

(19) 日本国特許庁(JP)

(12) 公表特許公報(A)

(11) 特許出願公表番号

特表2016-511847

(P2016-511847A)

(43) 公表日 平成28年4月21日(2016.4.21)

(51) Int.Cl.	F I	テーマコード (参考)
G 0 6 F 21/55 (2013.01)	G O 6 F 21/55	5 B O 8 9
G 0 6 F 13/00 (2006.01)	G O 6 F 13/00	3 5 1 N

審査請求 未請求 予備審査請求 未請求 (全 69 頁)

(21) 出願番号 特願2015-546521 (P2015-546521) (86) (22) 出願日 平成25年11月27日 (2013.11.27) (85) 翻訳文提出日 平成27年5月12日 (2015.5.12) (86) 国際出願番号 PCT/US2013/072388 (87) 国際公開番号 W02014/088912 (87) 国際公開日 平成26年6月12日 (2014.6.12) (31) 優先権主張番号 13/707,498 (32) 優先日 平成24年12月6日 (2012.12.6) (33) 優先権主張国 米国 (US)	(71) 出願人 500520743 ザ・ボーイング・カンパニー The Boeing Company アメリカ合衆国、60606-2016 イリノイ州、シカゴ、ノース・リバーサイド・プラザ、100 (74) 代理人 100108453 弁理士 村山 靖彦 (74) 代理人 100133400 弁理士 阿部 達彦 (74) 代理人 100163522 弁理士 黒田 晋平 (74) 代理人 100154922 弁理士 崔 允辰
--	--

最終頁に続く

(54) 【発明の名称】脅威検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリング

(57) 【要約】

開示する方法は、ユーザに対する挙動プロファイルを生成するために、ネットワーク内の、少なくとも1人のユーザと関連付けられた、少なくとも1つのノードの挙動をモニタリングすることを含む。本方法は、少なくとも1人のユーザに対する挙動プロファイルを、そのユーザに対するベースライン挙動プロファイルと比較することをさらに含む。また、本方法は、少なくとも1人のユーザに対する挙動プロファイルと、そのユーザに対するベースライン挙動プロファイルとの間の差異がいつ存在するかを判断することを含む。さらに、本方法は、その差異が、ベースライン閾値レベルを超えた場合、ベースライン閾値レベルを超えない場合、少なくとも1つの基準を満たす場合、および／または少なくとも1つの基準を満たさない場合、その差異と関連付けられたイベントにフラグを立てることを含む。さらに、本方法は、イベントをイベント種別に分類することを含む。さらに、本方法は、そのイベントを、ネットワーク内の少なくとも1つの他のノードおよび／またはネットワーク・オペレーション・センターに送信することを含む。

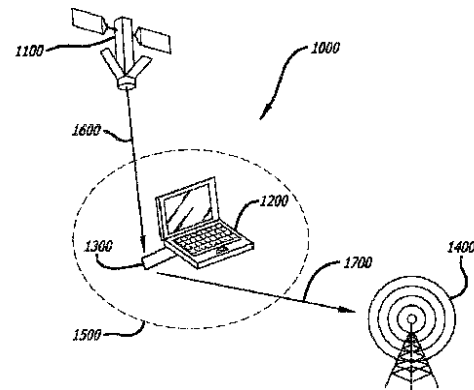


FIG. 1

【特許請求の範囲】

【請求項1】

脅威検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための方法であって、

前記方法は、

少なくとも1つのプロセッサによって、少なくとも1人のユーザに対する挙動プロファイルを生成するために、ネットワーク内の、前記少なくとも1人のユーザと関連付けられた、少なくとも1つのノードの挙動をモニタリングするステップと、

前記少なくとも1つのプロセッサによって、前記少なくとも1人のユーザに対する前記挙動プロファイルを、前記少なくとも1人のユーザに対するベースライン挙動プロファイルと比較するステップと、

10

前記少なくとも1つのプロセッサによって、前記少なくとも1人のユーザに対する前記挙動プロファイルと、前記少なくとも1人のユーザに対する前記ベースライン挙動プロファイルとの間の差異がいつ存在するかを判断するステップと、

前記少なくとも1つのプロセッサによって、前記差異が、ベースライン閾値レベルを超えた場合、ベースライン閾値レベルを超えない場合、少なくとも1つの基準を満たす場合、および少なくとも1つの基準を満たさない場合、前記少なくとも1つの差異と関連付けられたイベントにフラグを立てるステップと、

前記少なくとも1つのプロセッサによって、前記イベントをイベント種別に分類するステップとを備える、方法。

20

【請求項2】

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードと関連付けられた少なくとも1つの送信器によって、前記イベントを、前記ネットワーク内の少なくとも1つの他のノードおよびネットワーク・オペレーション・センターの少なくとも1つに送信するステップをさらに備える、請求項1に記載の方法。

【請求項3】

前記方法が、少なくとも1つの送信元によって、前記少なくとも1人のユーザに対する前記ベースライン挙動プロファイルを、前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードに送信するステップと、前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードと関連付けられた少なくとも1つの受信器によって、前記少なくとも1人のユーザに対する前記ベースライン挙動プロファイルを受信するステップとをさらに備える、請求項1に記載の方法。

30

【請求項4】

前記少なくとも1つの送信元が、前記ネットワーク内の少なくとも1つの他のノードおよび前記ネットワーク・オペレーション・センターの少なくとも一方と関連付けられる、請求項3に記載の方法。

【請求項5】

前記少なくとも1つのプロセッサが、前記少なくとも1人のユーザと関連付けられる前記少なくとも1つのノード、前記ネットワーク内の少なくとも1つの他のノード、および前記ネットワーク・オペレーション・センターの少なくとも1つと関連付けられる、請求項1に記載の方法。

40

【請求項6】

前記方法は、少なくとも1つの送信元によって、イベントアップデートを、前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードに送信するステップと、前記少なくとも1つのプロセッサによって、前記イベントアップデートを使用することにより、前記少なくとも1人のユーザに対する前記ベースライン挙動プロファイルをアップデートするステップとをさらに備える、請求項1に記載の方法。

【請求項7】

前記少なくとも1つの送信元が、前記ネットワーク内の少なくとも1つの他のノードおよび前記ネットワーク・オペレーション・センターの少なくとも一方と関連付けられる、請

50

求項6に記載の方法。

【請求項8】

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードの前記挙動をモニタリングする前記ステップが、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードの使用をモニタリングするステップと、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードの箇所をモニタリングするステップと、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードを通るデータをモニタリングするステップと、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードを通る前記データの量をモニタリングするステップと、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードを通る前記データの時間をモニタリングするステップと、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードを通る前記データの日付をモニタリングするステップと、

前記データを最初に送信した起点供給源をモニタリングするステップと、

前記データを送信する宛先をモニタリングするステップとの少なくとも1つを含む、請求項1に記載の方法。

【請求項9】

前記方法は、少なくとも1つの認証デバイスを用いて、前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードの箇所を認証するステップをさらに備える、請求項1に記載の方法。

【請求項10】

前記少なくとも1つの認証デバイスは、少なくとも1つの認証信号を評価することによって、前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードの前記箇所を認証する、請求項9に記載の方法。

【請求項11】

前記少なくとも1つの認証信号は、少なくとも1つの送信元によって送信され、前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードと関連付けられた少なくとも1つの受信先によって受信される、請求項10に記載の方法。

【請求項12】

前記少なくとも1つの送信元は、少なくとも1つの衛星および少なくとも1つの疑似衛星の少なくとも一方で使用される、請求項3、6、11のいずれか一項に記載の方法。

【請求項13】

前記少なくとも1つの衛星は、低軌道周回（LEO）衛星、中軌道周回（MEO）衛星、および静止地球軌道（GEO）衛星の少なくとも1つである、請求項12に記載の方法。

【請求項14】

前記少なくとも1つの基準は、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードの箇所と、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードを通るデータの種類と、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードが前記データを受信する時間と、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードが前記データを受信する日と、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードが前記データを送信する時間と、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノード

10

20

30

40

50

が前記データを送信する日と、

前記データを最初に送信した起点供給源の箇所と、

前記データが送信される宛先の箇所との少なくとも1つに関する、請求項1に記載の方法。

【請求項15】

少なくとも1人のユーザに対する挙動プロファイルを生成するために、ネットワーク内の前記少なくとも1人のユーザと関連付けられた少なくとも1つのノードの挙動をモニタリングし、前記少なくとも1人のユーザに対する前記挙動プロファイルを、前記少なくとも1人のユーザに対するベースライン挙動プロファイルと比較し、前記少なくとも1人のユーザに対する前記挙動プロファイルと、前記少なくとも1人のユーザに対する前記ベースライン挙動プロファイルとの間にいつ差異が生じたかを判断し、前記少なくとも1つの差異が、ベースライン閾値レベルを超える場合、ベースライン閾値レベルを超えない場合、少なくとも1つの基準を満たす場合、および少なくとも1つの基準を満たさない場合の少なくとも1つの場合に、前記差異と関連付けられたイベントにフラグを立て、前記イベントをイベント種別に分類するための少なくとも1つのプロセッサと、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードと関連付けられ、前記イベントを、前記ネットワーク内の少なくとも1つの他のノードおよびネットワーク・オペレーション・センターに送信するための少なくとも1つの送信器を備える、システム。

【請求項16】

前記少なくとも1人のユーザに対する前記ベースライン挙動プロファイルを、前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードに送信するための少なくとも1つの送信元と、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードと関連付けられ、前記少なくとも1人のユーザに対する前記ベースライン挙動プロファイルを受信するための少なくとも1つの受信器とをさらに備える、請求項15に記載のシステム。

【請求項17】

前記少なくとも1つの送信元が、前記ネットワーク内の少なくとも1つの他のノードおよび前記ネットワーク・オペレーション・センターの少なくとも一方と関連付けられる、請求項16に記載のシステム。

【請求項18】

前記少なくとも1つのプロセッサが、前記少なくとも1人のユーザと関連付けられる前記少なくとも1つのノード、前記ネットワーク内の少なくとも1つの他のノード、および前記ネットワーク・オペレーション・センターの少なくとも1つと関連付けられる、請求項15に記載のシステム。

【請求項19】

前記システムが、イベントアップデートを、前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードに送信する少なくとも1つの送信元をさらに備え、前記少なくとも1つのプロセッサが、前記イベントアップデートを使用することにより、前記少なくとも1人のユーザに対する前記ベースライン挙動プロファイルをさらにアップデートする、請求項15に記載のシステム。

【請求項20】

前記少なくとも1つの送信元が、前記ネットワーク内の少なくとも1つの他のノードおよび前記ネットワーク・オペレーション・センターの少なくとも1つと関連付けられる、請求項19に記載のシステム。

【請求項21】

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードの前記挙動をモニタリングする前記ステップが、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードの使用をモニタリングするステップと、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードの箇所をモニタリングするステップと、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードを通るデータをモニタリングするステップと、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードを通る前記データの量をモニタリングするステップと、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードを通る前記データの時間をモニタリングするステップと、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードを通る前記データの日付をモニタリングするステップと、

前記データを最初に送信した起点供給源をモニタリングするステップと、

前記データを送信する宛先をモニタリングするステップとの少なくとも1つを含む、請求項15に記載のシステム。

【請求項 2 2】

前記システムが、前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードの箇所を認証する少なくとも1つの認証デバイスをさらに備える、請求項15に記載のシステム。

【請求項 2 3】

前記少なくとも1つの認証デバイスが、少なくとも1つの認証信号を評価することによって、前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードの前記箇所を認証する、請求項22に記載のシステム。

【請求項 2 4】

前記少なくとも1つの認証信号は、少なくとも1つの送信元によって送信され、前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのノードと関連付けられた少なくとも1つの受信先によって受信される、請求項23に記載のシステム。

【請求項 2 5】

前記少なくとも1つの送信元は、少なくとも1つの衛星および少なくとも1つの疑似衛星の少なくとも一方で使用される、請求項16、19、24のいずれか一項に記載のシステム。

【請求項 2 6】

前記少なくとも1つの衛星は、低軌道周回（LEO）衛星、中軌道周回（MEO）衛星、および静止地球軌道（GEO）衛星の少なくとも1つである、請求項25に記載のシステム。

【請求項 2 7】

前記少なくとも1つの基準は、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードの箇所と、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードを通るデータの種類と、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードが前記データを受信する時間と、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードが前記データを受信する日と、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードが前記データを送信する時間と、

前記少なくとも1人のユーザと関連付けられた前記少なくとも1つのネットワークノードが前記データを送信する日と、

前記データを最初に送信した起点供給源の箇所と、

前記データが送信される宛先の箇所との少なくとも1つに関する、請求項15に記載のシステム。

【発明の詳細な説明】

【技術分野】

10

20

30

40

50

【0001】

関連出願の相互参照

本出願は、2010年11月18日に出願された、米国特許出願番号第12/949,404号「Spot Beam Based Authentication」の部分係属出願であり、その利益を主張するものである、2011年9月21日に出願された、米国特許出願番号第13/239,183号「Network Topology Aided by Smart Agent Download」の部分係属出願であり、その利益を主張するものである。両特許出願の内容は、その全体が、参照により、本明細書に組み込まれる。

【0002】

本出願は、2011年3月8日にKnappらに付与された米国特許第7,903,566号「Methods and Systems for Anomaly Detection Using Internet Protocol (IP) Traffic Conversation Data」および2011年8月9日にKnappらに付与された米国特許第7,995,496号「Methods and Systems for Internet Protocol (IP) Traffic Conversation Detection and Storage」に関する。

10

【0003】

さらに、本開示は、ネットワーク・セキュリティ・モニタリングに関する。具体的には、脅威検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングに関する。

【発明の概要】

【発明が解決しようとする課題】

【0004】

20

【課題を解決するための手段】

【0005】

1つまたは複数の実施形態において、本開示は、脅威検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための方法、システム、および装置に関する。特に、本開示は、少なくとも1つのプロセッサにより、そのユーザに対する挙動プロファイルを生成するために、ネットワーク内の、少なくとも1人のユーザと関連付けられた、少なくとも1つのノードの挙動をモニタリングすることを含む方法を教示する。本方法は、少なくとも1つのプロセッサにより、少なくとも1人のユーザに対する挙動プロファイルを、そのユーザに対するベースライン挙動プロファイルと比較することをさらに含む。また、本方法は、少なくとも1つのプロセッサにより、少なくとも1人のユーザに対する挙動プロファイルと、そのユーザに対するベースライン挙動プロファイルとの間の差異がいつ存在するかを判断することを含む。さらに、本方法は、少なくとも1つのプロセッサにより、その差異が、ベースライン閾値レベルを超えた場合、ベースライン閾値レベルを超えない場合、少なくとも1つの基準を満たす場合、および／または少なくとも1つの基準を満たさない場合、その差異と関連付けられたイベントにフラグを立てることを含む。または、本方法は、少なくとも1つのプロセッサにより、イベントをイベント種別に分類することを含む。さらに、本方法は、少なくとも1人のユーザと関連付けられた少なくとも1つのノードと関連付けられた少なくとも1つの送信器によって、そのイベントを、ネットワーク内の少なくとも1つの他のノードおよび／またはネットワーク・オペレーション・センターに送信することを含む。

30

40

【0006】

少なくとも1つの実施形態において、少なくとも1つのノード（少なくとも1人のユーザと関連付けられるか、または少なくとも1人のユーザと関連付けられない）は、携帯電話、携帯情報端末（PDA）、パーソナルコンピュータ、コンピュータノード、インターネットプロトコル（IP）ノード、サーバ、ルータ、ゲートウェイ、Wi-Fiノード、ネットワークノード、パーソナル・エリア・ネットワーク（PAN）ノード、ローカル・エリア・ネットワーク（LAN）ノード、ワイド・エリア・ネットワーク（WAN）ノード、Bluetoothノード、ZigBeeノード、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス（WiMAX）ノード、第2世代（2G）無線ノード、第3世代（3G）無線ノード、および／または第4世代（4G）無線ノードである。

50

【0007】

1つまたは複数の実施形態において、本方法は、少なくとも1つのプロセッサにより、少なくとも1人のユーザと関連付けられた、そのユーザに対するベースライン挙動プロファイルの生成するために、ネットワーク内の少なくとも1つのノードの挙動を最初にモニタリングすることをさらに含む。少なくとも1つの実施形態において、本方法は、少なくとも1つの送信元によって、少なくとも1人のユーザに対するベースライン挙動プロファイルを、少なくとも1人のユーザと関連付けられたノードに送信すること、および少なくとも1人のユーザと関連付けられたノードと関連付けられた少なくとも1つの受信器によって、そのユーザに対するベースライン挙動プロファイルを受信することをさらに含む。1つまたは複数の実施形態において、少なくとも1つの送信元は、ネットワーク内の少なくとも1つの他のノードおよび／またはネットワーク・オペレーション・センターと関連付けられる。少なくとも1つの実施形態において、少なくとも1つのプロセッサは、少なくとも1人のユーザと関連付けられる少なくとも1つのノード、ネットワーク内の少なくとも1つの他のノードおよび／またはネットワーク・オペレーション・センターと関連付けられる。

【0008】

少なくとも1つの実施形態において、少なくとも1つの送信元は、少なくとも1つの衛星および／または少なくとも1つの疑似衛星で使用される。いくつかの実施形態において、少なくとも1つの衛星は、低軌道周回（LEO）衛星、中軌道周回（MEO）衛星、および／または静止地球軌道（GEO）衛星である。1つまたは複数の実施形態において、開示する方法は、イリジウムLEO衛星コンステレーションを使用し、そのコンステレーションにおける衛星のそれぞれは、48スポットビームを特有のスポット・ビーム・パターンで送信するアンテナ形状を有する。少なくとも1つの実施形態において、少なくとも1つのベースライン挙動プロファイルおよび／またはスマート・エージェント・ダウンロードは、コンステレーションにおけるイリジウム衛星の少なくとも1つから送信することができる。イリジウム衛星の48スポットビームを使用して、地球表面上に設置されるか、または地球表面付近にある受信先に、局所的認証信号および／または少なくとも1つのベースライン挙動プロファイルならびに／もしくは少なくとも1つのスマート・エージェント・ダウンロード（少なくとも1人のユーザと関連付けられる少なくとも1つのノードと関連付けられる）を含む信号を送信することができる。これらの信号と関連付けられるブロードキャスト・メッセージ・バースト・コンテンツは、ランダムデータおよび／または疑似ランダムノイズ（PRN）データを含む。所与のメッセージバーストは、特定の時間で特定の衛星スポットビーム内に発生する可能性があるため、PRNおよび特有なビームパラメータ（例えば、時間、衛星識別（ID）、ビーム識別（ID）、時間バイアス、軌道データなど）を含むメッセージ・バースト・コンテンツを使用して、受信先の箇所を認証することができる。上記のイリジウムLEO衛星の1つを使用する場合、送信信号電力は、その信号が屋内環境に確実に侵入することを可能にするのに十分強く、信号符号化方法を使用して、それを行ってもよい。これにより、開示する方法を、多くの屋内用途に使用することを可能にする。

【0009】

少なくとも1つの実施形態において、本方法は、少なくとも1つの送信元によって、イベントアップデートを、少なくとも1人のユーザと関連付けられた少なくとも1つのネットワークノードに送信すること、および少なくとも1つのプロセッサによって、イベントアップデートを使用することにより、ユーザに対するベースライン挙動プロファイルをアップデートすることをさらに含む。1つまたは複数の実施形態において、少なくとも1人のユーザと関連付けられた少なくとも1つのノードの挙動のモニタリングは、少なくとも1人のユーザと関連付けられた少なくとも1つのノードの使用をモニタリングすること、少なくとも1人のユーザと関連付けられた少なくとも1つのノードの箇所をモニタリングすること、少なくとも1人のユーザと関連付けられた少なくとも1つのノードを通過するデータ（例えば、データおよびパケットヘッダを含むデータパケット）をモニタリングすること、少なくとも1人のユーザと関連付けられた少なくとも1つのノードを通るデータの量をモニタリングすること、少なくとも1人のユーザと関連付けられた少なくとも1つのノードを通るデ

ータの時間をモニタリングすること、少なくとも1人のユーザと関連付けられた少なくとも1つのノードを通るデータの日付をモニタリングすること、データを最初に送信した起点供給源をモニタリングすること、および／または送信されたデータの宛先をモニタリングすることを含む。

【0010】

少なくとも1つの実施形態において、本方法は、少なくとも1つの認証デバイスを用いて、少なくとも1人のユーザと関連付けられた少なくとも1つのノードの箇所を認証することをさらに含む。少なくとも1つの実施形態において、少なくとも1つの認証デバイスは、少なくとも1つの認証信号を評価することによって、少なくとも1人のユーザと関連付けられた少なくとも1つのノードの箇所を認証する。いくつかの実施形態において、少なくとも1つの認証信号は、少なくとも1つの送信元によって送信され、少なくとも1人のユーザと関連付けられた少なくとも1つのノードと関連付けられた少なくとも1つの受信先によって受信される。1つまたは複数の実施形態において、少なくとも1つの基準は、少なくとも1人のユーザと関連付けられた少なくとも1つのネットワークノードの箇所、少なくとも1人のユーザと関連付けられた少なくとも1つのネットワークノードを通るデータの種類、少なくとも1人のユーザと関連付けられた少なくとも1つのネットワークノードがデータを受信した時間、少なくとも1人のユーザと関連付けられた少なくとも1つのネットワークノードがデータを受信した日付、少なくとも1人のユーザと関連付けられた少なくとも1つのネットワークノードがデータを送信した時間、少なくとも1人のユーザと関連付けられた少なくとも1つのネットワークノードがデータを送信した日付、データが最初に送信された起点供給源の位置、および／またはデータが送信される最終的な宛先の箇所に関する。

【0011】

1つまたは複数の実施形態において、脅威検出に対するコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのためのシステムを開示する。本システムは、ユーザに対する挙動プロファイルを生成するために、ネットワーク内の少なくとも1人のユーザと関連付けられた少なくとも1つのノードの挙動をモニタリングし、少なくとも1人のユーザに対する挙動プロファイルを、ユーザに対するベースライン挙動プロファイルと比較し、少なくとも1人のユーザに対する挙動プロファイルと、ユーザに対するベースライン挙動プロファイルとの間にいつ差異が生じたかを判断し、差異が、ベースライン閾値レベルを超える場合、ベースライン閾値レベルを超えない場合、少なくとも1つの基準を満たす場合、および／または少なくとも1つの基準を満たさない場合に、差異と関連付けられたイベントにフラグを立て、イベントをイベント種別に分類するための少なくとも1つのプロセッサを備える。本システムは、少なくとも1人のユーザと関連付けられた少なくとも1つのノードと関連付けられた少なくとも1つの送信器をさらに備え、イベントを、ネットワーク内の少なくとも1つの他のノードおよび／またはネットワーク・オペレーション・センターに送信する。

【0012】

少なくとも1つの実施形態において、プロセッサはまた、そのユーザに対するベースライン挙動プロファイルを生成するために、ネットワーク内の、少なくとも1人のユーザと関連付けられた、少なくとも1つのノードの挙動を先ずモニタリングする。いくつかの実施形態において、本システムは、少なくとも1人のユーザに対するベースライン挙動プロファイルを、ユーザと関連付けられた少なくとも1つのノードに送信するための少なくとも1つの送信元、および少なくとも1人のユーザと関連付けられた少なくとも1つのノードと関連付けられ、ユーザに対するベースライン挙動プロファイルを受信するための少なくとも1つの受信器をさらに備える。

【0013】

1つまたは複数の実施形態において、本システムは、少なくとも1つの送信元をさらに備え、イベントアップデートを、少なくとも1人のユーザと関連付けられた少なくとも1つのネットワークノードに送信し、少なくとも1つのプロセッサは、イベントアップデートを使用して、ユーザに対するベースライン挙動プロファイルを更新する。少なくとも1つの

実施形態において、本システムは、少なくとも1つの認証デバイスをさらに備え、少なくとも1人のユーザと関連付けられた少なくとも1つのノードの箇所を認証する。1つまたは複数の実施形態において、少なくとも1つの認証デバイスは、少なくとも1つの認証信号を評価することによって、少なくとも1人のユーザと関連付けられた少なくとも1つのノードの箇所を認証する。いくつかの実施形態において、少なくとも1つの認証信号は、少なくとも1つの送信元によって送信され、少なくとも1人のユーザと関連付けられた少なくとも1つのノードと関連付けられた少なくとも1つの受信先によって受信される。

【0014】

本開示の一実施形態によれば、スマート・エージェント・ダウンロードを送信する前に、ノードの位置認証をする（すなわち、ノードの箇所を認証する）ための位置特定ネットワークノードを含むシステムを開示する。

10

【0015】

本開示の一実施形態によれば、少なくとも1つのスマート・エージェント・ダウンロードを使用する、（特定のノード（例えば、ルータ、コンピューティングデバイス、スマートフォン、およびサーバなど）と関連付けられた）個別ユーザのプロファイルの動的開発を含む方法を開示する。

【0016】

本開示の一実施形態によれば、少なくとも1つのスマート・エージェント・ダウンロードを使用する、（特定のノード（例えば、ルータ、コンピューティングデバイス、スマートフォン、およびサーバなど）と関連付けられた）個別ユーザのプロファイルの動的開発を含む方法を開示し、本プロファイルは、ノードと関連付けられた特定のユーザに対してパーソナライズされる。

20

【0017】

本開示の一実施形態によれば、ノードユーザの名目的コンピューティング、ストレージ、および／または通信動作に基づいて、ノードに対して少なくとも1つのユーザプロファイルをパーソナライズすることを含む方法を開示する。

【0018】

本開示の一実施形態によれば、少なくとも1つのユーザ・ベースライン・プロファイルを、より良好な脅威検出のために使用することができる複数のベースラインに分割することを含む方法を開示する。少なくとも1つの実施形態において、ベースラインの少なくとも1つは、時間的なものである。少なくとも1つの実施形態において、ベースラインの少なくとも1つは、地理空間的なものである。

30

【0019】

本発明の一実施形態によれば、ルータなどのノードでスマートエージェントを使用する（すなわち、スマート・エージェント・ダウンロードであり、「スマートエージェント」をノード上にダウンロードすることである）、地理空間ベースのユーザプロファイルの動的開発を含む方法を開示する。

【0020】

本発明の一実施形態によれば、ルータなどのノードでスマートエージェントを使用する（すなわち、スマート・エージェント・ダウンロードであり、「スマートエージェント」をノード上にダウンロードすることである）、地理空間ベースのユーザプロファイルの動的開発を含み、さらにデータ・パケット・ヘッダ内に測位署名を含む対応IPネットワークパケット構造と共にそれらを使用する方法を開示する。

40

【0021】

本発明の一実施形態によれば、（ルータなどの）ノードでスマートエージェントを使用する、時間ベースのユーザプロファイルの動的開発を含む方法を開示する。

【0022】

本開示の一実施形態によれば、確立されたユーザベースライン（すなわち、ユーザ・ベースライン・プロファイル）およびユーザプロファイルを使用して、既存の通常の挙動制限内で動作しているネットワークの内部ユーザ（すなわち、ネットワークの正当なユーザ

