタイアメントロジック 620
バックエンドロジック 618
プロセッサコア 600

フロントページの続き

(72)発明者　スパーロック、ジョエル　アール.
アメリカ合衆国、９５０５４　カリフォルニア州、サンタ　クララ、ミッション　カレッジ　ブールバード　２８２１　マカフィー，　インコーポレイテッド内

審査官　平井　誠

(56)参考文献　特表２０１４－５０４７６５（ＪＰ，Ａ）
特表２０１１－５２３７４８（ＪＰ，Ａ）
米国特許出願公開第２０１２／０３０４２８８（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５－５６