50

）をモニタリングする。

【0023】

本開示の一実施形態によれば、確立されたユーザベースライン（すなわち、ユーザ・ベースライン・プロファイル）およびユーザプロファイルを使用して、既存の通常の挙動制限外で動作しているネットワークの内部ユーザ（すなわち、ネットワークの正当なユーザ）の警告／通知をモニタリングおよび送信する。いくつかの実施形態において、既存の通常の挙動制限を識別する閾値および／または基準は、ネットワーク管理要素および／またはポリシーサーバなどの発信ポイントによって定義してもよい。

【0024】

本開示の一実施形態によれば、確立されたユーザベースライン（すなわち、ユーザ・ベースライン・プロファイル）およびユーザプロファイルを使用して、ネットワーク内のハッカー（すなわち、ネットワークの不正ユーザ）を識別する。

10

【0025】

本開示の一実施形態によれば、確立されたユーザベースライン（すなわち、ユーザ・ベースライン・プロファイル）およびユーザプロファイルを使用して、ネットワーク内のハッカー（すなわち、ネットワークの不正ユーザ）をモニタリングする。

【0026】

本開示の一実施形態によれば、確立されたユーザベースライン（すなわち、ユーザ・ベースライン・プロファイル）およびユーザプロファイルを使用して、ネットワーク内のハッカーをハニーポットにリルートする。ハニーポットは、情報システムの不正使用による試みを、検出し、逸らし、または場合によっては、相殺するためのトラップセットである。一般に、コンピュータデータ、すなわち、ネットワークの一部であると思われるネットワークサイトからなるが、実際には、分離およびモニタリングされ、攻撃者に対する情報または値のリソースを含むと思われる。

20

【0027】

本開示の一実施形態によれば、確立されたユーザベースライン（すなわち、ユーザ・ベースライン・プロファイル）およびユーザプロファイルを使用して、アドバンスド・パーシスタント・スレット（APT）をモニタリングする。

【0028】

本開示の一実施形態によれば、確立されたユーザベースライン（すなわち、ユーザ・ベースライン・プロファイル）およびユーザプロファイルを使用して、ネットワークの内部の無法ユーザ（すなわち、適切に振る舞っていない、したがって、無法な振る舞いをしている、ネットワークの正当なユーザ）をモニタリングする。

30

【0029】

本開示の一実施形態によれば、上流ネットワークノードによって学習および発信される情報を使用して、下流ネットワークによる「クラスタ状／ブートストラップ状」システム（すなわち、外部からの補助無く続行される、自律しているシステム）ビューの動的開発を含む方法を開示する。

【0030】

本開示の一実施形態によれば、既知の位置認証されたノードおよびエンド・ツー・エンド・トラフィック・フロー（すなわち、供給源ノードから始まり、宛先ノードで終了するネットワークを通る経路データ移動）情報を使用して、ルータ、ならびに他の同様のデバイスに対するネットワーク構成の地理空間的および時間的ユーザコンテキスト／プロファイルを動的開発することを含む方法を開示する。

40

【0031】

本開示の一実施形態によれば、ノードで、埋込ノードで、およびシステム／ネットワークレベルで、異常なユーザ挙動の軽減のモニタリングおよび検出をサポートすることを含む方法を開示する。

【0032】

本開示の一実施形態によれば、セキュリティ・モニタリング・インフラストラクチャ・

50

システム（SMIS）ツールを使用するシステムを開示する。

【0033】

1つまたは複数の実施形態において、本開示は、スマート・エージェント・ダウンロードによって補助されるネットワークポロジのための方法、システム、および装置に関する。特に、本開示は、少なくとも1つの認証デバイスで、少なくとも1人の要求者を認証することを含む方法を教示する。本方法は、少なくとも1つの送信元により、スマート・エージェント・ダウンロードを、少なくとも1人の要求者と関連付けられた少なくとも1つの受信先に送信することをさらに含む。さらに、本方法は、少なくとも1つの受信先によって、スマート・エージェント・ダウンロードを受信することを含む。さらに、本方法は、少なくとも1つのプロセッサによって、スマート・エージェント・ダウンロードを実行することを含む。さらに、本方法は、スマート・エージェント・ダウンロードによって、ネットワーク挙動をモニタリングすることを含む。

10

【0034】

1つまたは複数の実施形態において、少なくとも1つの認証デバイスは、少なくとも1人の要求者を認証する。少なくとも1つの実施形態において、認証は、少なくとも1つの認証信号を評価することによって実行される。少なくとも1つの実施形態において、少なくとも1つの認証信号は、少なくとも1つの送信元によって送信され、少なくとも1つの受信先によって受信される。いくつかの実施形態において、少なくとも1つの認証信号およびスマート・エージェント・ダウンロードは、同じ送信元から送信される。1つまたは複数の実施形態において、少なくとも1つの認証信号およびスマート・エージェント・ダウンロードは、異なる送信元から送信される。少なくとも1つの実施形態において、少なくとも1つの認証信号およびスマート・エージェント・ダウンロードは、同じ周波数で送信される。いくつかの実施形態において、少なくとも1つの認証信号およびスマート・エージェント・ダウンロードは、異なる周波数で送信される。

20

【0035】

少なくとも1つの実施形態において、少なくとも1人の要求者は、構成要素および／またはユーザである。1つまたは複数の実施形態において、少なくとも1つの送信元は、少なくとも1つの衛星および／または少なくとも1つの疑似衛星で使用される。いくつかの実施形態において、少なくとも1つの衛星は、低軌道周回（LEO）衛星、中軌道周回（MEO）衛星、および／または静止地球軌道（GEO）衛星である。

30

【0036】

1つまたは複数の実施形態において、開示する方法は、イリジウムLEO衛星コンステレーションを使用し、そのコンステレーションにおける衛星のそれぞれは、48スポットビームを特有のスポット・ビーム・パターンで送信するアンテナ形状を有する。少なくとも1つの実施形態において、少なくとも1つの認証信号および／またはスマート・エージェント・ダウンロードは、コンステレーションにおけるイリジウム衛星の少なくとも1つから送信することができる。イリジウム衛星の48スポットビームを使用して、地球表面に設置されるか、または地球表面付近にある受信先に、局所的認証信号および／またはスマート・エージェント・ダウンロードを含む信号を送信することができる。これらの信号と関連付けられるブロードキャスト・メッセージ・バースト・コンテンツは、疑似ランダムノイズ（PRN）データを含む。所与のメッセージバーストは、特定の時間で特定の衛星スポットビーム内に発生する可能性があるため、PRNおよび特有なビームパラメータ（例えば、時間、衛星識別（ID）、ビーム識別（ID）、時間バイアス、軌道データなど）を含むメッセージ・バースト・コンテンツを使用して、受信先の箇所を認証することができる。上記のイリジウムLEO衛星の1つを使用する場合、送信信号電力は、その信号が屋内環境に確実に侵入することを可能にするのに十分強く、信号符号化方法を使用して、それを行ってもよい。これにより、開示する方法を、多くの屋内用途に使用することを可能にする。

40

【0037】

少なくとも1つの実施形態において、少なくとも1つの受信先は、携帯電話、携帯情報端末（PDA）、パーソナルコンピュータ、コンピュータノード、インターネットプロトコル

50

(IP) ノード、サーバ、ルータ、ゲートウェイ、Wi-Fiノード、ネットワークノード、パーソナル・エリア・ネットワーク (PAN) ノード、ローカル・エリア・ネットワーク (LAN) ノード、ワイド・エリア・ネットワーク (WAN) ノード、Bluetoothノード、ZigBeeノード、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス (WiMAX) ノード、第2世代 (2G) 無線ノード、第3世代 (3G) 無線ノード、および／または第4世代 (4G) 無線ノードで使用される。1つまたは複数の実施形態において、要求者は、静止および／または移動する。いくつかの実施形態において、開示する方法は、メモリ内にスマート・エージェント・ダウンロードを格納することをさらに含む。少なくとも1つの実施形態において、少なくとも1つのプロセッサおよび／またはメモリは、携帯電話、携帯情報端末 (PDA)、パーソナルコンピュータ、コンピュータノード、インターネット
10
プロトコル (IP) ノード、サーバ、ルータ、ゲートウェイ、Wi-Fiノード、ネットワークノード、パーソナル・エリア・ネットワーク (PAN) ノード、ローカル・エリア・ネットワーク (LAN) ノード、ワイド・エリア・ネットワーク (WAN) ノード、Bluetoothノード、ZigBeeノード、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス (WiMAX) ノード、第2世代 (2G) 無線ノード、第3世代 (3G) 無線ノード、および／または第4世代 (4G) 無線ノードで使用される。

【0038】

1つまたは複数の実施形態において、ネットワーク挙動をモニタリングすることは、少なくとも1人の要求者と関連付けられた少なくとも1つのデバイスの使用をモニタリングすることを含み、少なくとも1つのデバイスは、携帯電話、携帯情報端末 (PDA)、パーソナル
20
コンピュータ、コンピュータノード、インターネットプロトコル (IP) ノード、サーバ、ルータ、ゲートウェイ、Wi-Fiノード、ネットワークノード、パーソナル・エリア・ネットワーク (PAN) ノード、ローカル・エリア・ネットワーク (LAN) ノード、ワイド・エリア・ネットワーク (WAN) ノード、Bluetoothノード、ZigBeeノード、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス (WiMAX) ノード、第2世代 (2G) 無線ノード、第3世代 (3G) 無線ノード、および／または第4世代 (4G) 無線ノードであり、さらに、少なくとも1人の要求者と関連付けられる少なくとも1つのデバイスの位置をモニタリングすること、ネットワークを通るデータ (例えば、データおよびパケットヘッダを含むデータパケット) をモニタリングすること、および／またはネットワーク
30
を通るデータの量をモニタリングすることを含む。少なくとも1つの実施形態において、開示する方法は、少なくとも1つのプロセッサによって、ネットワーク挙動を評価すること、およびスマート・エージェント・ダウンロードによって、ネットワーク挙動に異常が発生したことをプロセッサが判断した場合に実行すべき特定のタスクを起動することをさらに含む。少なくとも1つの実施形態において、開示する方法は、少なくとも1人の要求者と関連付けられた送信デバイスによって、ネットワーク挙動を、ネットワーク・オペレーション・センターに送信することと、ネットワーク・オペレーション・センターでの少なくとも1つのプロセッサによって、ネットワーク挙動を評価することと、スマート・エ
40
ージェント・ダウンロードによって、ネットワーク挙動に異常が発生したことをネットワーク・オペレーション・センターでの少なくとも1つのプロセッサが判断した場合に実行すべき特定のタスクを起動することをさらに含む。

【0039】

1つまたは複数の実施形態において、スマート・エージェント・ダウンロードによって補助されるネットワークトポロジーのためのシステムは、少なくとも1つの認証デバイス、少なくとも1つの送信元、少なくとも1つの受信先、および少なくとも1つのプロセッサを含む。少なくとも1つの実施形態において、少なくとも1つの認証デバイスは、少なくとも1人の要求者を認証するために使用される。いくつかの実施形態において、少なくとも1つの送信元は、スマート・エージェント・ダウンロードを、少なくとも1人の要求者と関連
50
付けられた少なくとも1つの受信先に送信するために使用される。1つまたは複数の実施形態において、少なくとも1つの受信先は、スマート・エージェント・ダウンロードを受信するために使用される。1つまたは複数の実施形態において、少なくとも1つのプロセッ

サは、スマート・エージェント・ダウンロードを実行するために使用され、実行されると、スマート・エージェント・ダウンロードは、ネットワーク挙動をモニタリングするために使用される。

【0040】

少なくとも1つの実施形態において、開示するシステムは、スマート・エージェント・ダウンロードを格納するために使用されるメモリをさらに含む。いくつかの実施形態において、開示するシステムは、ネットワーク挙動インジケータをネットワーク・オペレーション・センターに送信するために使用される少なくとも1人の要求者と関連付けられた送信デバイスと、ネットワーク挙動を評価するために使用されるネットワーク・オペレーション・センターでの少なくとも1つのプロセッサとをさらに含む。これらの実施形態に対して、スマート・エージェント・ダウンロードは、ネットワーク挙動に異常が発生したとネットワーク・オペレーション・センターでの少なくとも1つのプロセッサが判断した場合に実行される特定のタスクを起動する。

10

【0041】

1つまたは複数の実施形態において、スマート・エージェント・ダウンロードによって補助されるネットワークトポロジーのための装置は、本装置と関連付けられた少なくとも1人の要求者を認証するために使用される少なくとも1つの認証デバイスを含む。本装置は、スマート・エージェント・ダウンロードを受信するために使用される少なくとも1つの受信先を含む。さらに、本装置は、スマート・エージェント・ダウンロードを格納するために使用されるメモリを含む。さらに、本装置は、スマート・エージェント・ダウンロードを実行するために使用される少なくとも1つのプロセッサを含み、実行されると、スマート・エージェント・ダウンロードは、ネットワーク挙動をモニタリングする。いくつかの実施形態において、本装置は、ネットワーク挙動を送信するために使用される送信元をさらに含む。

20

【0042】

形態、機能、および利点は、本発明のさまざまな実施形態において独立して実現することができ、またはさらに他の実施形態において、組み合わせてもよい。

【0043】

本開示のこれらおよび他の形態、態様、および利点は、以下の説明、添付の特許請求の範囲、および添付図面を参照することで、より良好に理解されるであろう。

30

【図面の簡単な説明】

【0044】

図1から図12は、本開示の少なくとも1つの実施形態による、驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムおよび方法に関する。

【0045】

【図1】本開示の少なくとも1つの実施形態による、驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムの概略図である。

【図2】本開示の少なくとも1つの実施形態による、驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示する方法のフロー図である。

40

【図3】本開示の少なくとも1つの実施形態による、驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムおよび方法によって使用することができるセキュリティ・モニタリング・インフラストラクチャ・システム（SMIS）の概略図である。

【図4】本開示の少なくとも1つの実施形態による、図3のSMISの機能のブロック図である。

【図5】本開示の少なくとも1つの実施形態による、スマート・エージェント・ダウンロード（すなわち、ソフトウェアアップデート）によって補助される、驚異検出のためのコ

50

ンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムの概略図である。

【図6】本開示の少なくとも1つの実施形態による、驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示する方法の大まかな概要のフロー図である。

【図7】本開示の少なくとも1つの実施形態による、システムが位置認証対応ルータを使用している、驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムのトポロジー図である。

【図8】本開示の少なくとも1つの実施形態による、システムがネットワーク・ポリシー・サーバ（NPS）を使用している、驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムの概略図である。

【図9】本開示の少なくとも1つの実施形態による、ユーザ／ノード挙動をモニタリングする形態を示す驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムの概略図である。

【図10】本開示の少なくとも1つの実施形態による、図3のSMISの機能の他のブロック図である。

【図11】本開示の少なくとも1つの実施形態による、少なくとも1つの検出された異常挙動の少なくとも1つのノードを再調整する形態を示す、図3のSMISの機能のブロック図である。

【図12】本開示の少なくとも1つの実施形態による、ネットワーク管理要素を介して少なくとも1つの検出された異常挙動の少なくとも1つのノードを再調整する形態を示す、図3のSMISの機能のブロック図である。

【図13】本開示の少なくとも1つの実施形態による、システムがSMISを使用しているスマート・エージェント・ダウンロードによって補助される、驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムの概略図である。

【0046】

図14から図18は、本開示の少なくとも1つの実施形態による、スマート・エージェント・ダウンロードによって補助されるネットワークトポロジーのための、開示するシステムおよび方法に関する。

【図14】本開示の少なくとも1つの実施形態による、スマート・エージェント・ダウンロードによって補助されるネットワークトポロジーのための、開示するシステムの概略図である。

【図15】本開示の少なくとも1つの実施形態による、スマート・エージェント・ダウンロードによって補助されるネットワークトポロジーのための、開示する方法のフロー図である。

【図16】本開示の少なくとも1つの実施形態による、ネットワーク挙動をモニタリングするネットワーク・オペレーション・センター（NOC）を示す概略図である。

【図17】本開示の少なくとも1つの実施形態による、ネットワーク挙動における異常の検出を示すグラフである。

【図18】本開示の少なくとも1つの実施形態による、論理トポロジーをネットワークの物理トポロジーと相関する、メッシュ状物理的フレームワークの一例を示す概略図である。

【0047】

図19から図22は、本開示の少なくとも1つの実施形態による、要求者のスポットビーム式認証のための、開示するシステムおよび方法に関する。

【図19】本開示の少なくとも1つの実施形態による、開示するスポットビーム式認証システムによって使用することができる、衛星ベース通信システムの概略図である。

【図20A】本開示の少なくとも1つの実施形態による、衛星ベース認証システムを示す概略図である。

【図 20 B】本開示の少なくとも1つの実施形態による、衛星ベース認証システムを示す概略図である。

【図 20 C】本開示の少なくとも1つの実施形態による、衛星ベース認証システムを示す概略図である。

【図 21 A】本開示の少なくとも1つの実施形態による、開示するスポットビーム式認証システムを実施するために適合させることができるコンピューティングデバイスの概略図である。

【図 21 B】本開示の少なくとも1つの実施形態による、開示するスポットビーム式認証システムによって使用することができる、衛星ベース通信システムの概略図である。

【図 22】本開示の少なくとも1つの実施形態による、要求者を認証するための、開示するスポットビーム式認証方法を示すフロー図である。

【発明を実施するための形態】

【0048】

以下の説明では、本システムのより完全な説明を提供するために、多くの詳細を記載する。しかしながら、開示するシステムは、これらの特定の詳細無しに実施することができるが、当業者には明らかであろう。他の例において、不必要にシステムを不明瞭にしないように、周知の形態は詳細には説明していない。

【0049】

I. 脅威検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリング

本明細書で開示する方法およびシステムは、動的な状況ノードプロファイルのための動作システムを提供する。具体的には、このシステムは、サイバーおよびネットワークセキュリティ脅威検出アプリケーションのための、コンテキスト・アウェア・セキュリティ・モニタリング・システムに関する。特に、本開示は、動的なユーザ挙動プロファイルを開発する、対応（例えば、スマートエージェント可能）ネットワークノード、またはネットワークチェーンにおける他の接合部を教示する。これらのユーザプロファイルからの逸脱は、ネットワーク全体の、異常挙動検出、モニタリング、および異常軽減アルゴリズムを向上するために使用することができる。ネットワークの一部の領域における新たな脅威について第1に検出および学習することによって、ネットワークの残りの部分が適切に利益を得て、応答し、ネットワークの他の部分でのサイバー脅威のさらにネガティブな影響を防ぐことができる。

【0050】

現在、サイバーセキュリティは、電子システムが日々のビジネスおよび社会的タスクにより浸透しているため、ますます重要となっている。多くの以前に管理されたビジネス処理は、オンラインで処理する電子データに拡張され、実行中の情報およびコンピューティングセキュリティ促進技術を、必要要件にし、これらの日々使用されるシステムを保護する。社会保障番号から国家のインフラ関連情報までの情報を使用する重要な文書および他のデータは、ネットワーク化されたシステムに格納され、不正な当事者によってアクセスされた場合、迷惑行為から壊滅的な社会インフラ破壊までのさまざまな程度の社会的影響がもたらされる。電子システムへの依存度の増加と平行して、国家にも、テロおよびコンピュータハッキングの劇的な増加が見られる。したがって、我々のネットワーク化されたコンピュータシステムを保護する方法を改善する作業が社会に必要となっている。

【0051】

サイバー攻撃およびネットワーク侵入は、あまりに一般的になっている。これらの頻繁な発生により、商用および軍用環境における外部からの脅威によってネットワークに侵入される危険性についての説明を先ず行う。現在のアクセス制御アプローチは、静的パスワードに主に基づくか、または公開鍵基盤（PKI）に基づくパスワードおよびスマートバッジ証明書の使用に基づく認証である。システム攻撃は、エンドユーザに扮することによって行われることが多いので、ネットワークデータ傍受ネットワーク脆弱性を低減するためのユーザ認証方法に組織が集中する傾向がある。これらのアプローチは、精巧な攻撃に対

10

20

30

40

50

して脆弱になりつつあり、したがって、ユーザ箇所などの地理空間箇所／コンテキストを加えることによって通常は3つの要素（知識情報、所持情報、生体情報）の認証を超える追加の要素／情報を活用するアクセス制御の新しいパラダイムに対する必要性が開発されており、保護の追加および直交層を提供し、統合化物理的測位マッピングから論理ネットワークおよび情報管理ビューへの箇所および状況認識間の相互関係の向上をもたらす。

【0052】

さらに、既存のサイバー攻撃が、多くの場合、匿名で行われているという事実が、さらなる関連問題を作り出している。比較的大規模な攻撃は、多くの場合、将来の開発のためにシステムの脆弱性をより良好に理解するために、小規模な侵入／攻撃を行う考案者の試みによって防がれており、後のより破壊的な攻撃に対する基盤を敷設する。これまでに、多くの大規模なサイバー攻撃は、攻撃を受けている者を、まだ残っているダメージから回復中のままにするだけでなく、攻撃を受けた者が、報復による何らかのさらなるダメージを阻止することを不可能にさせ、そうでなければ、攻撃の起点にいる者を明らかにすることを不可能にさせ、権威者による応答を不可能にさせることが多い。攻撃の動機が不明確である場合、攻撃の受け手は、攻撃が単なる荒らし行為、意図的な窃盗、または脅威にさらされる国家安全に対するより悪意のあるアプローチであったかどうかを知ることはまず無い。したがって、無法ユーザに対するネットワークアクセスを拒否するのを補助する、および／または起点にいる者を識別するのを補助するための追跡可能データを提供する何らかのシステムが、サービス拒否（DoS）およびネットワークデータ傍受攻撃の低減および軽減に大いに役に立つであろう。

【0053】

本開示は、ネットワーク管理に関し、特に、既存のシステム、方法、およびデバイスと共に、またはそれらに対する代替アプローチとして、使用することができる、異常動作モニタリング、検出、および軽減を改善する。そのような既存の方法は、侵入検出システム（IDS）およびアドバンスド・パーシスタント・スレット（APT）管理を含んでもよい。本開示のシステムおよび方法は、セキュリティ・モニタリング・インフラストラクチャ・システム（SMIS）と関連付けられる機能を活用し、サイバーセキュリティおよびネットワーク・モニタリング・データを集計し、以下でさらに詳細に説明する完全な状況認識図を提供する。

【0054】

既存のシステムは、署名およびポリシーアップデートの間の事実上静的な署名およびポリシーに依存し、さらに、特定のコンピューティングデバイスならびに／もしくはシステムの通信、およびストレージ使用ユーザプロファイルに対して調整されていない。異常挙動を識別するための組込み済みの署名およびポリシーにより、既知のサイバー脅威に対して、迅速なイベント相関およびそれらの軽減が可能となり、さらに、多数のすでに分類された、既知のサイバー脅威に対して良好な防御になる。しかしながら、それらは、動的および時間的に新しい、および発展しているサイバー脅威には対応せず、一部のAPT脅威は、既知のパターンが欠落しており、長期にわたって履歴メモリを互いに関連付ける必要があり、それにより、これらの方法は、これらの問題の低減または全面的な軽減により改善され得る。

【0055】

本開示は、一般に、脅威検出によるネットワーク管理およびセキュリティに関する。特に、サイバーおよびネットワークセキュリティ脅威検出アプリケーションのためのコンテキスト・アウェア・セキュリティ・モニタリング・システムのための特定のノードと関連付けられた動的な状況ユーザプロファイルに関し、以下でより詳細に説明する、セキュリティ・モニタリング・インフラストラクチャ・システム（SMIS）ツールと別々に、または共に使用することができる。

【0056】

動的な状況プロファイルを開発して、サイバーおよびネットワークセキュリティ用途に対して、異常挙動モニタリング、検出、および軽減の調整を可能にする方法およびシステ

ムを、本明細書で開示する。1つまたは複数の実施形態において、開示する方法は、少なくとも1つの認証デバイスにより、少なくとも1人のユーザと関連付けられた少なくとも1つのノードを認証することと、少なくとも1つの送信元によって、ノードと関連付けられた少なくとも1つの受信先に、スマート・エージェント・ダウンロードを送信することと、受信先と関連付けられたメモリに、スマート・エージェント・ダウンロードを格納することと、メモリと関連付けられた少なくとも1つのプロセッサによって、スマート・エージェント・ダウンロードを実行することと、スマート・エージェント・ダウンロードによって、ユーザ挙動をベースライン化する（すなわち、ノードでのユーザ挙動をモニタリングして、ベースラインプロファイルを作成する）ことと、スマート・エージェント・ダウンロードによって、ノードでのユーザの挙動をモニタリングすることと、スマート・エージェント・ダウンロードによって、ノードに対するユーザのベースライン（すなわち、ユーザ・ベースライン・プロファイル）からユーザの挙動の逸脱を検出することと、スマート・エージェント・ダウンロードによって、逸脱が、以下の少なくとも1つである場合に、すなわち、許容可能な閾値と適合する、許容可能な閾値と適合しない、許容可能な基準と適合する、許容可能な基準と適合しない、および／またはそれらの組み合わせの少なくとも1つである場合に、イベントに適切にフラグを立てることを含む。

10

【0057】

本開示は、動的な脅威モニタリングおよび検出によりネットワーク管理およびセキュリティを改善するためのさまざまな実施形態による方法およびシステムに関する。すなわち、本開示は、特定のノードに対する動的な状況ユーザプロファイルを生成して、サイバーおよびネットワークセキュリティ脅威検出アプリケーションに対して、異常挙動モニタリング、検出、および軽減の調整を可能にする方法を教示する。

20

【0058】

1つまたは複数の実施形態において、本開示は、スマートエージェントを使用して、必要に応じて、対応ネットワークノードにスマート・エージェント・ソフトウェアをダウンロードし、開示するシステムおよび方法が、技術進歩をサポートし、発展するセキュリティ脅威に関する情報を発信することを可能にすることができる。（スマート・エージェント・ダウンロードの詳細な説明のために、本開示のスマート・エージェント・ダウンロード・セクションによって補助されるネットワークトポロジーに関する）。

【0059】

いくつかの実施形態において、本開示は、スマートエージェントを使用して、特定のノードに対する動的なコンテキスト・アウェア・ユーザ・プロファイルを開発し、個々のデバイスレベルで、異常挙動モニタリング、検出、および軽減の調整を可能にする。これらのプロファイルは、複数のノードまたはネットワークレベルにわたって抽出された情報を再調査するよう編集してもよい。対応デバイス内の対応埋込型デバイスおよびユーザプロファイル（すなわち、ユーザと関連付けられたノードに対するベースラインプロファイル）の動作プロファイルは、スマート・エージェント・ダウンロードを使用してベースライン化され（すなわち、ベースラインプロファイルを生成するためにモニタリングされ）、コンピューティング、ストレージ、および／または通信動作の点から開発される。プロファイルは、状況に応じてさらに開発され、ユーザプロファイルは、特定の埋込デバイスおよび／またはユーザが操作している特定のデバイスに関して開発され、プロファイルはまた、デバイスが動作しているべき箇所を基準としてもよい。少なくともいくつかの実施形態において、プロファイルは、エンドユーザおよびプロファイルの使用特性に基づいてパーソナライズされる。いくつかの実施形態において、1つのベースラインプロファイルは、より良好に脅威を検出するために使用することができる複数のベースラインに分割してもよい。少なくとも1つの実施形態において、これらのベースラインの少なくとも1つは、時間的なものである。少なくとも1つの実施形態において、これらのベースラインの少なくとも1つは、地理空間的なものである。次いで、本開示のシステムおよび方法は、学習した異常挙動パターンを、システム内の他のノードに発信することを可能にすることができ、これらのノードが、より良好に脅威を軽減するために使用することができ、自身の検

30

40

50

出アルゴリズムを立ち上げることを含む。

【0060】

さらに、本開示のシステムおよび方法は、同様に、ネットワーク・トラフィック・フローの地理空間的および／または時間的コンテキスト・アウェア・プロファイルを動的に開発するために使用することができ、さらに、システム内の対応ノードの構成管理のために使用することができる。

【0061】

1つまたは複数の実施形態において、開示するシステムは、屋内環境などの減衰環境に位置する対応デバイス（すなわち、対応ノード）に、スマート・エージェント・ソフトウェアをダウンロードすることができる。開示するシステムは、さらに、さまざまな異なる位置特定方法に加えて、典型的なインターネットプロトコル（IP）フレームワークに対するデバイスを物理的にマッピングするよう使用することができる。これにより、物理的箇所の点から、特定のデバイスが、どこから所与のネットワークにアクセスしているかの識別が可能となり、それにより、ネットワーク内の状況認識に適しており、さらに、ネットワークの構成の動的な理解をもたらすことを補助するのに適している。

【0062】

測位のための好ましい方法は、低軌道周回（LEO）衛星（すなわち、イリジウム衛星）からの信号を使用して、それらの箇所に基つきネットワークノードを認証するための手段（「位置認証」と称する）をネットワークノードに提供し、およびネットワークノードがスマート・エージェント・ソフトウェアを受信するための手段を提供する。ノードの位置認証は、意図していないユーザがソフトウェアダウンロードを受信しないことを確実にするために、アーキテクチャにとって重要である。いくつかの実施形態において、ソフトウェアは、配置前に、または地上のネットワークを介して、対応デバイス上に事前ロードされ、ソフトウェアアップロードだけがLEO衛星を通じて送信され、信号要請を最小にすることが好ましいであろう。その場合、スマート・エージェント・ソフトウェアを使用して、ノード挙動のモニタリングを補助し、異常なネットワーク動作を識別することができる。

【0063】

本開示のシステムおよび方法は、本質的にポートスニファの役目を果たす、セキュリティ・モニタリング・インフラストラクチャ・システム（SMIS）ツール・スイートを活用し、コンピューティング通信に及ぶことができる、認証された箇所および時間的関連名目的動作プロファイルと、時間的な属性に加えて認証された地理空間的箇所を含むデバイスコンテキスト認識を生じるストレージ使用プロファイルとの間の相関関係を向上させるための位置認証能力を向上することができる。コンピューティング、通信、およびストレージ機能を含む、時間的および認証された地理空間的箇所の両方にわたる、全デバイス挙動に対する名目的ベースライン動作プロファイルを動的に確立およびアップデートすることによって、特有な、統計的に重要な状況を、動作中の特定のデバイスに特有であるとして確立することができる。これは、動作中のデバイスのフィンガープリンティングに類似し、一方、突然変異に関する動作プロファイルへのアップデートの追跡は、統計的有意性で一度判断され、自動化された、またはネットワークマネージャー駆動された、決定サポートシステムに基づき、承認挙動または異常挙動のいずれかに分類することができる。

【0064】

少なくとも1つの実施形態において、ネットワークは、セキュリティ・モニタリング・システム（SMS）として本明細書で一括して既知の、SMISのフォレンジック・データ・コレクタ（FDC）およびセキュリティ・ユーティリティ・サーバ（SUS）要素の同等物を含んでもよい。SMISツールのアプリケーション内で、FDCは、モニタリングを必要とする、ノード付近に設置されたネットワークセンサの役目を果たし、商用オフ・ザ・シェルフ（COTS）侵入検出システム（IDS）と同様である。FDCは、起動したイベントに基づいてデータを収集することによってシステムを補助することができる。そのような収集されたデータは、ネットワーク内の特定のノードを通して経路づけられているIPヘッダまたはIPパケッ

10

20

30

40

50

ト全体を含んでもよい。セキュリティ・ユーティリティ・サーバ（SUS）により、ネットワーク管理要素は、閾値および／または他の基準を設定し、起動された場合、ネットワーク管理システム（NMS）に通知を送信するなどの、特定の動作をもたらす警告を開発することを可能にする。本開示内では、そのような例示は、インフラベースではなく、むしろ、アルゴリズムベースであり、単一要素としてFDCおよびSUSを含む、SMSと呼ばれる、ローカル・デバイス・レベルで異常挙動を主としてモニタリングする、検出する、および軽減する、全体的なSMISの機能を同一場所に配置するという点で、既存のSMIS表示（米国特許第7,903,566号で開示される）とは異なることに留意されたい。これは、デバイス上にダウンロードされるSMSソフトウェア、および／または必要に応じて必要なアップデートまたは警告を受信することができるデバイス上のソフトウェアの少なくとも一部のための手段を教示するスマート・エージェント・ダウンロード・アプリケーションによって可能になる。

10

【0065】

さらに、ノード（例えば、デバイス、ルータ、および埋込システム）内のSMSソフトウェア動作は、各対応ノードで維持することができるように分散され、したがって、無線ノマディックコンピューティングおよびルータならびに埋込システムなどの自己管理型インターネットデバイスの両方により適用可能である。

【0066】

SMSアルゴリズムは、ノードのコンピューティング、通信、およびストレージ使用挙動を含む名目的ベースラインプロファイルを開発し、それにより、ノードの完全なコンテキストを提供する。これは、異常挙動の指示が、通信活動に限定されず、コンピューティングおよびストレージ活動も含むので、重要である。SMS機能は、各エンド・ユーザ・デバイス、ルータ、および埋込システムに統合され、それにより、前記した位置認証および許可方法の機能を向上し、認証／許可処理の間の動作段階中の、さらなるサイバー脅威モニタリング、検出、および軽減能力をも提供する。さらに、開示するSMS機能は、特に、カスタマイズされた標的エンドユーザプロファイルおよび動作コンテキストを提供することによって、携帯電話および無線個人デバイスなどの、モバイル・エンド・ユーザ・デバイスの利用の、広く普及する、急速な拡大に対してとても役に立ち、それにより、動的な、発展するサイバー脅威の識別、通知、および軽減に対するIDS/APT管理を可能にする。

20

【0067】

本開示は、いくつかの重要な形態を有する。重要な形態の1つは、本開示が、SMSの原理を適用することによって前述の位置認証システムに機能拡張をもたらし、署名またはポリシーを静的にまたは周期的にリフレッシュする必要無く、特定のデバイス、ルータ、および埋込システムのコンピューティング、通信、およびストレージ使用プロファイルに対するコンテキストを動的に開発することである。他の重要な形態は、本開示が、アルゴリズムベースの、動的に生成された、名目的動作に対するコンテキストプロファイルを提供し、次いで、サイバー脅威のために起こる異常挙動の検出および管理のための基礎を形成することである。さらに、別の重要な形態は、本開示が、アルゴリズム駆動SMS機能拡張を前述の位置認証システム認証および許可方法にもたらし、標的の地理空間的および時間的コンピューティング、通信、およびストレージ使用プロファイルを含み、さらに、使用毎の確立された、および学習した名目的ベースラインをモニタリングして、異常挙動を検出、通知、および軽減することである。さらに、別の重要な形態は、本開示が動的な状況認識のために、ピアおよび隣接する協働位置認識対応デバイス、ルータ、および埋込システムで検出された異常挙動状態の交換を可能にするためのツールを提供し、積極的防止対策の呼び出しにより、サイバー脅威の集約的隔離および軽減を可能にすることである。

30

40

【0068】

A. ノードプロファイル:特定のユーザ、特定のノード

ノードプロファイルは、スマート・エージェント・ダウンロードを使用することによってベースライン化され（すなわち、ベースラインプロファイルが生成され）、特定のネットワークノードに対して調整される。一実施形態において、プロファイルは、エンドユー

50

ザノードに対して開発され、特定のユーザによって行われるコンピューティング、ストレージ、および／または通信動作の点から開発される。さらに、プロファイルは、状況により開発される。これは、少なくとも1つの、これらに限定されない、以下の、時間的、および地理空間的コンテキストに基づいて開発されるプロファイルを含むことができる。言い換えると、ユーザプロファイル（すなわち、ユーザと関連付けられたノードに対するプロファイル）は、ユーザが操作しているデバイスに関して開発され、さらに、デバイスが操作されるべき地理的領域、およびユーザが、通常、ある時間にわたってデバイスを操作する方法に関してもよい。例えば、あるユーザが、会社で、職務を行うのに使用する複数のエンド・ユーザ・デバイスにアクセスすることができる。これらは、携帯情報端末（PDA）、ラップトップコンピュータ、デスクトップコンピュータ、および代替デバイスなど

10

を含むことができる。デスクトップコンピュータの箇所は、常に、そのユーザに対して同じままとすることができ、一方、ラップトップは、ユーザの家、事務所、および研究所箇所などの、複数の異なる箇所で使用される可能性があり、したがって、代替デバイスは、より特異な箇所で使用される可能性がある。閾値および／または基準は、これらの状況、および、例えば、特定のユーザデバイスが、以前に定義された許容地理的領域内でのみ動作することができる場所およびデバイスがこの定義された閾値の外に位置する場合のそれぞれに対して開発することができ、アルゴリズムは、異常なイベントを認識し、フラグを立てる。

【0069】

さらに、ユーザプロファイルは、アプリケーションレベルで構築され、アプリケーション使用、インターネットウェブサイト使用、およびコンピューティング、ストレージ、ならびに／もしくは通信アプリケーションに基づく他のノード使用を考慮する。例えば、セッションプロファイルは、ユーザが、自信のemailまたはFacebookもしくはGoogle+などの他のアプリケーションにどのようにアクセスするかなどの、アプリケーションがどのように使用されたかに基づいてモニタリングしてもよい。

20

【0070】

ユーザのプロファイルにおける劇的な変化は、すぐに、イベントとしてフラグが立てられる。イベントは、良いか悪いかの評価および分類をすることができ、それに続く応答動作は、それに応じて、イベントに対して識別することができる。少なくとも1つの実施形態において、そのような結果は、融合センター（および／または発信ポイント）にもたらし

30

てもよく、時間的および地理的に分析することができる。このようにして、本システムは、他のデバイスの立ち上げを助けることができ、その結果、驚異に対してより迅速に検出および応答することができる。所与のシナリオに応じて、さまざまな動作が、特定のイベントに対して起こり得る。例えば、動作の一部には、これらに限定されないが、以下が含まれる可能性がある。すなわち、イベントをログに記録することができ、そのイベントに関連するデータをログに記録することができ、ノードをシャットダウンすることができ、ノードを隔離することができ、何らかの学習済み挙動を、将来のイベントを軽減するために他のノードに発信することができ、そのイベントと関連付けられたユーザを、ハニーポットに逸らすことができ、および／または、そのイベントと関連付けられたユーザのアクセス権を無効にすることができる。

40

【0071】

データおよび／または利用可能なシステム関数へのアクセス可能性は、パーソナライズされたノードプロファイルの要素に基づいて、さらに定義しても良い。例えば、旅行中のユーザは、望まないイベントが発生することをさらに軽減するために、潜在的に安全ではないエリアにいることに基づいて、データへのアクセスまたは能力を限定してもよい。しかしながら、より重要なことに、パーソナライズされたノードプロファイルは、一人当たりのプロファイルに基づく。複数のユーザを有する可能性がある既存のシステムは、異なるユーザが、異なるスタイルで同じ機械を使用することを認識しない。同じ機械は、ユーザ（ユーザ1）が、他のユーザ（ユーザ2）に属するアカウントにログオンした場合を認識せず、したがって、システムは、これがユーザ1にとって正しい挙動ではなかったと認識

50

しない。

【0072】

開発されるノードプロファイルは、ノードの種類に依存する。少なくとも1つの実施形態において、ノードプロファイルは、特定のユーザが特定のノードをどのように使用したかに基づくことができる。例えば、ノードプロファイルは、特定のノードに対して、ユーザが、以下のデバイス、すなわち、PDA、ラップトップ、デスクトップ、コンピュータ、代替デバイス、および／またはナビゲーションデバイスの内1つを使用する可能性があることを認識する。

【0073】

いくつかの実施形態において、エンドユーザ対応ネットワークデバイスに対する挙動プロファイルは、ユーザのコンピューティング、通信、および／またはストレージ使用に基づき開発することができる。少なくとも1つの実施形態において、ユーザプロファイルは、スマート・エージェント・ダウンロードを使用して開発される。プロファイルベースラインは、コンピューティング、ストレージ、および／または通信の点から開発してもよい。いくつかの実施形態において、プロファイルは、ユーザが操作しているデバイスおよびデバイスと関連付けられたアプリケーションの使用に関して、どこでユーザプロファイルが開発されたかなどの状況に基づいてさらに開発することができる。いくつかの実施形態において、プロファイルはまた、デバイスが操作されるべき箇所を基準としてもよい。より一般的には、ノードプロファイルは、一般に、以下に基づくことができるが、これらのみに限定されない。すなわち、(1) 誰がその動作を実行しているか？(ユーザ固有—すなわち、静的パスワード、バイオメトリクスなど)、(2) どのデバイスがその動作を実行しているか？(デバイス依存—すなわち、PDA、ラップトップ、デスクトップ、代替デバイス、ナビゲーションデバイスなど)、(3) どの種類の動作を実行しているか(および／または実行していないか)？(すなわち、コンピューティング／通信／ストレージ関連タスク／アプリケーション使用)、(4) いつその動作を実行しているか？(日毎のパターンなどの時間的パターン)、(5) どのようにその動作を実行しているか？(場合によっては、ここに挙げたいくつかのプロファイル要因の組み合わせ)、(6) どこからその動作を実行しているか？(地理空間的／測位／位置認証)である。

【0074】

例えば、ユーザAは、自身の仕事に関連したラップトップコンピュータ(ノード1)で仕事をしており、そのノード1を、自身の会社、研究所、および／または自宅からアクセス可能に使用する。プロファイルは、(ユーザAがノード1でどのアプリケーションを使用するか、ユーザAがノード1でどのウェブサイトを訪れたか、およびユーザAが各アプリケーションをどのように使用したか、などの情報を含むことができる) ベースラインプロファイルを動的に開発するノード1でユーザAに対してベースライン化され、コンピューティング、ストレージ、および／または通信の点からノード1の使用と関連付けられたユーザの指紋を本質的に構築することができる。ユーザAは、そのようにプロファイル内に割り当てることができるアクセス可能な箇所(会社、研究所、および自宅)のそれぞれで異なるアプリケーションを使用する可能性がある。

【0075】

他の例において、デスクトップコンピュータの箇所は、全時間において同じままとすることができる。他の例において、ラップトップは、複数の箇所(自宅、会社、研究所など)でを使用することができ、代替ラップトップは、同じユーザによる場合でさえも、より特異な箇所で使用する可能性がある。プロファイルは、アプリケーションおよびインターネットウェブサイト使用などについても考慮することができる。

【0076】

少なくとも1つの実施形態において、ユーザは、デバイスにアクセスすることが可能になる前に、アクセス可能な地理的箇所に設置されたことを証明する必要がある、コンピューティング、通信、および／またはストレージ動作を実行することができる。ユーザおよび／またはデバイスは、例えば、本開示のスポットビームベースの認証セクションで説

10

20

30

40

50

明するような測位／位置認証方法によって認証してもよい。

【0077】

B. ノードプロファイル：トラフィック・フロー特性

他の実施形態において、ノードプロファイルは、インターネットプロトコル（IP）ネットワークを通るトラフィックに基づくことができる。例えば、ノードは、ネットワークにわたって複数のIPデータパケットを通すネットワークルータとすることができる。一実施形態において、ルータノードは、そこを通過して経路づけられるトラフィック（すなわち、IPデータパケット）を有する。トラフィックは、地理空間的および／または時間的に特徴づけることができる。ベースラインモデル（すなわち、ノードに対するベースラインプロファイル）を、上記したエンドユーザノードプロファイルのものと同様に開発することができ、トラフィックをベースラインに対してモニタリングすることができる。

10

【0078】

一実施形態において、少なくとも2つの通信可能に結合されたノード（例えば、対応携帯電話）のシステムは、ネットワークにわたってインターネットプロトコル（IP）を介して通信するよう構成される。ベースラインモデルは、ある期間にわたってIPツーIPパケットトラフィックを観測することによって、および閾値ならびに／もしくは潜在的なサイバー脅威もしくは他の異常挙動をフラグ立てするようモニタリングすることができる他の基準を開発することによって、少なくとも2つの結合されたノードに対する名目的IPネットワークトラフィックに対して開発することができる。いくつかの実施形態において、複数のIPツーIPパケットと関連付けられる可能性がある特有なIPパケットヘッダの少なくとも1つのインスタンスは、異常挙動に対して解析される可能性がある。いくつかの実施形態において、IPパケットヘッダは、セキュリティ署名部を備えてもよい。少なくとも1つの実施形態において、セキュリティ署名部は、IPパケットが通過するか、または経路づけられる少なくとも1つのネットワークノードに対する測位情報を含むことができる。少なくとも1つの実施形態において、測位情報は、少なくとも1つの位置情報タグまたは地理証明書の形式である。他の、または補足的な実施形態において、イベントは、以下の少なくとも1つによって識別することができる。すなわち、自身における動作の特有性、週のある時間の特有性、日のある時間の特有性、週のある日の特有性、データ量の特有性、測位情報の特有性の少なくとも1つによって識別することができる。上記のように、イベントはフラグを立てることができ、その場合、検出された異常挙動に対応する警告をもたらすなどの、さまざまな動作が生じる可能性がある。例えば、警告は、ネットワーク・ポリシー・サーバなどの、発信ポイントから送信してもよい。少なくとも1つの実施形態において、この警告は、ネットワーク管理システムに送信される。他の実施形態において、この警告は、隣接するデバイス、ピア、またはそれ以外に送信してもよい。

20

30

【0079】

いくつかの実施形態において、モニタリングされているデータは、可能デバイスのメモリにログとして記録される。別の態様において、システムは、メモリにログとして記録されるパケットヘッダを解析するよう割り当てられる少なくとも1つのプロセッサを含む。少なくとも1つの実施形態において、これらの機能は、同じデバイスによって行われる。他の実施形態において、これらの機能は、有線または無線によって互いに結合される異なるデバイス内に維持される。

40

【0080】

いくつかの実施形態において、パケットヘッダの分析は、IPツーIPオンボート動作タブルに基づく、履歴および統計的に関連する期間にわたってIPネットワークで特定の動作が実行されたかの判断、履歴および統計的に関連する期間にわたって、週の特定の時間の間にIPネットワークで特定の動作が実行されたかの判断、および／または履歴ならびに統計的に関連する期間にわたって週の所与の時間において、統計的に異なる量の帯域幅を、IPネットワークで実行された特定の動作が使用したかの判断に基づく。

【0081】

開示するシステムおよび方法のさらなる能力は、これらに限定されないが、ネットワー

50

ク・トラフィック・フローおよび署名型IDS/APT管理の必要無く調整された異常挙動モニタリング、検出ならびに軽減をルータが可能にするための構成管理の地理空間的および時間的コンテキスト／プロファイルの動的開発、ピア／隣接衛星箇所／測位システムへの観測されたアルゴリズム的に学習済みの異常挙動パターンの発信により、潜在的サイバー脅威の協働モニタリングおよび軽減を開始することを可能にすること、および管理環境における他のデバイス／ルータ／埋込システムにわたって、イベント相関エンジンに対する先取り状況認識として、所与のデバイス／ルータ／埋込デバイス内の異常挙動パターン、もしくはそれらのクラスタの判断により、動的異常挙動検出アルゴリズムを立ち上げることを可能にすることを含む。

【0082】

C. ノードプロファイル:構成管理

少なくとも1つの実施形態において、複数の位置認証対応ルータは、それらを通るよう経路づけられたIPデータ・パケット・トラフィックを有する。これらは、位置認証対応ルータと協働しているので、ルータの箇所は既知である。さらに、データパケットがネットワークを通過するのにかかるトラフィック・フロー（エンド・ツー・エンド、すなわち、供給源ノードから宛先ノード）時間、およびIPパケットが通るパスもまた既知である。この情報により、ルータのシステムの構成管理は既知である。

【0083】

典型的なシステムにおいて、データパケットは検査され、既知のウィルスおよびマルウェアの定義が、検査済みパケットに対して再調査される。しかしながら、このことが既知の脅威に対して良好に作用する間、未知の脅威に対する定義は判別されず、これらの場合に対して、開示するシステムおよび方法は有用である。

【0084】

未知の脅威を発見する部分は、アドバンスド・パーシスタント・スレット（APT）に対するネットワークのモニタリングを含むことができる。これらは、それらの低く遅いアプローチによりそれらがノイズの一部になることを可能にすることが多いので、突き止めるのが困難であることが多く、したがって、検出されない。このシステムおよび方法は、新規のトラフィック・フローを識別するよう作動することができ、あるイベントが良好であるとして分類すべきかを識別するよう使用することができ、ベースラインを再調整するために使用することができ、またはそのイベントが不良であるとして分類すべきかを識別するよう使用することができ、次いで、適切な動作（例えば、イベントにフラグを立てるおよび／または警告を送信する）を行うことができる。例えば、システムは、比較的短時間にシステムに到達するデータパケットの新規のトラフィック・フローを識別するための手段を有することができるが、週に2つのピング（例えば、2つのデータパケット）を認識することができない可能性がある。本システムは、所定の閾値未満であるので、これを捕らえない可能性があるが、実際に、ネットワーク内で発生する、後の、より破壊的なイベントに関わっている可能性がある。開示するシステムおよび方法は、これらの種類の典型的に検出不可能な異常挙動を識別するよう作動する。

【0085】

APTは、すべてのネットワークファブリックにわたって適用され、侵入検知は、ネットワークの境界でなおさら適用される。これの一例には、境界での流入でデータパケットを再調査し、および電子メールから、zipファイルなどの怪しい添付ファイルを取り除く、企業電子メールシステムを挙げることができる。ネットワークの境界は、ネットワークの境界に設置されるエンド・ユーザ・デバイスおよび／またはルータを含むことができる。これらの境界でネットワークトラフィックをモニタリングすることは、その境界が新規の脅威に最初に出くわすことが多いので、重要である。この場合も、名目的ベースラインを確立することによって、開示するシステムおよび方法を使用して、アルゴリズム的に学習することができ、したがって、挙動において逸脱が承認された場合にベースラインを再調整することができ、および／または識別された驚異に適切に対応することができる。

【0086】

D. 異常挙動および状況認識の発信

いくつかの実施形態において、例えば、ネットワーク内のノードは、異常検出機構で異常を検出する。ノードがノードのネットワークの一部であり、ピアノード、または相互通信する比較的近傍の他のノードを有する場合、他のノードもまた影響を受ける可能性がある。と仮定することができるこのようにして、前方ノードは、学習して、観測した異常挙動を後続ノードに発信することができる。少なくとも1つの実施形態において、融合センターは、ピアノードとすることができる、少なくとも2つのノードから情報を得て、ピアノードが、もはや自身でそのイベントを分類することができないように攻撃が発生したかどうかを評価する際に補助することができ、他のノードがその分類を補助することができる。同様のパターンが、2つ以上のノードにわたって認識された場合、帰属信頼性が高まり、それにより、脅威に対してより良好に応答することが可能になる。少なくとも1つの実施形態において、発信ポイントを使用して、異常挙動または異常挙動パターンについての情報を発信し、まだ攻撃されていないノードへの影響を軽減する。少なくとも1つの実施形態において、発信ポイントは、ネットワーク・ポリシー・サーバの形式を取り、これらの新規の攻撃に基づいて新規のポリシーを開発し、そのポリシーを、ネットワーク内のノードの少なくとも一部に発信する。この手段により、ネットワークは、教師あり、強化機械学習機構を有することができる。

【0087】

異常挙動を学習するには時間がかかるが、後に、ネットワーク内の他のノードがこの情報を使用して、これらの動的な異常挙動検出アルゴリズムを立ち上げて、その挙動自体を学習することができる。少なくとも1つの実施形態において、APTは、ネットワークの脆弱性を発見しようとする際に、境界ノードをテストしようとしてもよい。本システムは、異常挙動パターンを学習することができ、後に、複雑な規則を開発することができる。例えば、特定のパターン（例えば、週に2つのピング）を見る必要があるとシステムが判断した場合、本システムは、挙動パターンを観測した場合に、特定のトリガが生じるよう、この挙動パターンへの応答を開発することができる。この情報（すなわち、観測された特定の挙動パターンに対する応答）は、次いで、ネットワーク内の他のノードに発信することができる。このようにして、下流ノードは、挙動パターンを単に検出し、後に、それに対して応答する代わりに、攻撃を防ぐことができる。しかしながら、いずれの例でも、本システムは、学習済みの異常挙動パターンを認識しているので、自身を保護することができる。

【0088】

本開示は、ノード挙動モニタリングセンサの役目を果たすなどの、さまざまな方法でネットワークをサポートするために使用することができる、ソフトウェアを屋内環境にあるネットワークノードに堅実にダウンロードするための機能を備える対応技術を介して、セキュリティ・モニタリング・インフラストラクチャ・システム（SMIS）ツールに機能拡張を提供する。スマート・エージェント・ダウンロードにより、ネットワークノードが、自身の箇所を判断することができるようになることを可能にし、それにより、さらなる地理空間コンテキストを提供し、さらに、必要に応じて、ノードが位置認証することを可能にする。

【0089】

本開示は、5つの主な形態を有する。第1の形態は、コンテキスト・アウェア・パーソナライズド・プロファイルに関する。この形態は、コンピューティング、通信、およびストレージ使用に基づくユーザ／埋込デバイスに対するコンテキスト・アウェア・パーソナライズド・プロファイルの動的な開発を含み、署名式侵入検出システム（IDS）／アドバンスト・パーシスタント・スレット（APT）管理に対する必要性無しに、異常挙動モニタリング、検出、および軽減の調整を可能にする。第2の形態は、ネットワーク・トラフィック・フロー・プロファイルに関する。この形態は、ルータに対するネットワーク・トラフィック・フローの地理空間的および時間的コンテキスト／プロファイルの動的開発を含み、署名式IDS／APT管理に対する必要性無しに、異常挙動モニタリング、検出、および軽減

の調整を可能にする。第3の形態は、構成管理を含む。この形態は、ルータ、および他の同様のデバイスに対するネットワーク構成の地理空間的および時間的コンテキスト／プロフィールの動的開発を含み、署名式IDS／APT管理に対する必要性無しに、異常挙動モニタリング、検出、および軽減の調整を可能にする。第4の形態は、異常挙動の発信に関する。この形態は、ピア／隣接対応サイバー位置特定システムにより観測された、アルゴリズム的学习済み異常挙動パターンの発信を含み、潜在的なサイバー脅威の協働モニタリングおよび軽減を開始する。第5の形態は、状況認識に関する。この形態は、所与のデバイス／ルータ／埋込システム内の異常挙動パターン、またはそれらのクラスタを、管理環境における他のデバイス／ルータ／埋込システムにわたるイベント相関エンジンに対する先取り状況認識として判断することを含み、それらの動的異常挙動検出アルゴリズムを立ち上げる。

10

【0090】

図1は、本開示の少なくとも1つの実施形態による、驚異検出のためのコンテキスト・ウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステム1000の概略図である。この図において、衛星1100は、衛星スポットビーム1500で信号1600を測位ハードウェア1300に送信しているものとして示され、測位ハードウェア1300は、受信器（図示せず）を含み、信号1600を受信し、さらに測位機能および認証機能を有する。いくつかの実施形態では、測位ハードウェア1300および受信器（図示せず）は、単一ユニットに共に収容され、他の実施形態では、それらは、有線または無線によって共に接続された2つの別々のユニットに収容されることに留意されたい。

20

【0091】

スポットビーム1500は、この図に示すような円形のフットプリントを有することができ、または他の実施形態では、不規則的な形状のフットプリントを有する整形スポットビームとしてもよい。さまざまな種類の衛星および／または準衛星を、システム1000の衛星1100として使用することができる。衛星1100として使用することができる衛星の種類は、これらに限定されないが、低軌道周回（LEO）衛星、中軌道周回（MEO）衛星、および静止地球軌道（GEO）衛星を含む。1つまたは複数の実施形態において、LEOイリジウム衛星は、衛星1100のためのシステム1000によって使用される。この種類の衛星を使用することは、その送信信号が、屋内を伝わる場合を含む、減衰環境を通して伝わるのに十分強いので、有利である。

30

【0092】

測位ハードウェア1300は、ユーザと関連付けられたデバイス1200（例えば、携帯電話、携帯情報端末（PDA）、および／またはパーソナルコンピュータ）で使用することができる、1人または複数のユーザと関連付けられた認証デバイス（図示せず）で実施することができる、および／またはユーザと関連付けられたネットワークコンポーネント（例えば、コンピュータノード、インターネットプロトコル（IP）ノード、サーバ、ルータ、ゲートウェイ、Wi-Fiノード、ネットワークノード、パーソナル・エリア・ネットワーク（PAN）ノード、ローカル・エリア・ネットワーク（LAN）ノード、ワイド・エリア・ネットワーク（WAN）ノード、Bluetoothノード、ZigBeeノード、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス（WiMAX）ノード、第2世代（2G）無線ノード、第3世代（3G）無線ノード、および／または第4世代（4G）無線ノード）で使用する。測位ハードウェア1300は、対応チップセットを備え、処理機能、受信機能、送信機能（いくつかの実施形態において）、および／またはメモリ機能を有し、したがって、いくつかの実施形態において、スマート・エージェント・ダウンロード（「スマートエージェント」とも称する）の受信、およびメモリへの格納を可能にする。測位ハードウェア1300は、有線および／または無線により、ネットワーク1700に接続される。この図では、測位ハードウェア1300は、リレーとしてセルタワー1400を使用する無線ネットワーク1700に接続されるものとして示される。デバイス1200、認証デバイス、および／またはユーザと関連付けられたネットワークコンポーネントは、据え置き型および／または移動体とすることができることに留意されたい。

40

50

【0093】

衛星1100がスマート・エージェント・ダウンロードを測位ハードウェア1300に送信する前に、ユーザは、デバイス1200、認証デバイス、および／またはユーザと関連付けられたネットワークコンポーネント（例えば、ノード）の箇所を認証することによって、システム1000によって認証される。さまざまな異なる種類の認証システムおよび方法を、システム1000によって、ユーザを認証するために使用することができる。1つまたは複数の実施形態において、スポットビーム式認証システムおよび方法は、システム1000によって、ユーザを認証するために使用される。これらの実施形態に対して、LEOイリジウム衛星が衛星1100として使用され、ユーザを認証するために使用される少なくとも1つの認証信号を送信する。スポットビーム式認証システムおよび方法に関する詳細な説明は、本開示のスポットビーム式認証セクションで、以下に提示する。さらに、認証デバイス（図示せず）が、開示するシステム1000によって使用され、衛星1100から送信される少なくとも1つの認証信号を評価することによって、ユーザを認証することができる。

10

【0094】

ユーザが認証されると、衛星1100は、スマート・エージェント・ダウンロード1600を、測位ハードウェア1300に（または、いくつかの実施形態では、受信器（図示せず）に）送信する。1つまたは複数の実施形態において、スマート・エージェント・ダウンロードおよび少なくとも1つの認証信号は、どちらも、衛星1100から送信される。代替実施形態において、スマート・エージェント・ダウンロードおよび少なくとも1つの認証信号は、衛星1100または送信元から送信される。さらに、1つまたは複数の実施形態において、スマート・エージェント・ダウンロードおよび少なくとも1つの認証信号は、同じ周波数で送信される。他の実施形態において、スマート・エージェント・ダウンロードおよび少なくとも1つの認証信号は、異なる周波数で送信される。

20

【0095】

測位ハードウェア1300（または、受信器）がスマート・エージェント・ダウンロードを受信すると、測位ハードウェア1300は、スマート・エージェント・ダウンロードを、メモリに格納する。スマート・エージェント・ダウンロードは、デバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）と関連付けられた少なくとも1人のユーザに対する初期ベースライン挙動プロファイル（「ベースライン」とも称する）、デバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）と関連付けられた少なくとも1人のユーザに対するアップデート挙動プロファイル（すなわち、イベントアップデート）、モニタリングソフトウェア、および／またはセキュリティ・モニタリング・インフラストラクチャ・システム（SMIS）ソフトウェアを備える。

30

【0096】

スマート・エージェント・ダウンロードがメモリに格納されると、測位ハードウェア1300の少なくとも1つのプロセッサが、スマート・エージェント・ダウンロードを実行および／または処理する。代替実施形態では、スマート・エージェント・ダウンロードを実行および／または処理する測位ハードウェア1300のプロセッサの代わりに、少なくとも1つの異なるプロセッサを使用して、スマート・エージェント・ダウンロードを実行してもよいことに留意されたい。この異なるプロセッサは、携帯電話、携帯情報端末（PDA）、パーソナルコンピュータ、コンピュータノード、IPノード、サーバ、ルータ、ゲートウェイ、Wi-Fiノード、ネットワークノード、パーソナル・エリア・ネットワーク（PAN）ノード、ローカル・エリア・ネットワーク（LAN）ノード、ワイド・エリア・ネットワーク（WAN）ノード、Bluetoothノード、ZigBeeノード、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス（WiMAX）ノード、第2世代（2G）無線ノード、第3世代（3G）無線ノード、第4世代（4G）無線ノード、およびネットワーク・オペレーション・センター（NOC）を含むが、これらに限定されない、少なくとも1人のユーザと関連付けられた（または、少なくとも1人のユーザと関連付けられない）さまざまなデバイスまたはコンポーネントで実現することができる。

40

【0097】

50

さらに、プロセッサが、スマート・エージェント・ダウンロードを実行および／または処理するために、1つまたは複数の実施形態において、プロセッサは、特定のキー、コード、および／または他のセキュリティ手段を使用して、スマート・エージェント・ダウンロード・ソフトウェアをアンロックして、それを実行する必要がある可能性があることにも留意されたい。特定のキー、コード、および／または他のセキュリティ手段を使用することにより、スマート・エージェント・ダウンロードを含む信号の近くの「リスナ」が、対象デバイス1200、承認デバイス、または少なくとも1人のユーザと関連付けられたネットワークコンポーネント（例えば、ノード）に供給されているスマート・エージェント・ダウンロードを、受信および解読することを不可能にすることが可能になる。

【0098】

スマート・エージェント・ダウンロードが、モニタリングソフトウェアおよび／またはSMISソフトウェアを含む場合、スマート・エージェント・ダウンロードの実行時に、少なくとも1つのプロセッサは、スマート・エージェント・ダウンロード・ソフトウェアを使用して、動作内の何らかの起こり得る異常に対して、（デバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）と関連付けられた）少なくとも1人のユーザのさまざまな種類の動作をモニタリングする。プロセッサがモニタリングする動作の種類は、これらに限定されないが、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）の使用をモニタリングすること（例えば、ユーザによる特定のノードの使用をモニタリングすること）と、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）の箇所をモニタリングすること（例えば、デバイス1200、認証デバイス、またはネットワークコンポーネントの箇所は、図19から図22の記述で説明する、スポットビーム式認証を介して判断することができる）と、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）を通る実データをモニタリングすること（例えば、ユーザと関連付けられた特定のノードを通る実データをモニタリングすること）と、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）を通るデータの量をモニタリングすることと、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）を通るデータの時間をモニタリングすることと、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）を通るデータの日付をモニタリングすることと、そのデータをもともと送信している起点供給源をモニタリングすることと、そのデータが送信される宛先をモニタリングすることとを含むことができる。プロセッサがスマート・エージェント・ダウンロード・ソフトウェアを使用して、ユーザによるさまざまな動作をモニタリングすると、少なくとも1つのプロセッサが、モニタリングデータを使用して、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）に関する、ユーザに対する挙動プロファイルを生成する。

【0099】

少なくとも1つのプロセッサは、スマート・エージェント・ダウンロード・ソフトウェアを使用して、ユーザのモニタリングされたネットワーク挙動を評価し、異常挙動が生じたかどうかを判断する。1つまたは複数の実施形態において、少なくとも1つプロセッサは、スマート・エージェント・ダウンロード・ソフトウェアを使用して、ユーザに対する挙動プロファイルと、そのユーザに対するベースラインプロファイル（すなわち、ベースライン挙動プロファイル）とを比較する。プロセッサは、（1）スマート・エージェント・ダウンロードからユーザに対するベースラインプロファイルを取得することにより、（2）ユーザのネットワーク挙動を先ずモニタリングするためにスマート・エージェント・ダウンロードを使用して、次いで、ユーザに対するベースラインプロファイルを生成するためにモニタリングデータを使用することにより、（3）ネットワーク内の他のノードからユーザに対するベースラインプロファイルを受信することにより、および／または（4）ネットワーク・オペレーション・センター（NOC）からユーザに対するベースラインプロ

ファイルを受信することにより、ユーザに対するベースラインプロファイルを取得することに留意されたい。ベースラインプロファイルおよび／または挙動プロファイル（すなわち、アップデート済み挙動プロファイル）は、1つまたは複数の挙動を含むことができることにも留意されたい。次いで、少なくとも1つのプロセッサは、ユーザに対する挙動プロファイルと、そのユーザに対するベースラインプロファイルとの間に差異があるかどうかを判断する。少なくとも1つのプロセッサは、その差異が、ベースライン閾値レベル（例えば、ある所定の、および／またはプログラム可能な動作閾値）を超えた場合、ベースライン閾値レベルを超えない場合、少なくとも1つの基準を満たす場合、および／または少なくとも1つの基準を満たさない場合、その差異と関連付けられたイベントにフラグを立てる。1つまたは複数の実施形態において、少なくとも1つの基準は、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）の箇所（例えば、デバイス1200、認証デバイス、またはネットワークコンポーネントの箇所を、図19から図22の記述で説明されるような、スポットビーム式認証を介して判断することができる）、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）を通るデータの種類、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）がデータを受信する時間、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）がデータを受信する日付、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）がデータを送信する時間、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）がデータを送信する日付、データがもともと送信された起点供給源の箇所、および／またはデータが送信される宛先の箇所、に関する。

【0100】

プロセッサがイベントにフラグを立てると、プロセッサは、そのイベントを、イベント種別に分類する。次いで、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）は、そのイベントを使用して、ユーザと関連付けられた挙動プロファイルを更新することができる、および／またはそれ自体に（すなわち、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）に）配置された他のユーザに対する挙動プロファイルの1つもしくは複数またはすべてを選択的にアップデートすることができる。さらに、イベントを使用して、ネットワーク内の他のデバイス、認証デバイス、またはネットワークコンポーネント（例えば、他のノード）に配置された、他のユーザに対する挙動プロファイルの1つもしくは複数またはすべてを選択的にアップデートすることができる。デバイス1200、他のデバイス、認証デバイス、および／またはネットワークコンポーネント（例えば、ノード）は、それらに1つまたは複数の挙動プロファイルを格納することができることに留意されたい。各挙動プロファイルは、ユーザ（人間、人のグループ、または組織とすることができる）と関連付けられ、または管理者（人間、人のグループ、または組織とすることができる）と関連付けられる。あるいは、管理者と関連付けられた挙動プロファイルは、単に、人間、人のグループ、または組織と関連付けられない、テンプレート挙動プロファイルとしてもよい。

【0101】

次いで、少なくとも1つの送信器は、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）と関連付けられ、イベントを、他のユーザに対する挙動プロファイルを含むことができる、ネットワーク内の少なくとも1つの他のノード、および／またはネットワーク・オペレーション・センター（NOC）に送信する。次いで、イベントアップデートが、ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）に送信される。ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）がイベントアップデートを受信すると、少なくとも1つのプロセッサ

は、イベントアップデートを使用して、デバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）と関連付けられたユーザに対するベースラインプロファイルをアップデートする。ユーザと関連付けられたデバイス1200、認証デバイス、またはネットワークコンポーネント（例えば、ノード）は、スマート・エージェント・ダウンロード、ネットワーク内の少なくとも1つの他のノード、および／またはネットワーク・オペレーション・センター（NOC）からイベントアップデートを受信する。

【0102】

1つまたは複数の実施形態において、NOCがイベントアップデートを受信する（すなわち、ユーザの動作に異常が発生したことを示す）と、NOCは、スマート・エージェント・ダウンロードにメッセージを送信し、スマート・エージェント・ダウンロード・ソフトウェアに異常を警告する。スマート・エージェント・ダウンロードがメッセージを受信すると、スマート・エージェント・ダウンロードは、実行すべき特定のタスクを起動し、その特定のタスクは、測位ハードウェア1300および／またはユーザと関連付けられたコンポーネントもしくはデバイス1200を、完全に、もしくはネットワーク1700で動作することからシャットダウンすることができる。他の実施形態において、NOCがイベントアップデートを受信すると、NOCは、警告メッセージをスマート・エージェント・ダウンロードに送信せず、むしろNOCは、実行すべき特定のタスクを起動し、その特定のタスクは、測位ハードウェア1300および／またはユーザと関連付けられたコンポーネントもしくはデバイス1200を、完全に、もしくはネットワーク1700で動作することからシャットダウンすることができる。

【0103】

他の実施形態において、NOCがメッセージをスマート・エージェント・ダウンロードに送信して、スマート・エージェント・ダウンロード・ソフトウェアに異常を通知する代わりに、NOCは、実行すべき特定のタスクを起動する。特定のタスクは、メモリに格納された異常リストに異常をログとして記録すること、メッセージをNOCのオペレータに送信して、ユーザと関連付けられたコンポーネントもしくはデバイス1200をネットワーク1700から切り離すこと、および／または測位ハードウェア1300ならびに／もしくはユーザと関連付けられたコンポーネントもしくはデバイス1200を完全に、もしくはネットワーク1700で動作することからシャットダウンすることとすることができる。

【0104】

図2は、本開示の少なくとも1つの実施形態による、驚異検出のためのコンテキスト・ウェア・ネットワーク・セキュリティ・モニタリングのための、開示する方法2000のフロー図である。方法2000の開始2100で、少なくとも1つのプロセッサはユーザに対する挙動プロファイルを生成するために、ネットワーク内の、少なくとも1人のユーザと関連付けられた、少なくとも1つのノードの挙動をモニタリングする（2200）。次いで少なくとも1つのプロセッサが、少なくとも1人のユーザに対する挙動プロファイルを、ユーザに対するベースライン挙動プロファイルと比較する（2300）。次いで、少なくとも1つのプロセッサは、少なくとも1人のユーザに対する挙動プロファイルと、ユーザに対するベースライン挙動プロファイルとの間の差異がいつ存在するかを判断する（2400）。次いで、少なくとも1つのプロセッサは、その差異が、ベースライン閾値レベルを超えた場合、ベースライン閾値レベルを超えない場合、少なくとも1つの基準を満たす場合、および／または少なくとも1つの基準を満たさない場合、その差異と関連付けられたイベントにフラグを立てる（2500）。次いで、少なくとも1つのプロセッサは、そのイベントを、イベント種別に分類する（2600）。次いで、少なくとも1人のユーザと関連付けられた少なくとも1つのノードと関連付けられた少なくとも1つの送信器が、そのイベントを、ネットワーク内の少なくとも1つの他のノードおよび／またはネットワーク・オペレーション・センターに送信する（2700）。送信器がイベントを送信すると、方法2000は2800で終了する。

【0105】

図3は、本開示の少なくとも1つの実施形態による、驚異検出のためのコンテキスト・ウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムおよび

方法によって使用することができるセキュリティ・モニタリング・インフラストラクチャ・システム (SMIS) の概略図3000である。SMISは、サイバーセキュリティおよびネットワーク・モニタリング・データを集約して、完全な状況認証図をもたらすツールである。SMISは、統合的、事前統一セキュリティ・モニタリング・ソリューションを提供し、ネットワークセンサ、データ集合、データならびにイベントストレージ、インシデント対応、およびレポート生成を備える。SMISにより、情報技術 (IT) マネージャーが、ネットワークをモニタリングして、異常ならびに攻撃の検出、脅威の隔離ならびに分析、および手動ならびに／もしくは自動決定サポートシステムを可能にすることを可能にする。SMIS設計アーキテクチャを図3に示し、2つの主要コンポーネント、すなわち、フォレンジック・データ・コレクタ (FDC) 3010およびセキュリティ・ユーティリティ・サーバ (SUS) 3020からなる。図3に示したように、SMIS配置は、複数のFDC3010からなり、FDCは、ネットワークセンサであり、モニタリングする必要があるネットワーク要素の近くに設置される。FDC3010は、TCPDUMPおよびSyslog-ngなどの署名式検出ならびに多データ収集ならびにロギングツールのための、SNORTなどの商用オフ・ザ・シェルフ (COTS) ソリューション、侵入検出システム (IDS) に主に基づく。FDC3010によって収集される情報は、IDSセンサならびにIPパケットのヘッダに基づく起動イベント、および特定のネットワーク要素にわたって通過する全IPパケットを含み、IPパケットは、インターネット・プロトコル・バージョン4 (IPv4) およびインターネット・プロトコル・バージョン6 (IPv6) の両方である。所与のFDC3010内のデータストレージ制約のため、利用可能なストレージは、構成可能限界で円形リングバッファとしてセットアップされることに留意されたい。したがって、アーカイブされる全IPパケットの数には限界がある。ヘッダのアーカイブは、トランザクションセッションのコンテキストを開発するキーであり、ヘッダは、アーカイブ前に圧縮され、所与のFDC3010に格納できるヘッダの数を最大にすることに留意されたい。FDC3010によって収集される情報は、SUS3020によって検索され、アルゴリズム的異常ならびに挙動検出ルーチンからなるイベント関連エンジン (ECE) 3030を介して分析される。SUS3020により、特定の関心イベントがFDC3010によって検出された場合に、ネットワークマネージャーが、警告基準および閾値をセットアップすることを可能にする。生成される通知／警告に対する所与の条件が起動されると、SUS3020は、それらを、ネットワーク管理システム (NMS) 3040を介して、ネットワークマネージャーに、ネットワーク・オペレーション・センター (NOC) 3050でHTTPベース「シンクライアント」ディスプレイに示す。SMISの主要区別属性の1つは、異常挙動を判断／検出する能力であり、構成可能スライディング・ウィンドウ・タイム・フレームにわたって一時的に関連するアルゴリズム的名目的トラフィック・フローのコンテキストを構築する能力である。

【0106】

SMISの主要な利点の1つは、静的署名／ポリシーファイルによらず、特定のデバイスに対する学習済み名目的挙動に調整されるので、異常挙動検出の領域にある。SUS3020は、FDC3010からヘッダを使用して、SMISによって定義されるような、トランザクションセッション、すなわち、「対話」を備える図を構築する。SMISは、識別されたトランザクションセッションを、構成セッティングおよび各セッションの状態により、該当期間にわたって、追跡する。SMISは、IPデータパケットのヘッダの、供給源アドレス、宛先アドレス、供給源ポート、および宛先ポートに基づき、特有なタブルスペースによって、トランザクションセッションを定義する。トランザクションセッションまたは「対話」が識別されると、その統計的挙動が、一時的に確立される。先ず、この識別されたトランザクションセッションはまた、表示され、さらに、ネットワークマネージャーに、HTTPベース「シンクライアント」を介して、状況認識のために通知される。本システムが、ある期間にわたって通常条件下で動作する場合、SUS3020は、名目的動作シナリオ下で発生することが予期される、トランザクションセッションまたは「対話」のすべてについての、統計的に有用な、時間的関連名目的動作プロファイルを確立する。

【0107】

新しいデバイスまたはアプリケーションが動作システムに追加された場合、これらの新

規のトランザクションセッションは、統計的重要性および／または条件に達すると識別され、次いで、通知／警告が、アップデートされた状況認識のためにネットワークマネジャーにもたらされる。何らの例外も、既存のものに対する新しく発見されたトランザクションセッションに対してネットワークマネジャーによってアサートされない場合、コンテキストの時間的関連名目的ベースラインプロファイルへの動的アップデートをもたらす。新しいトランザクションセッションが、名目的動作プロファイルベースラインの統計的制限を超えたと識別されると、通知および／または警告が生成され、ネットワークマネジャーに送信され、状況認識を更新し、さらなる分析の開始を可能にする。トランザクションセッションが、サーバ脅威に繋がる可能性のある異常挙動であると判断されると、軽減ステップが開始される。

10

【0108】

図4は、本開示の少なくとも1つの実施形態による、図3のSMISの機能のブロック図である。当技術分野で知られているように、ネットワーク・セキュリティ・モニタリングは、ネットワーク（例えば、ネットワークトラフィック／パケット）20を通る実データパケットに基づく。SMISは、このレベルのデータを閲覧するために、2つの手段を提供する。第1は、「パケット取得」ツール22であり、センサによって観測されたデータパケットのすべての先入れ先出し（FIFO）キューへの未処理アクセスを可能にする。ネットワークトラフィックレイヤ20での第2のツールは、「ヘッダ取得」ツール24であり、SMISシステム全体にわたる他のシステムコンポーネントに対する基礎を形成する。具体的には、SMISは、コンピュータネットワークから、IPパケットを収集、すなわち取得し、取得したIPパケットからパケット・ヘッダ・データを取り除き、複数存在する同種のパケット・ヘッダ・データに対して、取り除いたパケット・ヘッダ・データを再調査し、例えば、データベースにおいて、複数回発生したと判断された任意の再調査済みパケットヘッダに対して、各特有のパケットヘッダの単一インスタンスを格納する。

20

【0109】

すなわち、SMISは、各パケットから、完全なヘッダ情報を取得し、カウンタを使用して、複数の同種パケットの発生回数を示し、特定のヘッダ情報を、表示のため、さらには、処理、および分析のため、データベースに挿入する。SMISにより、完全なヘッダのみを取得および格納することが可能となり、それにより、ディスクスペース要件が減り、パケット・ヘッダ・トランザクションのリスクが削除される。また、SMISのみが、すべてのパケットヘッダを別々に格納する代わりに、同種のパケットの単一コピーとカウンタとを格納する。

30

【0110】

図4を参照すると、SMISにおいて、ネットワークトラフィックは、「アルゴリズム」26および「署名」28の両方を通り、セキュリティ分析の未処理ビルディングブロックである「イベント」30を生成する。これらのイベントは、連続的署名規則マッチに基づきセンサ内に生成することができ、例えば、従来の侵入検出システム（IDS）は、この技術に基づいており、かなり成熟しているが、イベントはまた、非連続的方法でパケットデータを処理するアルゴリズムに基づき、イベントストリームに生成および配置してもよい。

【0111】

セキュリティ「イベント」30は、「ログビューワ」ツール32を介して、SMISで閲覧することができる。次いで、セキュリティイベント30は、ネットワークにおける周知の根本的な条件に基づいているイベントを取り除くために使用される「フィルタ」34を通り、または通常の動作と見なされ、したがって、セキュリティ警告の相関関係またはエスカレーションの一部として使用されるべきではない。

40

【0112】

イベントがフィルタされ、正規化されると、セントラルレポジトリに回送され、「正規化されたフィルタ済みイベント」36にエスカレートされ、次いで、相関関係エンジンを供給するために使用することができる。「相関関係」38は、「正規化されたフィルタ済みイベント」36を「相関関係インスタンス」40に自動的にグループ化およびスコア付けするた

50

めに使用される、一般的な規則またはアルゴリズムである。次いで、これらの「相関関係インスタンス」40は、「エスカレータ」42を介して、時間と共にスコア付けおよび追跡され得、所与の相関関係インスタンス40が、セキュリティ「アナリスト」44の注意にエスカレートされるべきかどうかを判断するために使用される。

【0113】

「警告」46のポイントでは、人間が、例えば、状態メッセージ、ネットワーク管理ソフトウェアからの指示、および警告取得処理の1つまたは複数を通じて、取り扱い処理の一部となる。問題レポート（PR）インジケータを利用して、外部問題レポートシステムが、SMISシステムにどのように接続されるかを指示する。ここまでの、全システムが構築され、膨大なネットワークおよびセキュリティデータの処理を自動化し、その結果、最も重要なデータのみが、人間によって検討されるために、アナリストに提示される。この時点で、人間のアナリストが、セキュリティデータ環境のすべての単一レベルへのアクセスを取得して、必要な評価および分析をして、単一またはグループのセキュリティ警告に対して、何らかの形式の応答が必要かどうかを判断する。

【0114】

SMISは、警告46から、相関関係インスタンス40、正規化されたフィルタ済みイベント36、イベント30、およびパケットヘッダならびに未処理パケットデータ自体への完全なドリルダウンをもたらす、すべてが、単純ポイントおよびクリック環境内からである。SMISはまた、さらに高いレベルのセキュリティデータ処理をもたらす。アナリスト44が、警告46およびそのエスカレーションに供給されるデータのすべてを再調査すると、自動的に（必要に応じて）警告46と関連付けられる「知能ログ」48にコメントを入れることによって、人間の知能を処理に入れることができる。すべてが同じ根本的な問題に関連する「警告」46が多く存在する場合、SMISが、複数の知能ログエントリを、（根本的な警告46、相関関係38、正規化されたフィルタ済みイベント36などを照合することにより）その後を追跡およびレポートすることが可能な単一「問題ログ」50に関連付けるための手段を提供する。最後に、必要なら、SMISは、「知能ログ」50エントリに基づく「インシデントログ」52のコンセプトおよびツールを提供し、問題を、正式なセキュリティインシデント応答にエスカレートする。

【0115】

SMISは、同じ環境内の統一されたセキュリティ・データ・ピラミッドの全環境へのフルアクセスを提供し、すべての他のレベルからデータのすべてへの単純ポイント・アンド・クリック・アクセスを提供する。

【0116】

SMISを補足するために、スマート・エージェント・ダウンロードは、主として、ポートスニффイングにより、その機能を拡張することができることに留意されたい。ダウンロードされたスマート・エージェント・アルゴリズムの追加により、各ノードに対して、そのコンピューティング、ストレージ、および通信使用対ノードを流れるデータパケットだけをモニタリングすることが可能となる。これにより、システムが、未知のサイバー脅威に対する迅速なイベント相関関係を可能にし、さらに、ネットワークにわたるこれらの脅威の軽減を改善するために学習済み異常挙動を発信することを可能にすることによって、上記のようにSMISインフラを改善する。

【0117】

図5は、本開示の少なくとも1つの実施形態による、スマート・エージェント・ダウンロード（すなわち、ソフトウェアアップデート）によって補助される、驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステム5000の概略図である。この図では、衛星5060から放射される所与のスポットビーム5050内に対応デバイス（例えば、対応ネットワークノード）5030、5040を有する複数のユーザ5010、5020がいる。ユーザデバイス5030、5040は、アプリオリとして知られるソフトウェアアルゴリズムを備える（例えば、そのソフトウェアは、そのデバイスが携帯電話または他の同様のデバイスである場合に、デバイス5030、5040を起動したときにデバイス

5030、5040にインストールしておくことができ、またはそのソフトウェアは、デバイス5030、5040の起動後に、適切なダウンロードを通じて、デバイス5030、5040にインストールしておくことができる）。サイバー脅威は絶えず発展しているので、デバイス5030、5040は、ソフトウェアアップロードを受け取り続け、既存および新規の脅威の両方に対してアルゴリズムを調整する可能性がある。これらのソフトウェアアップデートは、対応衛星5060の送信元から、対応デバイス5030、5040に送信される、スマート・エージェント・ダウンロードを介して受信することができ、対応デバイス5030、5040は、ダウンロードを受信することができ、それをメモリに格納し、実行することができる。対応デバイス5030、5040は、有線および／または無線により、ネットワークに接続される。この図では、対応デバイス5030、5040は、リレーとしてセルタワー5070を使用する無線ネットワークに接続される。

10

【0118】

図6は、本開示の少なくとも1つの実施形態による、驚異検出のためのコンテキスト・ウェア・ネットワーク・セキュリティ・モニタリングのための、開示する方法6000の大きな概要のフロー図である。方法6000の開始で、スマート・エージェント・ダウンロードを使用することによって、特定のノード（例えば、コンピュータなどのデバイス）でのユーザの挙動が、ベースライン化される（すなわち、ベースライン挙動プロファイルが、そのノードのユーザに対して生成される）（6010）。逸脱についてユーザの挙動をモニタリングするために、閾値および／または基準を定義し、適切なイベントにフラグを立てる際に補助する。一例において、ネットワーク・ポリシー・サーバは、閾値および／または基準を定義することができ、一方、他の例では、閾値および／または基準は、よりローカルに管理され、それらがまた、特定のノードでの特定のユーザの名目的使用に基づいて、適切に調整されることを確実にする。ベースラインからの逸脱が検出され、イベントとしてフラグが立てられ（6020）、次いで、良好な／承認されたイベントとして分類され（6030）または不良イベントとして分類される（6040）。例えば、承認されたイベントは、従業員（すなわち、ユーザ）が、自身のランチタイム中に、ローカルニュースウェブサイトアクセスしたことを通常使用で示された場合、その従業員が、自身のデスクトップコンピュータ（すなわち、ユーザの関連ノード）で、作業時間中に、同じウェブサイトをチェックすることなどである。一方、不良イベントとは、例えば、電子メールからのマルウェアが実行された場合のイベントとすることができ、非通常使用によると識別される可能性がある。あるイベントが良好／承認されたと証明されると、アルゴリズムは、6050で、1つまたは複数のノードに対する1つまたは複数のユーザ挙動プロファイルのベースライン内にこのイベントを含むよう再調整され得る。そのイベントが不良であるに関連付けられると、6060で、複雑規則プロセッサが、ネットワークの適切な応答を定義する際に補助することができる。これには、統計的にマルウェアである可能性がある場合に、所与のノードを隔離することを含むことができる。不良イベントが分類され、理解されると、6070で、ネットワークは、他のノードが感染することを防ぐ可能性を高めるために、他のノードに異常挙動パターンをさらに発信することができる。

20

30

【0119】

図7は、本開示の少なくとも1つの実施形態による、システムが位置認証対応ルータ7050、7060、および7070を使用している、驚異検出のためのコンテキスト・ウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムのトポロジー図7000である。この図は、論理トポロジー7020を、ネットワークの物理トポロジー7030と関連づけるメッシュ型物理的フレームワーク7010を示す。この図では、論理トポロジー7020は、データをネットワーク内で伝送する方法に関する。この場合、データ（すなわち、IPデータパケット）は、複数の位置認証対応ルータ7050、7060、7070およびデバイス（すなわち、ラップトップコンピュータ）7080、7090を介して、ネットワーク7030全体に伝送される。

40

【0120】

物理トポロジー7030は、物理的ネットワーク設計に関し、この用途では、地球表面の、または地球表面付近のノード（すなわち、ルータ）7050、7060、7070箇所に基づく。開示

50

するシステムは、衛星7040および受信器を使用して、対応ネットワークノード（すなわち、ルータ）7050、7060、7070が位置認証により、自身の位置特定をすることを可能にする。（位置認証処理の詳細な説明のために、本開示のスポットビーム式認証セクションを参照）。その場合、それらの物理的箇所は、IPプロトコル論理マッピングに対してマッピングされ、ネットワークセキュリティの向上を補助することができる。例えば、ルータ7060などの、汚染ネットワークノード7060は、例えば、汚染ノードのチップセットに直接、または懸念されるエリアを隔離するためにゲートウェイノードに、通知を送信することによって、NOCによって識別およびブロックされ得る。

【0121】

さらに、トラフィック・フロー（エンド・ツー・エンド）（すなわち、データパッケージがネットワークを通過する時間）およびIPデータパッケージが通る経路もまた、既知である。この情報により、ルータのシステムの構成管理は、より良好に理解され得る。これは、サイバー攻撃が発生しているかどうかを理解すること、およびデータルーティング選択を含むいくつかの潜在的用途を含む。

【0122】

図8は、本開示の少なくとも1つの実施形態による、システムがネットワーク・ポリシー・サーバ（NPS）8090を使用している、驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムの概略図8000である。少なくとも1つの実施形態において、ユーザと関連付けられたノードは、標準機械学習アルゴリズムを使用して、そのユーザに対するベースラインプロファイルを確立し、その場合、そのノードは、挙動からの逸脱を識別する際に補助するために使用することができる。次いで、ノードは、一部の挙動が基準外である（すなわち、挙動プロファイルにある挙動がベースラインプロファイルから逸脱している）ことを、異常検出機構により検出する。次いで、ノードは、実際に何らかの種類のサイバー攻撃下にある場合、自身の付近にある他のノードもまた、これと同じイベントにより影響された可能性があるか、または影響されるだろうと仮定することができる。ノードは、このイベントにフラグを立て、発信ポイント、例えば、ポリシーサーバに沿って通すことができ、次いで、イベントを評価し、適切な応答をもたらすことができる。少なくとも1つの実施形態において、ノード自身は、イベントを発信ポイントにもたらす前に、自身の評価をすることができる。この手段により、あるノードを前縁部に配置することができ（例えば、フォワードルータが、他の後端ルータの前に攻撃を認識する）、情報をシステム全体に流すことができる。したがって、フォワードルータは、異常挙動を、発信ポイントを介して、他のルータに教示することができ、各個々のルータは、自身で異常挙動を学習する必要が無い。

【0123】

この図では、4つのノード8010、8020、8030、8040（すなわち、1つのユーザデバイス8010および3つのルータ8020、8030、8040）が、サーバ攻撃による攻撃を受けている。それらは、情報を交換するか、または融合センター（例えば、ネットワーク・ポリシー・サーバ（NPS））8090にその情報を報告することができ、ネットワーク・ポリシー・サーバ（NPS）8090は、検出された異常を取得し、そのイベントをさらに定義する助けをし、攻撃が存在するかどうかというような、より最終的な決定に至ることができる。複数のノード8010、8020、8030、8040が、同様の異常挙動を検出している場合、攻撃が発生している可能性が高いことが統計的に有意になる。次いで、この融合センター／発信ポイント8090は、この情報を使用して、新しいポリシーを、他の下流のローカルノード8050、8060、8070、8080に送り出すことができ、またはポリシーをネットワーク全体に送り出すために選択してもよい。他の動作は、脅威をブロックするか、隔離するために使用されるピアグループを含んでもよい。

【0124】

例えば、この実施例において、隣接したネットワーク近傍に設置されたノードのピアグループがあってもよい。いくつかの実施形態において、これは、1つの箇所でネットワークに接合するが、異なる地理的領域に設置される（すなわち、ノード上の2人のユーザは

10

20

30

40

50

それぞれ、一方のノードは衛星に設置され、他方のノードは、サンノゼに設置され、南カリフォルニアに設置されたサーバで動作するバーチャルプライベートネットワーク（VPN）処理を通じて、同じネットワークにつながる）ユーザノードを含むことができるが、ネットワークオーバーレイから、潜在的に、ユーザノードは、同じグループ内にある。ノードの1つが異常を検出した場合、南カリフォルニアにある発信ポイントにフラグを立て、次いで、その情報を、ピアグループ内の他のノードにリレーすることができる。

【0125】

図9は、本開示の少なくとも1つの実施形態による、ユーザノード挙動をモニタリングする形態を示す驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムの概略図9000である。この実施形態において、ノードは、すでに、ノードのユーザに対するベースラインプロファイルを確立している。異常が検出される（すなわち、ベースラインからの挙動の逸脱が検出される）。本システムは、挙動パターンにおける不良または通常シフトであるか（すなわち、ユーザが、何かを使用する手段を単純にシフトしたかどうか）を判断しなければならない。イベントは、そのイベントがネガティブであるか、またはニュートラル／良好イベントであるかを判断する際に補助するように分類される。そのような要因は状況に関係する可能性があり、この状況では、ネットワークフローは、時間に依存することが知られている。例えば、従業員（すなわち、ユーザ）が、自身のランチタイム中に、自身のデバイス（例えば、デスクトップコンピュータ）でニュースウェブサイトをチェックすることは、ベースラインイベントである可能性があり、時間的に名目的である。有効なトラフィック・フローはまた、1日のある時間、すなわち、ユーザのランチタイムであることを条件としている。

【0126】

この図では、従業員Aの典型的な挙動は、電子メールを受信すること（9010）、その電子メールを開き、電子メールを読むこと（9020）、数分以内にいくつかの電子メールを互いに送信すること（9030）である。この実施例において、従業員Aは、ウィルスを含む電子メールを受信している（9040）。従業員Aは、その電子メールを開き、電子メール内の添付リンクをクリックする（9050）と、知らないうちにウィルスをばらまき始めるリンクは、ウィルスリンクを含む電子メールのバッチを、（数分以内に互いに）従業員Aのアドレスブックにある個人に送信し（9060）、ウィルスを広める。通常、従業員Aは、短い時間枠内で、大量の電子メールすべてを送信することはないので、ノードは、これが異常挙動であると認識することができるが、不良イベントであるか、従業員Aの挙動が突然シフトしたのかは認識することができない。その間に、従業員Bは、同じウィルスリンクを含む電子メールを受け取り（9070）、同様のノード挙動パターンが発生する（すなわち、従業員Bが、電子メールを開き、添付のウィルスリンクをクリックすると、ウィルスをばらまき始め、ウィルスを含む電子メールのバッチを送信する）（9080、9090）。複数の機械（すなわち、複数のノード）でこのことが発生する確率は非常に低いため、システムは、ここで、この挙動を不良イベントとして分類することができる。より多くの機械（すなわち、ノード）が、これらと同じ挙動を識別した場合、これがサイバー攻撃であることが、すぐに明らかになる。

【0127】

本システムは、挙動を分類することができ、それが不良挙動によるものとする。従来、ユーザがウィルスリンクをクリックすることによってウィルスが分散されたことを判断することができ、したがって、送達メカニズムが識別された。このシナリオでは、システムは、すぐに動作してウィルスを隔離し、電子メールの分散速度を落とし、さらに、個々のノード挙動を調整して、ウィルスが伝わった／通過したかどうかを確認することができる。いくつかの実施形態において、これは、自動化されるか、または部分的に自動化されている（例えば、個人が動作の鑑識を調整し、その情報を使用して、他のノードを保護することを助ける、ループ中に人間を含む処理である）可能性がある。少なくとも1つの実施形態において、発信ポイントは、自分で自身を隔離することによって、ノードがそのような攻撃に応じる、新しいポリシーをリレーしてもよい。

【0128】

図10は、本開示の少なくとも1つの実施形態による、図3のSMISの機能の他のブロック図である。図11は、本開示の少なくとも1つの実施形態による、少なくとも1つの検出された異常挙動の少なくとも1つのノードを再調整する形態を示す、図3のSMISの機能のブロック図11000である。図12は、本開示の少なくとも1つの実施形態による、ネットワーク管理要素を介して少なくとも1つの検出された異常挙動の少なくとも1つのノードを再調整する形態を示す、図3のSMISの機能のブロック図12000である。図10は図11と図12との組み合わせであり、したがって、図11および図12のみを以下に詳細に説明することに留意されたい。図11および図12の説明は、図10に適用される。

【0129】

図11では、警告11010が発せられる。一例において、ユーザ（すなわち、ユーザA）は、イベントを「良好」11030または「不良」11020として分類する際に補助するようユーザが使用しているノード（すなわち、ノード1）から、プロンプトを受信することができる。プロンプトでユーザ（すなわち、ユーザA）によってイベントが「良好」11030と分類されると、ノード（すなわち、ノード1）は、ユーザに対するノードのベースラインプロファイル（すなわち、プロファイルA）を再調整し、その結果、将来、ノードは、この挙動についてすでに学習しており、それが通常イベントであるとシステムが学習するために、何らの動作もユーザによって必要とされない。プロンプトでユーザによってイベントが「不良」と分類されると、ユーザに対するノードのベースラインプロファイル（すなわち、プロファイルA）は、同様に再調整される。

【0130】

しかしながら、この場合、システムはまだ、同じノード（すなわちノード1）に対する他のユーザ（例えば、ユーザB）プロファイル（例えば、プロファイルB）11040をアップデートしてもよく、および／または他のローカル／ピアノード（例えば、ノード4）11050に、検出されたのは脅威であることを通知してもよい。図3では、ノード1は、ユーザAと関連付けられ、それらの関連付けられたプロファイル（すなわち、プロファイルA）は、警告を受信することができ、ノードは、「不良」として分類することができる。次いで、ノード1は、第2のユーザ（すなわち、ユーザB）に対するベースラインプロファイル（すなわち、プロファイルB）を再調整することによって応じる。さらに、ノード1（11070）はローカルネットワーク11060を通じてこの情報を、ローカル／ピアノード（例えば、ノード4）11050に同じ情報をリレーすることができ、その結果、それらのユーザに対するベースラインプロファイルを再調整することができる（例えば、ノード4が、ユーザBに対するベースラインプロファイル（すなわち、プロファイルB）を再調整する。

【0131】

図12は、他のバリエーションを示し、警告12010が発せられ、プロンプトがローカルユーザ（すなわち、ユーザA）12050にもたらされる代わりに、警告が、ネットワーク管理要素（NME）12020、例えば、ポリシーサーバに発せられる。NME12020では、ネットワーク内の少なくとも2つのノード（例えば、ノード2（12030）およびノード3（12040））をモニタリングする際にさらなる理解が得られ、システム全体に脅威が広がる方法に関するさらなる情報を取得することができる。NME12020が、脅威に関する情報を学習するので、サービス中のノード（例えば、ノード1（12050）、ノード2（12030）、ノード3（12040））および／または追加ノード（図示せず）にも、アップデートを供給することができる。一例において、NME12020は、上流ノード（すなわちノード1）12050が識別されたという、アップデートされた驚異署名を、下流ノード（例えば、ノード2（12030）およびノード3（12040））に、何らかの地上ネットワークを介して送信することができる。他の例において、NME12020は、情報を送信し、特定のユーザに対するベースラインプロファイルもしくは複数のプロファイルを再調整することができ、および／または脅威署名をアップデートすることができる。少なくとも1つの実施形態において、これらのアップデートは、（例えば、衛星のイリジウムコンステレーションを介して）スマート・エージェント・ダウンロードを使用することによって行うことができ、スマート・エージェント・ダウンロードは、図

13に示すような対応ノードによってダウンロードされる。

【0132】

図13は、本開示の少なくとも1つの実施形態による、システムがSMISを使用しているスマート・エージェント・ダウンロードによって補助される、驚異検出のためのコンテキスト・アウェア・ネットワーク・セキュリティ・モニタリングのための、開示するシステムの概略図13000である。一例では、システムには3人のユーザ（すなわち、ユーザA、ユーザB、およびユーザC）がいて、モニタリングされている。ユーザAは、2つのノード（すなわち、どちらもユーザAと関連付けられたラップトップコンピュータ13010および携帯電話）へのアクセス権（すなわち、定義されたユーザプロファイル）を有する。ユーザBは、3つのノード（すなわち、どちらもユーザBと関連付けられたラップトップコンピュータならびに携帯電話、および共有されたデスクトップコンピュータ）へのアクセス権を有する。ユーザCは、2つのノードへのアクセス権を有する（すなわち、携帯電話およびユーザBと同じ共有ラボデスクトップコンピュータがアクセス権を有する）。

10

【0133】

一例において、ユーザAのベースラインラップトッププロファイルは、ユーザAが、通常、太平洋標準時（PST）午前8時から8時30分の間にラップトップ13010にログインすることを学習している。ユーザAのプロファイルは、ユーザAが、Google Chrome（すなわち、特定のウェブブラウザ）を使用して、ローカルニュースウェブサイトを閲覧していること、ならびに他のあらゆるウェブサイトにアクセスしていることを示し、さらにユーザAがまた、ログインした時点で電子メールをチェックし、各電子メールに対して、通常、1つの返信で、または場合によっては、伝送（すなわち、送信）間の所定時間Xより早くは生じない複数の返信で応答することを示す。ある朝、ユーザAは、いつもの時間にログインし、続けて、ローカルニュースウェブサイトをチェックする。しかしながら、この日は、Google Chromeを使用する代わりに、ユーザAは、Internet Explorerを使用する。これは、ユーザAのベースラインプロファイルからの逸脱であり、したがって、イベントとしてフラグが立てられる。

20

【0134】

簡潔にするために、対応する動作は、ユーザAがこのイベントの発生についてのプロンプトを介して通知されることを必要とすると仮定する。（すなわち、実際には、このことが当てはまらないかもしれないが、おそらく、これを問題にすることが可能になるように閾値を設定する場合、この項目の相関関係に対する驚異段階が、閾値を超える）。したがって、ユーザAは、促された場合、ユーザAに知らされた理由のために、このイベントを「良好」イベントと分類することができ、ユーザAのプロファイルに対するベースラインを再調整することができる。

30

【0135】

代替例において、ユーザBは、個人の電子メールアカウントに、ユーザCと共有するノードを使ってログインした。ユーザBは、不審なファイルを含む電子メールを開き、自身の動作の潜在的な影響を認識することなく、その電子メールを開く。この例では、マルウェア実行可能ファイルが動作し、多くの電子メールを、個人的および仕事上の人脈を含む、ユーザBのローカル・コンタクト・データベースにある個人に送信することが可能となる。この例において、システムは、ノードに送信された、ならびにノードから送信されたデータパケットを、およびユーザが電子メールアプリケーションをどのように操作したかを、モニタリングするよう設定される。システムは、実際に、ユーザBが別々に個々の電子メールを、数秒以内にいくつもの連絡先に送信することができないことを判別するよう学習済みのため、システムは、これがユーザBにとって、基準外のイベントであると識別する。

40

【0136】

この例において、システムは、ユーザを促すことなくこの区別を行うことができ、というのも、何らかの潜在的な動作基準外である（すなわち、当面のイベントの状況のコンテキストによる、異なる動作（例えば、ノードのユーザを促す、NME13020に警告する、また

50

はノードを隔離するなど)を引き起こす可能性があるイベントに対する異なる閾値が存在する可能性がある)ためである。ノードは、脅威に関する詳細を用いて、スマートエージェント13040を介して、アップデートを、脅威に関する下流ノード13050に送信する(すなわち、実行可能ファイルアップデートが、イリジウム衛星13030を介してノードに送信される)ことで、NME13020に警告することができ、その結果、その脅威から保護される。さらに、NME13020は、そのノードを隔離することができ、またはそのノード自体が、そのような問題を認識することを可能にすることができ、自身を自己隔離することができる。

【0137】

II. スマート・エージェント・ダウンロードによって補助されるネットワークポロジ

本明細書で開示する方法および装置は、スマート・エージェント・ダウンロードによって補助されるネットワークポロジに対する動作システムを提供する。具体的には、このシステムは、スマート・エージェント・ソフトウェアを、対応システムおよび/またはネットワークコンポーネントもしくはデバイスに、必要に応じてダウンロードし、技術的進歩をサポートすること、および脅威に対するセキュリティを発展させることに関する。開示するシステムは、スマート・エージェント・ソフトウェアを、屋内などの減衰環境に設置されたコンポーネントまたはデバイスにダウンロードすることができる。さらに、開示するシステムは、さまざまな異なる位置特定方法に加えて使用され、典型的なインターネットプロトコル(IP)フレームワークに対してデバイスを物理的にマッピングすることができ、物理的箇所の点から特定のデバイスがどこから所与のネットワークにアクセスしているかを識別する(例えば、デバイスのIPアドレスを使用して、デバイスの物理的箇所を識別することができる。電話番号エリアコードと同様に、デバイスのIPアドレスは、デバイスの物理的箇所/領域を説明する)。スマート・エージェント・ソフトウェアを使用して、さまざまな異なる種類のネットワーク挙動をモニタリングし、異常なネットワーク動作を識別し、非合法および/または未承認の要求者がネットワークで動作していることを示すことができる。

【0138】

現在、サイバーセキュリティは、電子システムが日々のビジネスおよび社会的タスクにより浸透しているため、ますます重要となっている。多くの以前に管理されたビジネス処理は、オンラインで処理する電子データに拡張され、実行中の情報およびコンピューティングセキュリティ促進技術を、必要要件にし、これらの日々使用されるシステムを保護する。社会保障番号から国家のインフラ関連情報までの情報を使用する重要な文書および他のデータは、ネットワーク化されたシステムに格納され、不正な当事者によってアクセスされた場合、迷惑行為から壊滅的な社会インフラ破壊までのさまざまな程度の社会的影響がもたらされる。電子システムへの依存度の増加と平行して、国家にも、テロおよびコンピュータハッキングの劇的な増加が見られる。したがって、我々のネットワーク化されたコンピュータシステムを保護する方法を改善する作業が社会に必要となっている。

【0139】

サイバー攻撃およびネットワーク侵入は、あまりに一般的になっている。これらの頻繁な発生により、商用および軍用環境における外部からの脅威によってネットワークに侵入される危険性についての説明を先ず行う。現在のアクセス制御アプローチは、静的パスワードに主に基づくか、または公開鍵基盤(PKI)に基づくパスワードおよびスマートバッジ証明書の使用に基づく認証である。システム攻撃は、エンドユーザに扮することによって行われることが多いので、ネットワークデータ傍受ネットワーク脆弱性を低減するためのユーザ認証方法に組織が集中する傾向がある。これらのアプローチは、精巧な攻撃に対して脆弱になりつつあり、したがって、ユーザ箇所およびユーザコンテキストなどの地理空間箇所/コンテキストを加えることによって通常は3つの要素(知識情報、所持情報、生体情報)の認証を超える追加の要素/情報を活用するアクセス制御の新しいパラダイムに対する必要性が開発されており、保護の追加および直交層を提供し、統合化物理的測位マッピングから論理ネットワークおよび情報管理ビューへの箇所およびコンテキスト認識

間の相互関係の向上をもたらす。

【0140】

さらに、既存のサイバー攻撃が、多くの場合、匿名で行われているという事実が、さらなる関連問題を作り出している。比較的大規模な攻撃は、多くの場合、将来の開発のためにシステムの脆弱性をより良好に理解するために、小規模な侵入／攻撃を行う考案者の試みによって防がれており、後のより破壊的な攻撃に対する基盤を敷設する。これまでに、多くの大規模なサイバー攻撃は、攻撃を受けている者を、まだ残っているダメージから回復中のままにするだけでなく、攻撃を受けた者が、報復による何らかのさらなるダメージを阻止することを不可能にさせ、そうでなければ、攻撃の起点にいる者を明らかにすることを不可能にさせ、権威者による応答を不可能にさせることが多い。攻撃の動機が不明確である場合、攻撃の受け手は、攻撃が単なる荒らし行為、意図的な窃盗、または脅威にさらされる国家安全に対するより悪意のあるアプローチであったかどうかを知ることはまず無い。したがって、無法ユーザに対するネットワークアクセスを拒否するのを補助する、および／または起点にいる者を識別するのを補助するための追跡可能データを提供する何らかのシステムが、サービス拒否（DoS）およびネットワークデータ傍受攻撃の低減および軽減に大いに役に立つであろう。

10

【0141】

本開示は、一般に、サイバーおよび／またはネットワークセキュリティのためになるネットワーク化システムに関する。すなわち、本開示のシステムは、認証済みスポットビーム伝送を介してダウンロードされたスマートエージェントの使用を通じて、情報、システム／ネットワーク管理、およびセキュリティを改善する。

20

【0142】

本開示は、2つの重要な形態を有する。第1の形態は、スマート・エージェント・ソフトウェアを使用することであり、スマート・エージェント・ソフトウェアは、開示するシステムアーキテクチャを通じて（すなわち、より強い信号および改善された信号構造を提供する、LEO衛星ダウンリンクを介して）ダウンロードすることができる。LEO衛星ダウンリンクと異なり、ダウンリンクのための既存の方法は、屋内のネットワークデバイスが、そのようなソフトウェアアップデートを確実に受信することを可能にするほど十分に堅実ではない。さらに、スポットビーム式認証方法を使用して、特定のスマート・エージェント・ソフトウェアを送信する正確なスポットビームを識別し、正しい対応受信デバイスに、スマート・エージェント・ソフトウェアを届ける。近傍にある他のデバイスと違い、標的デバイスは、これらの認証方法を使用して、実行可能ソフトウェアを開き、抽出することができる。標的ユーザは、さらに、ダウンロードの保全性を検証することができる。

30

【0143】

本開示の第2の形態は、位置特定デバイスを使用して、典型的なIPフレームワークに対してネットワークデバイスを物理的にマッピングすることであり、物理的箇所の点から特定のデバイスがどこから所与のネットワークにアクセスしているかを識別する（例えば、デバイスの電話番号および／またはインターネットプロトコル（IP）番号を使用して、デバイスの特定の箇所／領域を位置特定する）。さらに、ダウンロードされたスマートエージェントを使用して、個々のユーザおよびネットワークをモニタリングおよび管理することができる。取得したデータおよびトレンドを使用して、ネットワーク挙動モデルを作り出すことができる。モデルおよび既存／潜在的脅威を使用して、スマートエージェントもしくは他の利用可能なシステムノードソフトウェアおよび／またはハードウェアの使用を通じて管理することができる、防衛および攻撃測定法を開発し、ネットワークのセキュリティを向上することができる。この形態は、システム内のユーザおよび／またはデバイスの改善、追跡、およびモニタリングのための新しい情報管理視点を提供する。

40

【0144】

A. スマートエージェント関連実施形態

1つまたは複数の実施形態において、スマートエージェントは、さまざまな種類の認証方法を使用して、隣接するネットワークノードやデータパケットなどを認証する。これら

50

のさまざまな異なる種類の認証方法は、本開示のスポットビーム式認証セクションで、以下に詳細に説明する。

【0145】

少なくとも1つの実施形態において、スマートエージェントは、ネットワーク内の、またはネットワークに入るトラフィックを管理することができる。例えば、スマートエージェントを使用して、ネットワークデバイスが汚染されることが明らかである場合か、またはマルウェアが検出された場合に、潜在的脅威領域に最も近いトラフィックを減速することができる。スマートエージェントは、各潜在的脅威に対して特定の動作をするようセットアップすることができ、例えば、トラフィックを停止またはリルートして、システム全体に対する影響を最小にするか、または全体の脅威を停止するよう構成することができる。スマートエージェントは、潜在的脅威を識別することができる主要指標をモニタリングするよう構成してもよい。例えば、中間者攻撃は、データ待ち時間指標におけるスパイクを通じて識別することができる。識別されると、システム内のスマートエージェントは、必要に応じて、データをリルートすることができる。重要なデータおよび／またはユーザは、高い優先度で調整することができ、その結果、DoS攻撃による影響は、それらの重要なユーザに対して低くなる。これらの場合に対して、重要なデータ／ユーザは、キューの先頭に押し出され、攻撃による影響を最小にする。

10

【0146】

いくつかの実施形態において、スマートエージェントは、スポットビーム認証方法を使用して、ユーザアクセス権限を強化することができ、またはネットワークのセキュリティを向上するために実施された他のポリシーを強化することができる。

20

【0147】

1つまたは複数の実施形態において、スマートエージェントにより、追加のソフトウェア、変更、またはアップデートを、必要に応じて、ルータまたは他の種類のシステムノードにロードすることができるように、迅速なネットワークおよびシステム管理が可能になる。これには、ソフトウェアに対するルーチンアップデート、または新規の脅威を扱うための、より標的を絞ったアップデートを含むことができる。ソフトウェア変更／アップデートなどは、アクセス可能なシステムにより完成され得、一方、本開示は、サイバーおよびネットワーク管理およびセキュリティに主に注目し、ソフトウェアを、必要に応じて、さまざまな理由のためにロードすることができることは明らかである。例えば、自動車、列車、または飛行機などの車両に対して調整されたシステムを使用する場合、このシステムを使用して、これまでは、既存のアーキテクチャでは完了できなかった、必要なソフトウェアアップデートを完了することができる。

30

【0148】

少なくとも1つの実施形態において、スマートエージェントを使用して、技術進歩としてシステムの精度をより良好に向上することができる。例えば、スマートエージェントをアップデートして、新しく立ち上げられたインフラと関連付けられた追加の作動補正を受け入れる際にシステムを補助することができる。コンステレーションダウンリンク／ダウンロードを介するスマートエージェントに対するアップデートにより、システムは、最も新しい／最良の利用可能な技術にアップデートすることを可能にすることができる。

40

【0149】

B. ネットワーク・トポロジー・マッピング関連実施形態

1つまたは複数の実施形態において、スマートエージェントを使用して、ネットワーク挙動モデルを生成および／または改善するために使用されるデータおよびトレンドを取得する。モデルおよび既存／潜在的脅威を使用して、スマートエージェントもしくは他の利用可能なシステムノードソフトウェアおよび／またはハードウェアの使用を通じて管理することができる、防衛および攻撃測定法を開発し、ネットワークのセキュリティを向上することができる。

【0150】

図14は、本開示の少なくとも1つの実施形態による、スマート・エージェント・ダウン

50

ロードによって補助されるネットワークポロジータのための、開示するシステム100の概略図である。この図において、衛星110は、衛星スポットビーム150で信号160を測位ハードウェア130に送信しているものとして示され、測位ハードウェア130は、測位機能および認証機能を有する。スポットビーム150は、この図に示すような円形のフットプリントを有することができ、または他の実施形態では、不規則的な形状のフットプリントを有する整形スポットビームとしてもよい。さまざまな種類の衛星および／または準衛星を、システム100の衛星110として使用することができる。衛星110として使用することができる衛星の種類は、これらに限定されないが、低軌道周回（LEO）衛星、中軌道周回（MEO）衛星、および静止地球軌道（GEO）衛星を含む。1つまたは複数の実施形態において、LEOイリジウム衛星は、衛星110のためのシステム100によって使用される。この種類の衛星を使用することは、その送信信号が、屋内を伝わる場合を含む、減衰環境を通して伝わるのに十分強いので、有利である。

【0151】

測位ハードウェア130は、要求者と関連付けられたデバイス120（例えば、携帯電話、携帯情報端末（PDA）、および／またはパーソナルコンピュータ）で使用することができ、1人または複数の要求者と関連付けられた認証デバイス（図示せず）で実施することができ、および／または要求者と関連付けられたネットワークコンポーネント（例えば、コンピュータノード、インターネットプロトコル（IP）ノード、サーバ、ルータ、ゲートウェイ、Wi-Fiノード、ネットワークノード、パーソナル・エリア・ネットワーク（PAN）ノード、ローカル・エリア・ネットワーク（LAN）ノード、ワイド・エリア・ネットワーク（WAN）ノード、Bluetoothノード、ZigBeeノード、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス（WiMAX）ノード、第2世代（2G）無線ノード、第3世代（3G）無線ノード、および／または第4世代（4G）無線ノード）で使用することができる。測位ハードウェア130は、対応チップセットを備え、処理機能、受信機能、送信機能（いくつかの実施形態において）、およびメモリ機能を有し、したがって、スマート・エージェント・ダウンロードの受信、およびメモリへの格納を可能にする。測位ハードウェア130は、有線および／または無線により、ネットワーク170に接続される。この図では、測位ハードウェア130は、リレーとしてセルタワー140を使用する無線ネットワーク170に接続されるものとして示される。要求者は、ユーザならびに／もしくは構成要素とすることができ、および据え置き型ならびに／もしくは移動体とすることができ、ことに留意されたい。

【0152】

衛星110が、スマート・エージェント・ダウンロードを、測位ハードウェア130に送信する前に、要求者は、システム100によって認証される。さまざまな異なる種類の認証システムおよび方法を、システム100によって、要求者を認証するために使用することができる。1つまたは複数の実施形態において、スポットビーム式認証システムおよび方法は、システム100によって、要求者を認証するために使用される。これらの実施形態に対して、LEOイリジウム衛星が衛星110として使用され、要求者を認証するために使用される少なくとも1つの認証信号を送信する。スポットビーム式認証システムおよび方法に関する詳細な説明は、本開示のスポットビーム式認証セクションで、以下に提示する。さらに、認証デバイス（図示せず）が、開示するシステム100によって使用され、衛星110から送信される少なくとも1つの認証信号を評価することによって、要求者を認証することができる。

【0153】

要求者が認証されると、衛星110は、スマート・エージェント・ダウンロード160を、測位ハードウェア130に送信する。1つまたは複数の実施形態において、スマート・エージェント・ダウンロードおよび少なくとも1つの認証信号は、どちらも、衛星110から送信される。代替実施形態において、スマート・エージェント・ダウンロードおよび少なくとも1つの認証信号は、衛星110または送信元から送信される。さらに、1つまたは複数の実施形態において、スマート・エージェント・ダウンロードおよび少なくとも1つの認証信号は

、同じ周波数で送信される。他の実施形態において、スマート・エージェント・ダウンロードおよび少なくとも1つの認証信号は、異なる周波数で送信される。

【0154】

測位ハードウェア130がスマート・エージェント・ダウンロードを受信すると、測位ハードウェア130は、スマート・エージェント・ダウンロードを、メモリに格納する。スマート・エージェント・ダウンロードがメモリに格納されると、測位ハードウェア130のプロセッサが、スマート・エージェント・ダウンロードを実行する。代替実施形態では、スマート・エージェント・ダウンロードを実行する測位ハードウェア130のプロセッサの代わりに、異なるプロセッサを使用して、スマート・エージェント・ダウンロードを実行してもよいことに留意されたい。この異なるプロセッサは、携帯電話、携帯情報端末（PDA）、パーソナルコンピュータ、コンピュータノード、IPノード、サーバ、ルータ、ゲートウェイ、Wi-Fiノード、ネットワークノード、パーソナル・エリア・ネットワーク（PAN）ノード、ローカル・エリア・ネットワーク（LAN）ノード、ワイド・エリア・ネットワーク（WAN）ノード、Bluetoothノード、ZigBeeノード、ワールドワイド・インターオペラビリティ・フォー・マイクロウェーブ・アクセス（WiMAX）ノード、第2世代（2G）無線ノード、第3世代（3G）無線ノード、および第4世代（4G）無線ノードを含むが、これらに限定されない、要求者と関連付けられたさまざまなデバイスまたはコンポーネントで実現することができる。

10

【0155】

さらに、プロセッサがスマート・エージェント・ダウンロードを実行するために、1つまたは複数の実施形態において、プロセッサは、特定のキー、コード、および／または他のセキュリティ手段を使用して、スマート・エージェント・ダウンロード・ソフトウェアをアンロックして、それを実行する必要がある可能性があることにも留意されたい。特定のキー、コード、および／または他のセキュリティ手段を使用することにより、スマート・エージェント・ダウンロードを含む信号の近くの「リスナ」が、対象デバイス120に供給されているスマート・エージェント・ダウンロードを、受信および解読することを不可能にすることが可能になる。

20

【0156】

スマート・エージェント・ダウンロードを実行する場合、スマート・エージェント・ダウンロード・ソフトウェアは、動作内の何らかの潜在的異常に対して、さまざまな種類のネットワーク動作をモニタリングする。スマート・エージェント・ダウンロードによってモニタリングされるネットワーク動作の種類は、これらに限定されないが、要求者と関連付けられたデバイス120またはコンポーネントの利用をモニタリングすること（例えば、特定のノードの利用をモニタリングすること）、要求者と関連付けられたデバイスまたはコンポーネントの箇所をモニタリングすること、ネットワーク170で動作しているユーザをモニタリングすること、ネットワーク170を通る実データをモニタリングすること（例えば、特定のノードを通る実データをモニタリングすること）、およびネットワーク170を通るデータの量をモニタリングすることを含むことができる。スマート・エージェント・ダウンロードは、モニタリングされたネットワーク挙動を評価し、異常が発生したかどうかを判断する。異常が発生したかどうかを判断するために、ある所定の、および／またはプログラム可能な動作閾値を、スマート・エージェント・ダウンロードのためのガイドラインとして使用することができる。動作閾値が超えられ、したがって、ネットワーク挙動異常が発生したとスマート・エージェント・ダウンロードが判断したら、スマート・エージェント・ダウンロードは、実行すべき特定のタスクを起動する。特定のタスクとは、ネットワーク挙動異常メッセージをネットワーク・オペレーション・センター（NOC）（図示せず）に送信すること、および／または要求者と関連付けられた測位ハードウェア130および／またはコンポーネントもしくはデバイス120を、完全に、またはネットワーク170での動作から、シャットダウンすることとすることができる。

30

40

【0157】

代替実施形態では、スマート・エージェント・ダウンロードが、モニタリングされたネ

50

ットワーク挙動を評価して、異常が発生したかどうかを判断する代わりに、スマート・エージェント・ダウンロードがモニタリングしたネットワーク動作を取得したら、モニタリングされたネットワーク動作は、送信元によって、NOCに送信され、NOCがネットワーク挙動を評価して、その動作内で異常が発生したかどうかを判断する。NOC内のプロセッサを使用して、モニタリングされたネットワーク動作を評価し、異常が発生したかどうかを判断する。NOCでのプロセッサが、動作内に異常が発生したと判断した場合、NOCは、スマート・エージェント・ダウンロードにメッセージを送信し、スマート・エージェント・ダウンロード・ソフトウェアに異常を警告する。スマート・エージェント・ダウンロードがメッセージを受信すると、スマート・エージェント・ダウンロードは、実行すべき特定のタスクを起動し、その特定のタスクは、測位ハードウェア130および／または要求者と関連付けられたコンポーネントもしくはデバイス120を、完全に、もしくはネットワーク170で動作することからシャットダウンすることができる。他の実施形態において、NOCでのプロセッサが、動作内に異常が発生したと判断した場合、NOCは、警告メッセージをスマート・エージェント・ダウンロードに送信せず、むしろNOCは、実行すべき特定のタスクを起動し、その特定のタスクは、測位ハードウェア130および／または要求者と関連付けられたコンポーネントもしくはデバイス120を、完全に、もしくはネットワーク170で動作することからシャットダウンすることができる。

10

【0158】

他の実施形態において、NOCがメッセージをスマート・エージェント・ダウンロードに送信して、スマート・エージェント・ダウンロード・ソフトウェアに異常を通知する代わりに、NOCは、実行すべき特定のタスクを起動する。特定のタスクは、メモリに格納された異常リストに異常をログとして記録すること、メッセージをNOCのオペレータに送信して、要求者と関連付けられたコンポーネントもしくはデバイス120をネットワーク170から切り離すこと、および／または測位ハードウェア130ならびに／もしくは要求者と関連付けられたコンポーネントもしくはデバイス120を完全に、もしくはネットワーク170で動作することからシャットダウンすることとすることができる。

20

【0159】

図15は、本開示の少なくとも1つの実施形態による、スマート・エージェント・ダウンロードによって補助されるネットワークトポロジーのための、開示する方法のフロー図200である。本方法の開始210では、認証デバイスを使用して、要求者を認証する(220)。要求者が認証されると、230で、送信元は、スマート・エージェント・ダウンロードを、要求者と関連付けられた受信先に送信する。次いで、240で、受信先が、スマート・エージェント・ダウンロードを受信する。受信先がスマート・エージェント・ダウンロードを受信すると、250で、プロセッサが、スマート・エージェント・ダウンロードを実行する。スマート・エージェント・ダウンロードが実行されると、260で、スマート・エージェント・ダウンロード・ソフトウェアがネットワーク挙動をモニタリングし、次いで、270で、本方法は終了する。

30

【0160】

図16は、本開示の少なくとも1つの実施形態による、ネットワーク挙動をモニタリングするネットワーク・オペレーション・センター(NOC) 350を示す概略図300である。この図では、複数のネットワークノード330、340が、有線および／または無線ネットワークを介して接続されているとして図示する。ネットワークノード330のいくつかは、ハブ(例えば、ノードB)の役目を果たし、ネットワーク全体にデータをルーティングする。また、ネットワークノード330のいくつかは、関連付けられ、認証された、および／または正当な、要求者310を有するよう図示され、1つのノード340は、認証されない、および／または不正な、要求者320を有するよう図示される。スマート・エージェント・ダウンロードは、ネットワークノード330、340にダウンロードされ、実行されて、ネットワーク動作をモニタリングする。1つまたは複数の実施形態において、モニタリングされたネットワーク動作は、NOC350に無線で送信され、セルタワー360を介して評価される。

40

【0161】

50

少なくとも1つの実施形態によれば、スマート・エージェント・ダウンロード・ソフトウェアを使用して、個々のユーザ（または、要求者）挙動プロファイルを開発し、ユーザ・ベースライン・パラメータおよびトレンドを確立することができる。ユーザの受け入れ可能な通常状態を理解することによって、感染したハードウェアおよび／またはマルウェアの発生などにより、パラメータが適切な閾値から外れたことが、より迅速に識別され、解決することができる。個々のユーザの挙動プロファイルの収集およびそれらの相互接続を同様に再調査して、受け入れ可能なネットワーク挙動基準のプロファイルを開発し、その結果、中間者攻撃などに対してより良好な反応をするために使用することができる、少なくとも1つの実施形態によれば、スマートエージェントを使用して、ネットワーク内の、またはネットワークに入るトラフィックを管理することができる。

10

【0162】

図16に示すように、なりすまし人320は、感染ノード340により、ノードA340でネットワークにアクセスを試みる。さまざまな手段（例えば、スポットビーム式認証システムならびに方法およびスマート・エージェント・ダウンロードモニタリングソフトウェア）により、感染ノード340を識別することができる。識別されると、ノード340と関連付けられた測位対応ハードウェア（図16には図示せず）を使用して、潜在的問題領域に最も近いトラフィックを減速し、ネットワークに対するリスクを最小にすること、ネットワークトラフィックをリルートすること、またはノードB330でのネットワークトラフィックを停止して、なりすまし人320を隔離し、ネットワークをさらに害することを不可能にするか、もしくは脅威をまとめて停止することなどの、さまざまなタスクを実行することができる。スマート・エージェント・ダウンロード・ソフトウェアは、これらの潜在的脅威および中間者攻撃などの他の脅威を識別することができる主要指標をモニタリングするよう構成することができる。例えば、中間者攻撃は、データ待ち時間指標におけるスパイクを通じて識別することができる。識別されると、システム内のスマートエージェントは、必要に応じて、データをリルートすることができる。重要なデータおよび／またはユーザは、高い優先度で調整することができ、その結果、サービス拒否（DoS）攻撃による影響は、それらの重要なユーザに対して低くなる。重要なデータ／ユーザは、キューの先頭に押し出され、攻撃による影響を最小にする。

20

【0163】

スマート・エージェント・ダウンロード・ソフトウェアを使用することにより、本ソフトウェアは、ネットワークトラフィックに対する重要なインターネットバックボーン／基幹ルートをモニタリングおよび追跡することができる。インターネットルータは、ネットワーク全体の、集約ネットワークトラフィック回送およびリルートを行う。これらの回送およびリルート経路は、ネットワークへのアクセス権を取得しようとしている無法ユーザからの操作を受けやすい。ネットワークトラフィックは、リアルタイムに、および後にオフラインで、スマート・エージェント・ダウンロード・ソフトウェアによって分析され、潜在的サービス拒否（DoS）攻撃を識別することができる。

30

【0164】

この潜在的リスクの軽減を補助するために、1つまたは複数の実施形態において、開示するシステムは、隣接するルータ（すなわち、ピア・ツー・ピア・ルータ）を活用して、互いに回送しているネットワークトラフィックを分類し、各ネットワークトラフィック分類に対するデータ待ち時間特性を推定することができる。これらのルータは、互いの供給された測位データを交換および検証することを通じて、互いに認証することができる。これらのルータは、これらに限定されないが、グローバル測位システム（GPS）信号を使用することおよびスポットビーム式認証システムならびに方法を使用することを含む、さまざまな方法を通じて、測位データを取得することができる。すべてのネットワークトラフィックが、サービス品質（QoS）準備ポリシーおよび各ネットワークトラフィック分類と関連付けられた帯域幅の実際量を変えるなどの要因のため、同じデータ待ち状態特性を受けていない間、データ待ち状態特性は、バックボーン／基幹ネットワークインフラにおける日毎のパターンおよび潜在的欠陥などの要因に基づいて変化するトラフィックプロファ

40

50

イルを考慮し、適合する、動的スライディングウィンドウに基づき計算することができることに留意されたい。

【0165】

ルータがインターネット・ネットワーク・インフラに追加されるか、または除去された場合、ネットワークトポロジーのアップデート、およびOSPFおよびBGPなどのリンク状態プロトコルによって駆動されるパケット回送経路への変化を引き起こす。日毎のトラフィックパターンに起因するネットワーク・トラフィック・プロファイルの遷移は、徐々に、ネットワークトポロジーをアップデートし、パケット回送経路を変更し、ネットワークトポロジーをより迅速にアップデートする。ネットワークトポロジーおよびパケット回送経路の変更は、ネットワーク管理イベントおよびリンク状態プロトコルを介して、インターネット・ネットワーク・インフラにわたって伝送され、したがって、各ルータは、そのような変更が発生した場合に離散的イベントを認識し、それに応じて、データ待ち時間などのさまざまな推定処理を考慮することができる。インターネット・ネットワーク・インフラが正常に動作している場合の環境下で、ルータの間の回送およびルーティング経路の劇的な変化は考えないだろう。したがって、隣接ピア・ツー・ピア・ルータに対するスマート・エージェント・ダウンロードが、ベースライン受け入れ可能範囲を超えたネットワーク・トラフィック・クラスの1つまたは複数に対する2つのルータ間のネットワークトラフィック特性における逸脱を検出した場合、スマート・エージェント・ダウンロードは、ネットワーク管理要素に対して警告を引き起こすことができ、さらに、自律機構を制限し、ネットワークトラフィックの特定のクラスの割合を規制するか、または、極端なシナリオでは、代替経路を介してトラフィックを完全に停止するか、もしくはリルートすることによって、潜在的悪影響を限定することができる。

【0166】

隣接ピア・ツー・ピア・ルータの間のネットワーク・トラフィック・フローをモニタリングおよび管理する調整済み機構はまた、重要なネットワークトラフィックが、DoS攻撃中にQoS優先順位付けを使用してネットワークをトラバースすることを確実に可能にさせることができるよう使用することができる。そのようなシナリオでは、期待されたトラフィック形状特性から基準外であると見なされるネットワークトラフィックのクラスは、出口ルータでレート制限され得る。レート制限は、最も重要なネットワークトラフィックが、基準外と見なされたネットワークトラフィックを通過することを可能にする、および可能にしないことによって、ネットワークトラフィックのレートが、ある閾値レート未満を維持するようモニタリングされ、要求されることを含む。この制限を使用して、DoS攻撃がネットワークを通じてさらに伝わらないことを確実にすることができ、一方、重要なネットワークトラフィックがネットワークを通ることを可能にすることができる。モニタリング、検出、および決定に至るための警告および通知機構は、複合イベント処理（CEP）および分析を使用することができ、そのような分析には、異常および相関関係を検出して、データ・トラフィック・ストリーム特性およびポリシー駆動自律ネットワーク管理決定ならびに／もしくは動作を識別するための因果連鎖解析などがある。このアプローチは、各ルータ内にダウンロードされた標的スマート・エージェント・ソフトウェアの使用を活用することができ、裏付けされたNOC350またはネットワーク管理要素とインターフェースして、必要に応じて、追加の実行ファイルを抽出することができる。

【0167】

図17は、本開示の少なくとも1つの実施形態による、ネットワーク挙動における異常440の検出を示すグラフ400である。特に、特定のノードを通るネットワークトラフィックをモニタリングするスマート・エージェント・ダウンロードから収集されたデータの例示的グラフを示す。この図では、x軸線は、特定のノード410を通過するネットワークトラフィックの量を示し、y軸線は、時間420の経過を示す。時間ゼロ（0）から時間Tまでは、ノードのトラフィック動作レベルは、ノードに対する通常のトラフィック動作レベル430に近いままである。しかしながら、時間Tでは、ノードのトラフィック動作は、著しく高いレベルまで急上昇する。時間Tから後は、ノードに対するノードのトラフィック動作レベル

は、通常のノードのトラフィックレベルよりもかなり高いことが示され、したがって、このデータを分析することによって、スマート・エージェント・ダウンロードは、ノード異常440がそのノードに対して発生した（例えば、ノード攻撃が発生している）と判断する。

【0168】

図18は、本開示の少なくとも1つの実施形態による、論理トポロジー510をネットワークの物理トポロジー520と関連する、メッシュ状物理的フレームワーク500の一例を示す概略図である。物理的ビューおよび論理的ビューを合わせ、両方のビューからのネットワーク挙動モデルに視認可能にすることにより、スマート・エージェント・ダウンロードが、特定のイベントおよび挙動を確実および堅実に追跡およびさかのぼることを可能にし、さらに、観測下で異常イベントの1つまたは複数の供給源を確かめることを可能にする。バックエンドNOCまたはネットワーク管理要素は、協働対応コンピューティングデバイスおよびルータによってリレーされたモニタリング情報を使用して、挙動モデルを構築することができ、サイバー防御および攻撃のために、通信およびコンピューティングの調整を可能にすることができる。

【0169】

この図では、論理トポロジー510は、データをネットワーク内で伝送する方法に関する。この場合、データは、IPルーティングを介して、およびリレー衛星580を使用することによって、ネットワーク570全体に伝送される。物理トポロジー520は、物理的ネットワーク設計に関し、この用途では、地球表面の、または地球表面付近のノード箇所に基づく。開示するシステムは、衛星530および受信器を使用して、ネットワークノードが、自身の位置特定をすることを可能にする。その場合、それらの物理的箇所は、IPプロトコル論理マッピングに対してマッピングされ、ネットワークセキュリティの向上を補助することができる。例えば、ルータ550などの、汚染ネットワークノード540は、例えば、汚染ノードのチップセットに直接、または懸念されるエリアを隔離するためにゲートウェイノードに、通知を送信することによって、NOCによって560で識別およびブロックされ得る。

【0170】

III. スポットビーム式認証

要素またはユーザ認証技術により、サードパーティの検証器が、一方向認証方法による遠隔リソースに対して、ユーザ、資産、またはデバイスの識別を検証することを可能にする。しかしながら、この一方向方法はまた、ホストシステムによって、要求者を検証するために直接使用してもよいことに留意されたい。要素は、追跡する必要のあるデバイス（例えば、携帯電話、コンピュータ、またはサーバなど）または資産とすることができ、一方、ユーザは、人間、または他の生物／非生物要素とすることができ、要素および／またはユーザは、接続またはセッション全体の期間、認証することができる。要素および／またはユーザは、元の認証後に、再認証を要求される可能性がある。再認証要求は、ホストネットワークによって定義することができ、コンテキスト特有としてもよい。あるいは、このシステムは、各メッセージに対して別々の認証処理を要求する、メッセージ式認証システムに対して使用することができる。本明細書で説明する技術は、セッション式認証、メッセージ式認証、またはそれらの組み合わせのいずれに対しても使用することができる。

【0171】

さらに、この方法は、受信デバイス自身に適用してもよく、一方向認証を、遠隔のサードパーティによって完了する必要はなく、むしろ、1つまたは複数の受信デバイスによって完了する。この方法が、単一デバイスで実行される場合、一方向認証方法が依然として考慮される。しかしながら、この方法はまた、多方向認証技術で適用され、少なくとも2つのピアデバイスが、互いに認証することを可能にすることができる。この一方向または多方向デバイス・ツー・デバイス認証方法では、認証は、一般に、2つの正当な受信デバイスのそれぞれが把握しているか、または任意の非認証または無法受信デバイスが把握していない、共有シークレット（対称性および非対称性）に依存する可能性がある。各デバ

イスは、セキュリティ証明書の形式で、自身とピアデバイスとの間で共有される秘密パスワードまたは公開／秘密鍵ペアなどの、特有な認証証明書を有する。デバイスは、他のピアデバイスによる要件を満たすために、共有シークレットを把握している、すなわち、正当であると証明された場合に、自身を認証してきた。この多方向認証方法における少なくとも2つのデバイスの間で認証が完了すると、デバイスは、互いに識別情報を証明する。次いで、デバイスは、同意したサイバー・セキュリティ・ポリシーを実施するために選択することができる自身の認証ネットワークを生成して、所与のコンテキストに対してネットワーク化されたリソースへの通信およびアクセスを保護することができる。

【0172】

既存の認証方法は、初期セキュリティキーを生成するために使用または組み合わせることができる。例えば、初期セキュリティキーは、Diffie-Hellman技術を使用して、協働的に生成してもよく、または単に一方のピアデバイスにより生成して、代替の安全なチャネル／方法を介して他方に送信してもよい。

【0173】

あらゆる場合において、初期セキュリティキーには、（上記のように）何らかの共有活性情報を添付することを含んでもよい。この用途では、活性情報は、衛星スポットビームを通じてもたらされ、タイムスタンプおよび疑似乱数（PRN）として認証時に使用するためのそのようなパラメータを含むことができる。

【0174】

共有活性情報を使用することにより、導出時に使用され、開始デバイスが自身をピアデバイスに認証する度に異なるセキュリティキーを使用することを可能にすることができる。これにより、開始デバイスが認証される毎に潜在的な不正盗聴者が統計的攻撃を開始することを妨害し、新規の傍受メッセージを、開始デバイスの前のセッション中に傍受されたメッセージの分析に追加する。次いで、活性情報および初期セキュリティキーは、決定的関数への入力として通すことができる。本明細書で使用される場合、「決定的」という用語は、その機能の出力が、入力によって完全に決定される関数を意味する。この決定的関数は、開始デバイスおよびピアデバイスで別々に動作することができる。これら2つのデバイスが、決定的関数を実行した場合に異なる出力を生成した場合、関数から生じたセキュリティキーは一致せず、デバイスは認証されず、したがって、相互通信のために使用することができない。

【0175】

決定的であることに加え、セキュリティのために、本関数は、本質的に不可逆的であるべきである。本関数の出力を把握しても、その入力を判断することは非常に難しいか、または不可能であろう。ハッシュは、決定的および本質的に不可逆である関数のクラスを形成し、したがって、暗号化および認証計算で使用されることが多い。周知のトランスポート・レベル・セキュリティ（TLS）プロトコルで使用される疑似乱数関数（PRF）は、使用され得る決定的関数導入の一例である。

【0176】

PRFは、2つの周知のハッシュ関数、メッセージ・ダイジェスト・アルゴリズム5（MD5）、およびセキュア・ハッシュ・アルゴリズム1（SHA-1）の結果を組み合わせる。PRFは、2つのハッシュ関数を使用して、誰かが2つのハッシュ関数の1つを反転する方法を決定した場合にのみ、セキュリティを保護する。これら2つのハッシュ関数は、短すぎてセキュリティに対して最適ではない可能性がある出力を生成する。SHA-1は、20バイト出力を生成し、MD5は、16バイト出力を生成する。したがって、2つのハッシュ関数のそれぞれに対して、「データ拡張関数」は、ハッシュ関数を使用して、任意の長さの出力を生成するものとして定義することができる。SHA-1の場合、データ拡張関数は、P_SHA-1として定義することができる。

EQ 1: $P_SHA-1(\text{initial-security key, liveness}) = SHA-1(\text{initial-security key, } A(1) + \text{liveness}) + SHA-1(\text{initial-security key, } A(2) + \text{liveness}) + SHA-1(\text{initial-security key, } A(3) + \text{liveness}) + \dots$

ここで、 $A(0)$ = 活性情報;

$A(i) = \text{SHA-1}(\text{initial-security key}, A(i - 1))$

および、「+」記号は、文字列の連結を意味する。

【0177】

データ拡張関数P_MD5の定義は、「SHA-1」を「MD5」で置き換えることで、上記の定義と同様となる。データ拡張関数は、必要なステップだけ繰り返され、所望の長さの出力を生成することができる。所望の出力長は、導入オプションとして設定してもよい。少なくとも1つの実施形態において、各ハッシュ関数に対する所望出力長は、128バイトである。P_SHA-1は、 $A(7)$ まで繰り返され、総出力長を140バイトにすることができる（各繰り返しにより、20バイトずつ出力長が増える）。その場合、出力を、128バイトに切り捨ててもよい。P_MD5の各繰り返しは、16バイトを生成し、 $A(8)$ まで繰り返すと、切り捨てることなく、所望の128バイトを生成する。

10

【0178】

スポットビーム式認証のための一実施形態において、ハッシュ関数を選択し、データ拡張関数を所望の出力長まで繰り返し、PRFは、入力として、拡張初期セキュリティキー、ラベル（予め決められたASCII文字列）、および交換される活性情報を受け取る。PRFは、2つのハッシュデータ拡張関数P_MD5およびP_SHA-1の出力の、排他的ビット単位OR（XOR）であるものとして定義される。

EQ 2: $\text{PRF}(\text{expanded initial-security key}, \text{label}, \text{liveness}) = \text{P_MD5}(S1, \text{label} + \text{liveness}) \text{ XOR } \text{P_SHA-1}(S2, \text{label} + \text{liveness})$

20

ここで、S1は、拡張初期セキュリティキーの前半であり、バイト単位で測定され、S2は、拡張初期セキュリティキーの後半である。（拡張初期セキュリティキーの長さが奇数である場合、その中間バイトは、S1の最終バイトとS2の最初のバイトとの両方である。P_MD5およびP_SHA-1が繰り返され、128バイト出力を生成すると、PRFの出力もまた、128バイトになる。

【0179】

PRFの128バイト出力は、4つの32バイト・セッション・セキュリティ・キーに分割される。その場合、セッション・セキュリティ・キーのそれぞれは、使用される認証および暗号化プロトコルによって要求される長さに切り捨てられる。切り捨てられた結果は、一時的セッション・セキュリティ・キーの新規セットの1つである。一時的セッション・セキュリティ・キーの導出により、開始デバイスおよびピアデバイスの両方に対して、初期秘密鍵または拡張初期セキュリティキーのいずれも直接使用しないことを可能にし、セキュリティキー情報の漏洩を最小にするか、または少なくとも減らすことを可能にする。一時的セッション・セキュリティ・キーの導出により、さらに、開始デバイスおよびピアデバイスが、規則的間隔で、またはセッション・セキュリティ・キーの使用を制限することによって統計分析を妨げるよう指示された場合に、拡張初期セキュリティキーから生じたセッション・セキュリティ・キーをリフレッシュすることを可能にする。

30

【0180】

認証および暗号化一時的セッション・セキュリティ・キーのそれぞれは、以下の特定の目的、すなわち、i) 機密保護のため、開始デバイスからピアデバイスへのデータ交換の暗号化、ii) 機密保護のため、ピアデバイスから開始デバイスへのデータ交換の暗号化、iii) 保全性のため、開始デバイスからピアデバイスへのデータ交換の署名、およびiv) 保全性のために、ピアデバイスから開始デバイスへのデータ交換の署名、を有する。

40

【0181】

スポットビーム式認証のための初期セキュリティキーの導出は、取り決められた、周知の、パブリック・プリミティブ・ルート・ジェネレータ「g」およびプライムモジュラス「p」を使用するDiffie-Hellman技術を使用してもよい。開始デバイスおよびピアデバイスは、それぞれ、ランダムな秘密整数（secret integer）を選択し、それぞれ $(g^{\text{secret integer}}) \bmod p$ を交換する。この交換により、開始デバイスおよびピアデバイスは、Diffie-Hellmanを使用して、共有された初期秘密鍵を導出することが可能となる。

50

【0182】

開始デバイスおよびピアデバイスの両方の間で共有された初期秘密鍵を導出した場合、データ拡張を使用して、例えば、P_SHA-1を用いて、拡張初期秘密鍵を導出することができる。データ拡張処理に対する活性情報は、開始デバイスおよびピアデバイスによって取り決められる既知の乱数値またはタイムスタンプとすることができる。いくつかの実施形態において、ピアデバイスは、乱数値を選択して、それを、衛星または地上ネットワークを介して、開始デバイスに送信する。あるいは、開始デバイスおよびピアデバイスの両方は、タイムスタンプを取り決めることができ、というのも、両者が時間的に密に同期しているからであり、それにより、共有／共通タイムスタンプ値から活性を選択することができる間、データ交換を避けることができる。

10

【0183】

これに続き、開始デバイスおよびピアデバイスは、一時的セッション・セキュリティ・キーの新規セットを導出するために使用することができる、共有拡張初期秘密鍵を有する。この場合も、活性のために、開始デバイスおよびピアデバイスは、ピアデバイスによって送信される共有乱数値または共有／共通タイムスタンプ値のいずれかを使用することができる。一時的セッション・セキュリティ・キーは、開始デバイスおよびピアデバイスによって使用され、開始デバイスおよびピアデバイスの間の暗号化、測位の署名、および他のコンテキスト情報交換をさらに行うことができる。測位および他のコンテキスト情報は、機密性を考慮され、したがって、そのような情報は、暗号化され、認証された開始デバイスおよびピアデバイスのみが、交換された測位およびコンテキスト情報を抽出できることを確実にするのに適切である。測位は、疑似ランダム（PRN）コードセグメントおよび特有のビームパラメータを使用して、本特許出願において説明される手順により認証されることに留意されたい。共有されたコンテキスト情報は、標的サイバー防御アプリケーション実行または決定サポートシステムのための他の状態または制御情報を含んでもよい。暗号化に加え、交換された測位およびコンテキスト情報の保全性が、上記のように、署名のために一時的セッション・セキュリティ・キーを使用することにより、確実にする。

20

【0184】

簡潔に述べると、いくつかの実施形態において、本明細書で説明する認証システムおよび方法は、測位技術を活用し、認証処理の一部として要求者の位置を判断することができる。そのような測位技術の1つは、同一出願人による同時係属米国特許出願第12/756961号「Geolocation Leveraging Spot Beam Overlap」に定義され、その開示は、参照により全体が本明細書に組み込まれる。認証が必要な場合、要求者デバイスは、特有の署名パラメータを取得し、それを検証デバイスに送信することができる。さらに、要求者デバイスは、要求された移動経路（すなわち、それぞれにおける中間地点と時間）を送信することができる。中間地点は、デバイスが据え置きか移動体かについて送信することができる。検証デバイスは、要求者の要求したビーム署名パラメータ、少なくとも1つの箇所中間地点、およびこの取得した中間地点およびビームパラメータと関連付けられた少なくとも1つの時間を使用して、要求者を認証することができる。例えば、要求者は、少なくとも1つのスポットビームおよび少なくとも1つの要求された中間地点から取得されたビームパラメータが、既知の検証データセットに対して確認された場合、検証器によって認証されたと考えることができる。このような方法で、特定の時間に領域内にあるとして、要求者を認証することができる。これらのパラメータに基づく復号コードは、エミュレート、ハッキング、またはスプーフィングすることが極めて困難な信号をもたらす。さらに、信号構造および衛星が受信した信号電力により、認証のために屋内または他の減衰環境で使用する事が可能になる。これにより、このシステムアプローチの全体的な実用性が向上する。

30

40

【0185】

本出願の発明の主題は、イリジウム衛星によって実現されるような、低軌道周回（LEO）衛星のコンテキストで主に説明される。しかしながら、本明細書で説明する技術は、他の衛星システム、例えば、中軌道周回（MEO）衛星システム、および静止地球軌道（GEO）

50

衛星システムに容易に適用可能であることを当業者は認識するであろう。そのような衛星式通信システムは、他のモバイル通信システム、例えば、空中通信システムなど、および、これらに限定されないが、船または携帯電話タワーを含む静止通信プラットフォームを含むか、または使用することができる。

【0186】

図19は、実施形態による、衛星式通信システム600の略図である。実際には、衛星式通信システム600は、軌道上の少なくとも1つの衛星610を備えることができる。簡略にするため、図19には、衛星を1つだけ図示する。図19を参照すると、いくつかの実施形態において、システム600は、1つまたは複数の受信デバイス620と通信する1つまたは複数の衛星610を備える。いくつかの実施形態において、衛星610は、イリジウム衛星コンステレーション内の衛星などの、LEO衛星として実現してもよい。衛星610は、既知の起動で地球を周回し、1つまたは複数のスポットビーム630を、既知のパターンで、地球の表面に送ることができる。各スポットビーム630は、疑似ランダム（PRN）データおよび1つまたは複数の特有のビームパラメータ（例えば、時間、衛星ID、時間バイアス、および衛星軌道データなど）の情報を含むことができる。

10

【0187】

受信デバイス620は、衛星電話もしくは携帯電話などの通信デバイスとして、または通信もしくはコンピューティングデバイス、例えば、パーソナルコンピュータ、ラップトップコンピュータ、もしくは携帯情報端末などのコンポーネントとして、実現することができる。いくつかの実施形態において、受信デバイス（620）は、グローバル測位システム（GPS）と関連して使用されるデバイスと類似する1つまたは複数の位置特定もしくはナビゲーションデバイスもしくはモジュールを備えてもよい。

20

【0188】

図20A、図20B、および図20Cは、実施形態による、衛星式認証システム700の略図である。図20Aを先ず参照すると、いくつかの実施形態において、軌道上の衛星610は、1つまたは複数のスポットビーム630を、地球表面に送る。受信デバイス620は、スポットビームから信号を受信するよう構成することができる。図20Aに示す実施形態において、受信デバイスは、地上に設置されており、減衰環境内で動作している可能性がある。例えば、屋根またはビルなどの物体710は、衛星610と受信デバイスとの間の通信経路の一部を遮断する可能性がある。

30

【0189】

送信器720は、受信デバイス620が受信したデータおよび／または受信デバイス620が生成したデータを、検証器730に送信する。図20Aに示す送信器720は、受信デバイスからのデータを検証器にリレーする無線送信器である。しかしながら、受信デバイス620からのデータを、有線通信システム、無線通信システム、または有線ならびに無線システムの組み合わせを介して送信することができることは、当業者が認識するであろう。検証器730は、受信デバイス620によってスポットビームを介して取得されたデータを使用して、図20Bと同様の一方向認証アプローチを介して認証ユーザであることを検証器730に証明する。

40

【0190】

さらに、図20Bは、受信デバイス620を、空中に置く、例えば、航空機625内に置くことができる構成を示す。図20Bで示す実施形態において、航空機625は、衛星610でアップリンク、例えば、Lバンドアップリンクを維持することができ、航空機内の受信デバイス620が取得したデータを、アップリンクを介して衛星610に送り返すことができる。衛星610は、データを、第2のクロスリンクされた衛星610に送信することができ、そのデータを、検証器730に送信することができる。

40

【0191】

図20Cに示すシステムは、2つ（または、それ以上）のピアデバイス620が、二方向認証技術を実施して、互いに認証することができる実施形態を示す。図20Cを簡単に参照すると、上記のように、軌道上の衛星610は、1つまたは複数のスポットビーム630を、地球表

50

面に送る。第1の受信デバイス620Aは、スポットビームから信号を受信するよう構成することができる。第1の受信デバイス620Aは、上記したようなDiffie-Hellmanアプローチを使用して、スポットビームからのPRNデータを組み込むセキュリティキーを導出するよう構成することができる。

【0192】

PRNデータはまた、第2のデバイス620Bに送信される。いくつかの実施形態において、第2のデバイス620Bは、スポットビーム630の外部にあってもよく、その場合、PRNデータは、第2のデバイス620Bに結合されたコンピューティングデバイス740によって、通信ネットワークを介して送信することができる。コンピューティングデバイス740は、衛星610に通信可能に結合することができる。例えば、限定のためではないが、コンピューティングデバイス740は、通信リンクを介して衛星610に別々に結合されたサーバとしてもよい。コンピュータ740は、衛星610に対する制御ネットワークと関連付けることができ、それにより、スポットビーム630と関連付けられたPRNデータを有することができる。

【0193】

動作中、第1の受信デバイス620Aは、認証データのための要求を開始し、第2の受信デバイス620Bに送信する。第2の受信デバイス620Bとの間の通信リンクは、直接結んでもよいし、または送信ネットワーク720を通じて実現してもよい。第2の受信デバイス620Bは、要求に対して応答し、第1の受信デバイス620Aからの認証データに対する要求をほぼ同時に発行する。第1の受信デバイス620Aは、第2の受信デバイス620Bを認証し、認証データに対する応答を、第2の受信デバイス620Bに、ほぼ同時に発行し、次いで、第1の受信デバイス620Aを認証する。

【0194】

上記のように、第1の受信デバイス620Aと第2の受信デバイス620Bとの間で実施される認証処理は、共有シークレットがスポットビーム630によって送信されたPRNデータの少なくとも一部を備えるDiffie-Hellman交換とすることができる。したがって、図20Cで示すシステムにより、受信デバイス620A、620Bのピア・ツー・ピア認証が可能になる。この二方向認証アプローチは、受信デバイスならびにサーバおよび他のハードウェアアーキテクチャ、または3つ以上のデバイスに拡張することができることを、当業者は認識するであろう。

【0195】

図21Aは、実施形態による、衛星式認証システムを実施するよう適合することができるコンピューティングシステムの略図である。例えば、図20Aおよび図20Bに示す実施形態において、検証器730は、図21Aに示すようなコンピューティングシステムによって実施することができる。図21Aを参照すると、一実施形態において、システム800は、コンピューティングデバイス808およびスクリーン804を有するディスプレイ802、1つまたは複数のスピーカ806、キーボード810、1つまたは複数の他のI/Oデバイス812、ならびにマウス814を含む1つまたは複数の付属入力/出力デバイスを含むことができる。他のI/Oデバイス812は、タッチスクリーン、音声作動入力デバイス、トラックボール、およびシステム800がユーザから入力を受け取ることを可能にする何らかの他のデバイスを含むことができる。

【0196】

コンピューティングデバイス808は、システムハードウェア820およびメモリ830を含み、メモリ830は、ランダム・アクセス・メモリおよび/またはリード・オンリー・メモリとして実現することができる。ファイルストア880は、コンピューティングデバイス808に通信可能に結合することができる。ファイルストア880は、例えば、1つまたは複数のハードドライブ、CD-ROMドライブ、DVD-ROMドライブ、または他の種類のストレージデバイスなどの、コンピューティングデバイス808の内部にあるものとしてすることができる。ファイルストア880はまた、例えば、1つまたは複数の外部ハードドライブ、ネットワーク接続ストレージ、または別個のストレージネットワークなどの、コンピュータ808の外部にあるものとしてもよい。

【0197】

システムハードウェア820は、1つまたは複数のプロセッサ822、少なくとも2つのグラフィックプロセッサ824、ネットワークインターフェース826、およびバスアーキテクチャ828を含むことができる。一実施形態において、プロセッサ822は、Intel Corporation, Santa Clara, California, USAから市販されるIntel（登録商標）Core2 Duo（登録商標）プロセッサとしてもよい。本明細書で使用する場合、「プロセッサ」という用語は、これらに限定されないが、マイクロプロセッサ、マイクロコントローラ、複合命令セットコンピューティング（CISC）マイクロプロセッサ、縮小命令セット（RISC）マイクロプロセッサ、超長命令語（VLIW）マイクロプロセッサ、または他の任意の種類のプロセッサもしくは処理回路などの、任意の種類の計算要素を意味する。

【0198】

グラフィックプロセッサ824は、グラフィックおよび／またはビデオ操作を管理する補助プロセッサとして機能することができる。グラフィックプロセッサ824は、コンピューティングシステム800のマザーボード上に一体化してもよく、またはマザーボード上の拡張スロットを介して結合してもよい。

【0199】

一実施形態において、ネットワークインターフェース826は、イーサネットインターフェースなどの有線インターフェース（例えば、米国電気電子学会／IEEE802.3-2002参照）またはIEEE802.11a、bまたはg対応インターフェースなどの無線インターフェース（例えば、IEEE Standard for IT-Telecommunications and information exchange between systems LAN/MAN--Part II:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4:Further Higher Data Rate Extension in the 2.4 GHz Band, 802.11G-2003参照）とすることができる。無線インターフェースの他の例は、汎用パケット無線サービス（GPRS）インターフェースがある（例えば、Guidelines on GPRS Handset Requirements, Global System for Mobile Communications/GSM Association, Ver.3.0.1, December 2002参照）。

【0200】

バスアーキテクチャ828は、システムハードウェア820のさまざまなコンポーネントを接続する。一実施形態において、バスアーキテクチャ828は、メモリバス、周辺バスもしくは外部バス、および／またはこれらに限定されないが、11ビットバス、業界標準アーキテクチャ（ISA）、マイクロチャネルアーキテクチャ（MSA）、拡張ISA（EISA）、インテリジェント・ドライブ・エレクトロニクス（IDE）、VESAローカルバス（VLB）、周辺構成機器相互接続（PCI）、ユニバーサル・シリアル・バス（USB）、アドバンスド・グラフィック・ポート（AGP）、パーソナル・コンピュータ・メモリ・カード規格協会バス（PCMCIA）、およびスモール・コンピュータ・システム・インターフェース（SCSI）を含む任意のさまざまな利用可能なバスアーキテクチャを使用するローカルバスを含む、いくつかの種類のバスアーキテクチャの1つまたは複数とすることができる。

【0201】

メモリ830は、オペレーティングシステム840を含み、コンピューティングデバイス808の動作を管理することができる。一実施形態において、オペレーティングシステム840は、インターフェースをシステムハードウェア820にもたらすハードウェア・インターフェース・モジュール854を含む。さらに、オペレーティングシステム840は、コンピューティングデバイス808の動作で使用するファイルを管理するファイルシステム850およびコンピューティングデバイス808で実行する処理を管理する処理制御サブシステム852を含むことができる。

【0202】

オペレーティングシステム840は、システムハードウェア820と共に動作して、遠隔供給源からデータパケットおよび／またはデータストリームを送受信することができる1つまたは複数の通信インターフェースを含む（または、管理する）ことができる。さらに、オペレーティングシステム840は、オペレーティングシステム840と、メモリ830に格納されている1つまたは複数のアプリケーションモジュールとの間にインターフェースをもたら

10

20

30

40

50

すシステム・セル・インターフェース・モジュール842を含むことができる。オペレーティングシステム840は、UNIXオペレーティングシステムもしくはその派生システム（例えば、Linux、Solaris、Berkeley Software Distribution (BSD)、Androidなど）もしくはWindows（登録商標）ブランドのオペレーティングシステム、または他のオペレーティングシステムとして実現してもよい。

【0203】

さまざまな実施形態において、コンピューティングデバイス808は、パーソナルコンピュータ、ラップトップコンピュータ、携帯情報端末、携帯電話、エンターテインメントデバイス、または他のコンピューティングデバイスとして実現してもよい。

【0204】

一実施形態において、メモリ830は、認証モジュール862を含み、要求者から受信したデータに基づいて、要求者を認証する。一実施形態において、認証モジュール862は、プロセッサ822によって実行された場合、プロセッサ822に、要求者から受信したデータに基づいて要求者を認証させる、非一時的コンピュータ可読媒体内に符号化された論理命令を含むことができる。さらに、メモリ830は、地球の周囲の所定の軌道にある衛星610に対する軌道情報を含む衛星軌道データベース864を備えることができる。認証モジュール862が実施する認証処理および動作についてのさらなる詳細は、以下で説明する。

【0205】

いくつかの実施形態において、受信デバイス620は、従来のコンピューティングデバイス622（例えば、ラップトップ、PDA、またはスマートフォンデバイス）と結合するよう適合された衛星通信モジュールとして実現してもよい。受信デバイス620は、適切な通信接続によって、例えば、ユニバーサル・シリアル・バス（USB）インターフェース、RS-232インターフェース、または光学インターフェースなどによって、コンピューティングデバイス622に結合することができる。図21Bに示す実施形態において、受信デバイス620は、受信器と、限定処理能力、例えば、認証ルーチンを実施するよう構成される特定用途向け集積回路（ASIC）またはフィールド・プログラマブル・ゲートアレイ（FPGA）を含むことができるという意味で「シン」デバイスとすることができる。

【0206】

動作中、コンピューティングデバイス622のユーザは、受信デバイス620を使用して、ホストネットワーク890でコンピューティングデバイス622を認証することができる。上記のように、図21Bに示す受信デバイス620は、特有のビーム署名および疑似乱数（PRN）を含む、衛星610からのスポットビーム伝送630を受け取ることができる。コンピューティングデバイス622は、ホストネットワーク890へのアクセス要求を開始することができる。アクセス要求は、ユーザの具体的な情報、例えば、ユーザID、地球規模の座標系からの1つまたは複数の座標情報（例えば、郵便番号、地域コード、経度／緯度、万国横メルカトル（UTM）、地球固定（ECEF）、ジョーレフ法（GEOREF）、または他の雑多なシステム、例えば、郵便番号）、および衛星610から受信したPRNデータの少なくとも一部を含むことができる。

【0207】

ホストネットワーク890は、ユーザアクセス要求を、認証要求として、検証器730に送信することができる。いくつかの実施形態において、ホストネットワークは、追加情報を要求に追加し、検証器730がコンピュータ622を認証することを可能にすることができる。例えば、ホストネットワーク890は、要求者をどこで（すなわち、どの地理的箇所から）認証することができるかに関して限定を設けることができる。検証器730は、要求者を検証し、認証要求をホストネットワーク890にもたらしすることができる。次に、ホストネットワーク890は、アクセス要求を、コンピューティングデバイス622に回送することができる。

【0208】

図22は、実施形態による、要求者を認証するための方法における動作を示すフローチャートである。図22を参照すると、動作910で、要求者デバイスは、要求者デバイスの物理的箇所を判断する。いくつかの実施形態において、要求者デバイス620は、1つまたは複数

10

20

30

40

50

の箇所モジュールを備え、要求者デバイス620の箇所を判断することができる。例えば、限定するものではないが、要求者デバイス620は、グローバル測位システム（GPS）モジュールを含むか、または通信可能に結合し、グローバル測位システムからの信号に基づいて、箇所を判断することができる。あるいは、またはさらに、要求者デバイス620は、米国特許第7,489,926号、米国特許第7,372,400号、米国特許第7,579,987号、および米国特許第7,468,696号の1つまたは複数で説明されるような、1つまたは複数のLEOまたはMEO衛星610からの信号に基づいて、箇所を判断するロジックを含むことができ、それらの開示は、参照により各全体が本明細書に組み込まれる。いくつかの実施形態において、要求者デバイス620の箇所は、経度／緯度または他の地球規模座標系で表すことができる。

【0209】

10

動作915では、要求者デバイス620は、衛星610からスポットビーム伝送を受ける。いくつかの実施形態において、要求者デバイス620は、衛星スポットビームからの疑似乱数コードセグメントを含む1つまたは複数の特有のビームパラメータ（例えば、時間、衛星ID、ビームID、時間バイアス、衛星軌道データなど）を抽出する。いくつかの実施形態において、要求者デバイス620は、要求者デバイス620内の、または要求者デバイス620に通信可能に結合したメモリモジュール内に、ビームパラメータを格納することができる。1つまたは複数の実施形態において、動作915は、先行する動作910とほぼ同時に行ってもよい。

【0210】

20

動作920では、要求者デバイス620は、続いて、動作910からの要求者デバイス620に対する箇所情報を含むことができる1つまたは複数の中間地点データスナップショット、および動作920で示すような衛星スポットビームを介して伝送される特有のビームパラメータの1つまたは複数を作成することができる。いくつかの実施形態において、中間地点データスナップショットは、要求者デバイス620内の、または要求者デバイス620に通信可能に結合したメモリモジュール内に格納することができる。

【0211】

いくつかの実施形態において、要求者デバイス620は、ある時間にわたって、中間地点データスナップショットのアレイを収集することができる。例えば、中間地点データスナップショットのアレイは、ある時間にわたって、要求者デバイス620を通過する複数の衛星610からスポットビームを受けることによって構成することができる。あるいは、またはさらに、中間地点データスナップショットのアレイは、衛星610に対して要求者デバイス620を動かすことによって、例えば、図20Bで示すように、航空機625内に要求者デバイス620を設置することによって、構成してもよい。さらなる例には、追跡器の役目を果たし、危険物を含む可能性のある要素または資産の進行ルートを検証する要求者デバイスがある。要求者デバイスは、中間地点データを提供して、予期された経路が実際の経路と整合するかを検証するようポーリングすることができる。要求者デバイスは、ランダムにポーリングしてもよい。

30

【0212】

動作920では、中間地点データスナップショットは、要求者デバイス620から検証器デバイス730に伝送される。例えば、図20Aに示す実施形態において、中間地点データスナップショットは、送信器720を介して、または他の通信ネットワークによって、送信することができる。図20Bに示す実施形態において、中間地点データスナップショットは、航空機625から衛星610に送信することができ、次いで、衛星ネットワークを介して、検証器デバイス730に送信することができる。

40

【0213】

動作925で、検証器デバイス730は、要求者デバイス620から、箇所データおよび中間地点データを受信する。動作930で、検証器デバイス730は、箇所情報および中間地点データと、既知の有効なデータ内の対応データとを比較し、要求者を認証する。例えば、イリジウム衛星コンステレーションなどのLEO衛星は、既知の軌道で地球を周回し、その近似パラメータは、事前に利用可能である。検証器デバイス730は、衛星軌道データベース864を

50

含むか、または衛星軌道データベース864に通信可能に結合され得、衛星軌道データベース864は、地球の周りの既知の軌道にある衛星610についての軌道情報を含む。

【0214】

いくつかの実施形態において、要求者デバイスから受信した箇所データおよび中間地点データは、既知のデータセットからの箇所および中間地点データと比較され（動作930）、要求者デバイス620が、実際に、期待時間で予期した地理的箇所の適度な閾値距離内にあるかどうかを判断する。例えば、限定するものではないが、衛星軌道データベース864は、要求者デバイス620から送信された特有のビームパラメータに対応するデータレコードについて検索され得る。マッチングレコードが見つかり、軌道データベース864から検索されたレコードからの軌道データを、要求者デバイス620から受信したデータと比較することができる。例えば、既知のデータは、スポットビーム630の中心に対する座標および地球の表面上でのスポットビーム630の半径の指示を備えることができる。要求者デバイス620から受信した座標は、スポットビームの箇所と比較され、要求者デバイス620が、要求者デバイスから受信したデータで示される時間にスポットビームによって取り囲まれる領域内にあることを受信データが示すかどうかを判断することができる。少なくとも1つの実施形態において、スポットビームは不規則的な形状である可能性がある。少なくとも1つの実施形態において、要求者デバイスは、地球の表面より高い位置にある可能性がある。

10

【0215】

動作935で、要求者デバイス620が、要求者デバイスからのデータと関連付けられた時間で衛星610からのスポットビームによって取り囲まれる地理的領域内にあると、要求者デバイス620から受信したデータが示す場合、要求者デバイス620は、認証されたと考えることができる。認証システムにおいて、制御は、次いで、動作940に渡され、要求者は、リソースへのアクセスを許可される。例えば、限定するものではないが、検証器デバイス730は、認証された要求者デバイス620に対するトークンを承諾してもよい。トークンは、遠隔システムによって使用され、リソースへのアクセスを承諾することができる。

20

【0216】

対照的に、要求者デバイス620が、要求者デバイス620からのデータと関連付けられた時間で衛星610からのスポットビームによって取り囲まれる地理的領域内にないと、要求者デバイス620から受信したデータが示す場合、要求者デバイス620は、認証されたと考えることができない。認証システムにおいて、制御は、次いで、動作945に渡され、要求者は、リソースへのアクセスを拒否される。例えば、限定するものではないが、検証器デバイス730は、認証された要求者デバイス620に対するトークンを拒否する可能性がある。トークンがない場合、要求者デバイスは、遠隔システムによって管理されたリソースへのアクセスを拒否される可能性がある。

30

【0217】

したがって、図19から図21に示すシステムアーキテクチャおよび図22に示す方法により、1つまたは複数の要求者デバイス620の衛星式認証が可能となる。認証システムを使用して、遠隔コンピューティングシステムによって管理される1つまたは複数のリソースへのアクセスを許可または拒否することができる。いくつかの実施形態において、要求者デバイスは据え置きとすることができ、一方、他の実施形態では、要求者デバイスは移動体とすることができ、認証処理は、時間ベース、箇所ベース、またはその両方の組み合わせのいずれかとすることができる。

40

【0218】

いくつかの実施形態において、本システムを使用して、要求者デバイス620が認証されて、全セッションのためにリソースを使用する、セッションベース認証を実施してもよい。他の実施形態において、本システムは、要求者デバイス620が、要求者デバイス620から遠隔リソースに送信された各メッセージに対して別々に認証されなければならない、メッセージベース認証を実施してもよい。

【0219】

50

1つの例示的実装態様において、本明細書で説明するような認証システムを使用して、企業電子メールシステム、企業ネットワーク、軍用もしくは公共インフラネットワーク、または電子銀行決済設備などの、安全なコンピューティングリソースにアクセスするための認証をもたらすことができる。他の例示的実装態様において、認証システムを使用して、物流管理システムにおける車両の運行ルートを確認することができる。例えば、トラック、列車、船、または航空機などの移動体は、1つまたは複数の要求者デバイス620を備えることができる。スケジュールされた任務中に、物流管理システムは、要求者デバイス620を、周期的にポーリングすることができ、要求者デバイス620は、衛星610から取得した認証データで応答することができる。認証データは、物流管理システムに収集され、要求者デバイスが、物流計画による所定の時間で特定の箇所にあることを確認するために使用することができる。

【0220】

さらに他の例において、本明細書で説明する認証システムの実装態様を使用して、例えば、自宅監禁監視システムなどのモニタリング・システムと関連付けられた要求者デバイスの箇所を検証することができる。そのような実施形態において、要求者デバイスは、指紋生体認証センサなどの1つまたは複数の生体認証センサを組み込み、システムのユーザを認証することができ、一方、認証システムを使用して、要求者デバイスが、所定の時間に所定の箇所にある（すなわち、要求者が、適切な時間に適切な場所にあり、適切な人間である）ことを確認することができる。認証デバイスはまた、承認された期間に箇所の承認されたセットに対して要求者デバイスの箇所および時間を再調査することによって、認証システムによってさらに改良され得る承認された箇所の定義リストに対して、要求者デバイス箇所を再調査してもよい。さらに、このシステムを使用して、登録された性犯罪者を追跡することができる。

【0221】

いくつかの実施形態において、衛星610は、既知の軌道で地球を周回し、さらに既知の形状を有するスポットビームを送信する、イリジウムコンステレーションなどのLEO衛星システムの一部とすることができ、要求者デバイスが所定の時間に指定されたスポットビーム内にあることを確認することによって、要求者デバイスを認証することができる。したがって、要求者は、単一信号供給源（例えば、単一の衛星610）を使用して、認証することができる。また、イリジウムコンステレーションおよびMEO衛星などのLEO衛星は、比較的高出力信号レベルを送信するので、本システムを使用して、屋内または都会などの遮断環境に位置する1つまたは複数の要求者デバイスを認証することができる。また、LEO衛星およびMEO衛星の比較的高い信号強度により、これらの信号が、電波妨害の影響を受けにくくする。

【0222】

ある種の例示的実施形態および方法を本明細書で開示してきたが、そのような実施形態および方法の変更および変形は、開示する技術の主旨および範囲から逸脱せずに行うことができることが、当業者には上記開示から明らかであろう。開示する技術の他の多くの例が存在し、それぞれ、細部の事項のみが他と異なる。したがって、開示する技術は、添付の特許請求の範囲および準拠法の規則ならびに原理によって求められる範囲のみに限定されることが意図される。

【符号の説明】

【0223】

- 20 ネットワークトラフィック／パケット
- 22 パケット取得ツール
- 24 ヘッダ取得ツール
- 26 アルゴリズム
- 28 署名
- 30 セキュリティイベント
- 32 ログビューワツール

34	フィルタ	
36	正規化されたフィルタ済みイベント	
38	相関関係	
40	相関関係インスタンス	
42	エスカレータ	
44	アナリスト	
46	警告	
48	知識ログ	
50	問題ログ	
52	インシデントログ	10
100	システム	
110	衛星	
120	デバイス	
130	測位ハードウェア	
140	セルタワー	
150	衛星スポットビーム	
160	信号／スマート・エージェント・ダウンロード	
170	ネットワーク	
200	フロー図	
300	概略図	20
310	要求者	
320	要求者（なりすまし人）	
330	ネットワークノード	
340	ネットワークノード	
350	ネットワーク・オペレーション・センター（NOC）	
360	セルタワー	
400	グラフ	
410	ノード	
420	時間	
430	通常のトラフィック動作レベル	30
440	ノード異常	
500	メッシュ状物理的フレームワーク	
510	論理トポロジー	
520	物理トポロジー	
530	衛星	
540	汚染ネットワークノード	
550	ルータ	
570	ネットワーク	
580	リレー衛星	
600	衛星式通信システム	40
610	衛星	
620	受信デバイス／要求者デバイス	
620A	第一の受信デバイス	
620B	第二の受信デバイス	
622	コンピューティングデバイス	
625	航空機	
630	スポットビーム	
700	衛星式認証システム	
710	物体	
720	送信器	50

730	検証器	
740	コンピューティングデバイス	
800	コンピューティングシステム	
802	ディスプレイ	
804	スクリーン	
806	スピーカ	
808	コンピューティングデバイス	
810	キーボード	
812	I/Oデバイス	
814	マウス	10
820	システムハードウェア	
822	プロセッサ	
824	グラフィックプロセッサ	
826	ネットワークインターフェース	
828	バスアーキテクチャ	
830	メモリ	
840	オペレーティングシステム	
842	システム・セル・インターフェース・モジュール	
850	ファイルシステム	
852	処理制御サブシステム	20
854	ハードウェア・インターフェース・モジュール	
862	認証モジュール	
864	衛星軌道データベース	
880	ファイルストア	
890	ホストネットワーク	
1000	システム	
1100	衛星	
1200	デバイス	
1300	測位ハードウェア	
1400	セルタワー	30
1500	衛星スポットビーム	
1600	信号／スマート・エージェント・ダウンロード	
1700	ネットワーク	
3000	概略図	
3010	フォレンジック・データ・コレクタ (FDC)	
3020	セキュリティ・ユーティリティ・サーバ (SUS)	
3030	イベント関連エンジン (ECE)	
3040	ネットワーク管理システム (NMS)	
3050	ネットワーク・オペレーション・センター (NOC)	
5000	システム	40
5010	ユーザ	
5020	ユーザ	
5030	対応デバイス	
5040	対応デバイス	
5050	スポットビーム	
5060	衛星	
5070	セルタワー	
7000	トポロジー図	
7010	メッシュ型物理的フレームワーク	
7020	論理トポロジー	50

7030	物理トポロジー	
7030	ネットワーク	
7040	衛星	
7050	位置認証対応ルータ	
7060	位置認証対応ルータ	
7070	位置認証対応ルータ	
7080	デバイス	
7090	デバイス	
8000	概略図	
8010	ノード	10
8020	ノード	
8030	ノード	
8040	ノード	
8050	下流のローカルノード	
8060	下流のローカルノード	
8070	下流のローカルノード	
8080	下流のローカルノード	
8090	ネットワーク・ポリシー・サーバ (NPS)	
8090	ネットワーク・ポリシー・サーバ (NPS)	
9000	概略図	20
11000	ブロック図	
11010	警告	
11020	不良	
11030	良好	
11040	プロファイル	
11050	ローカル／ピアノード	
11060	ローカルネットワーク	
11070	ノード1	
12000	ブロック図	
12010	警告	30
12020	ネットワーク管理要素 (NME)	
12030	ノード2	
12040	ノード3	
12050	ローカルユーザ	
12050	ノード1	
13000	概略図	
13010	ラップトップコンピュータ	
13030	イリジウム衛星	
13040	スマートエージェント	
13050	下流ノード	40

【図 1】

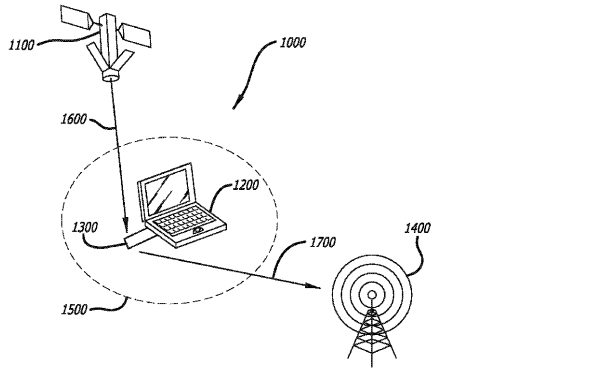
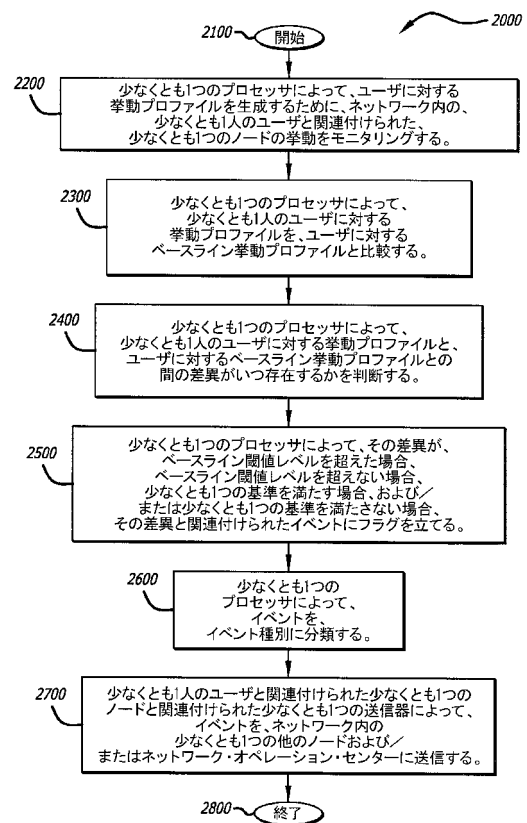
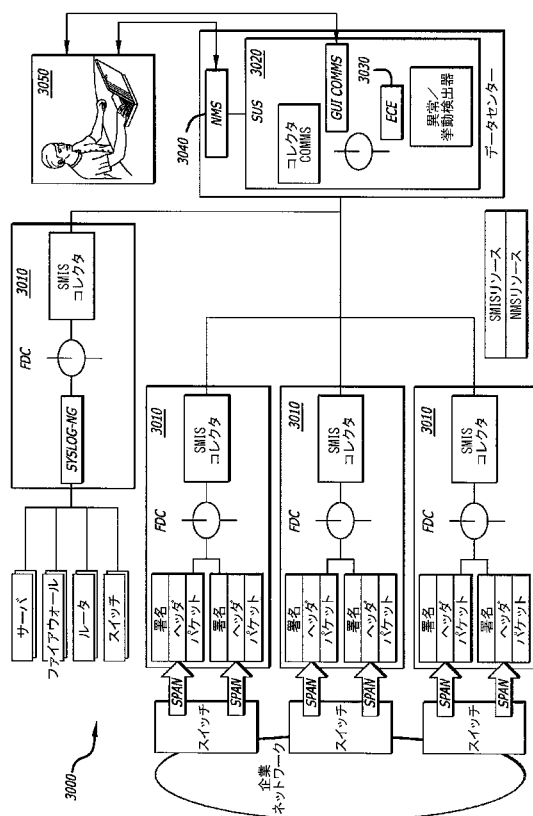


FIG. 1

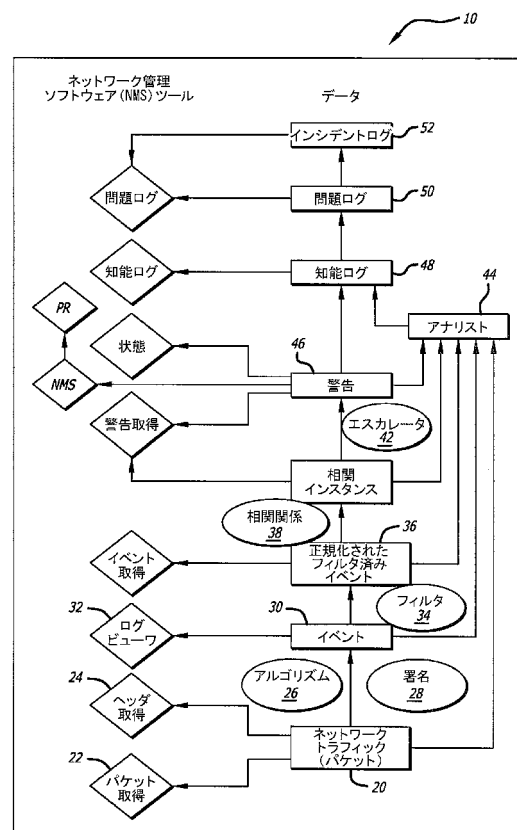
【図 2】



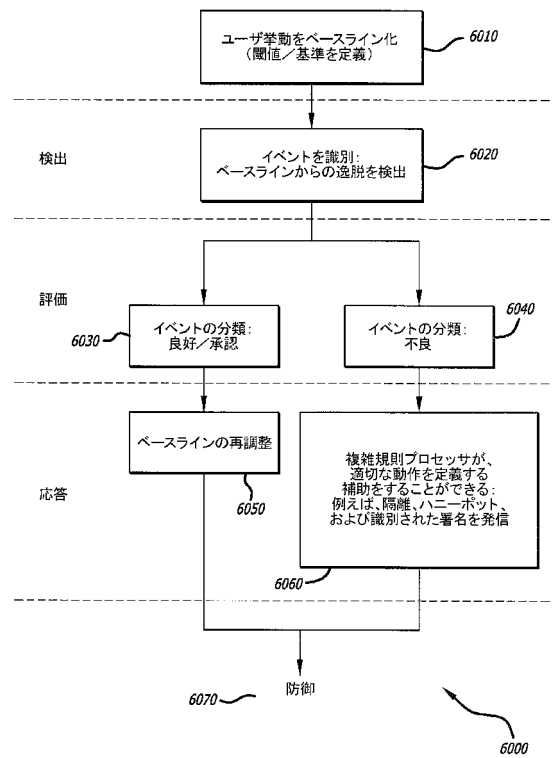
【図 3】



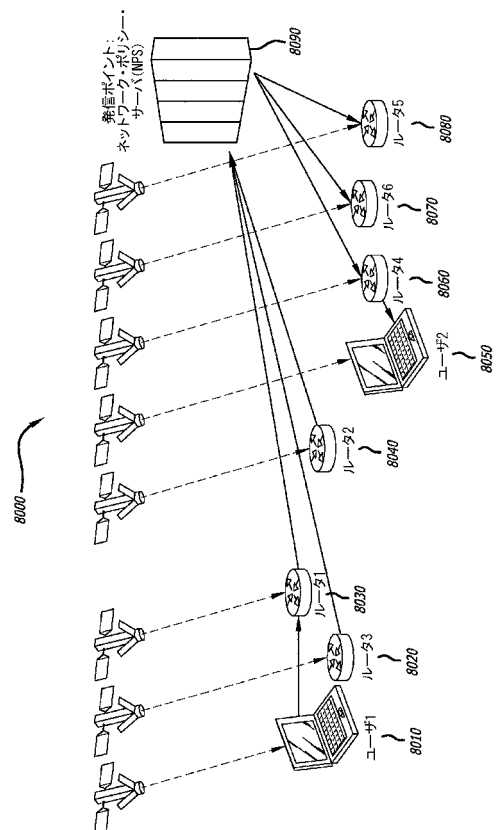
【図 4】



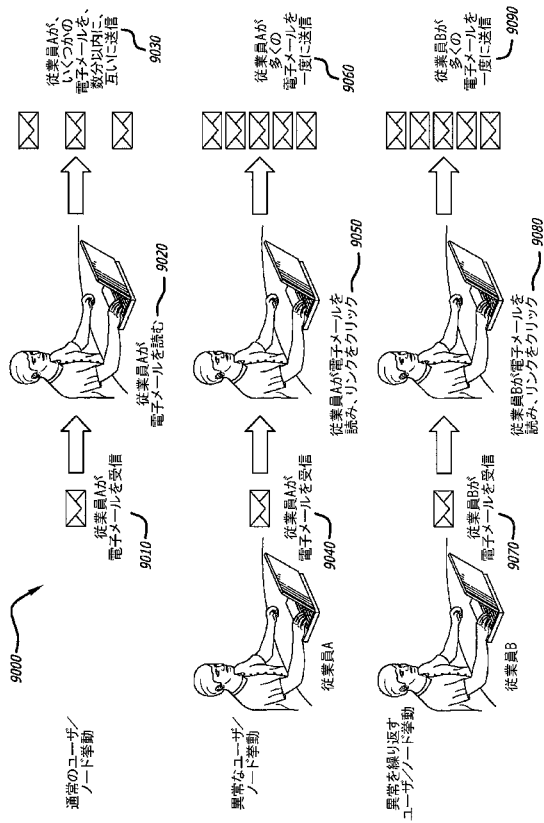
【図 6】



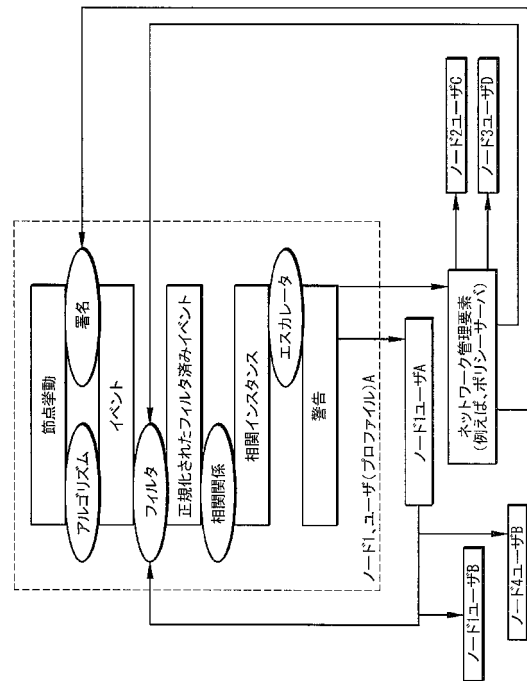
【図 8】



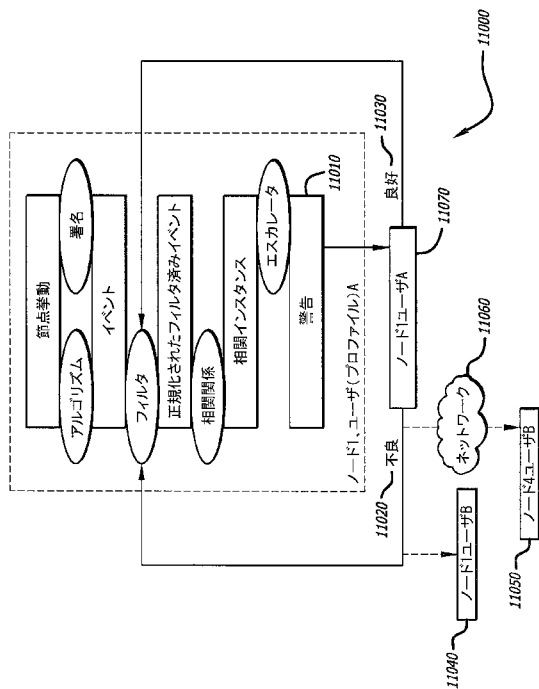
【図 9】



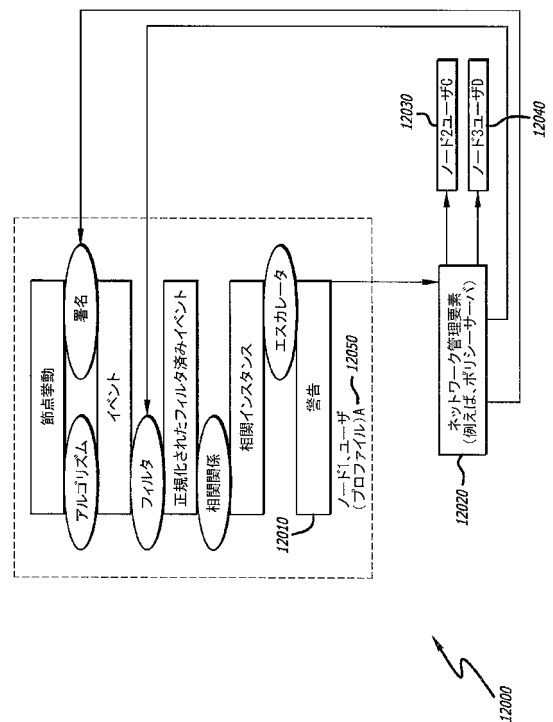
【図 10】



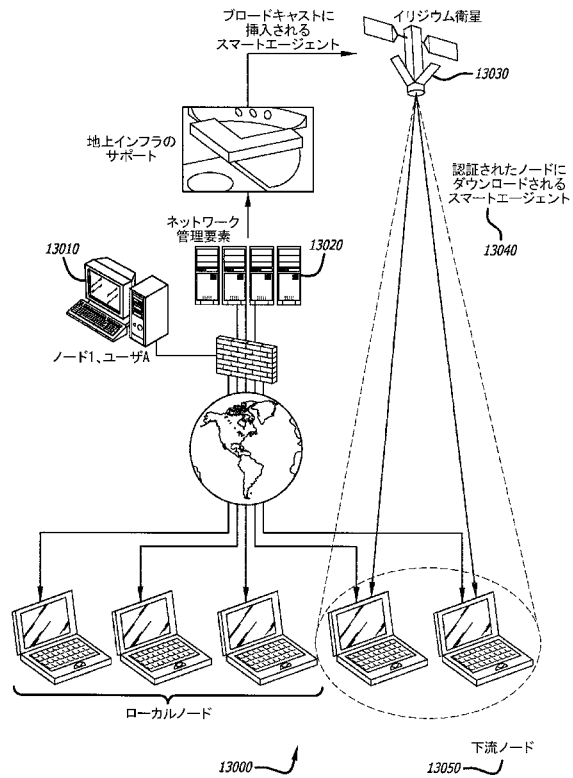
【図 11】



【図 12】



【図 13】



【図 14】

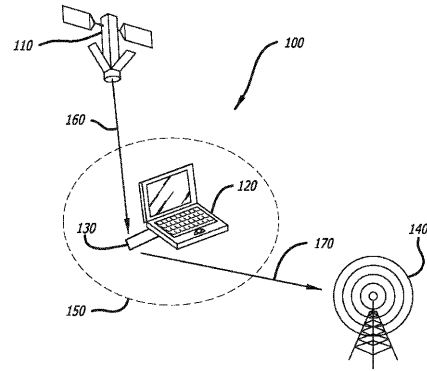
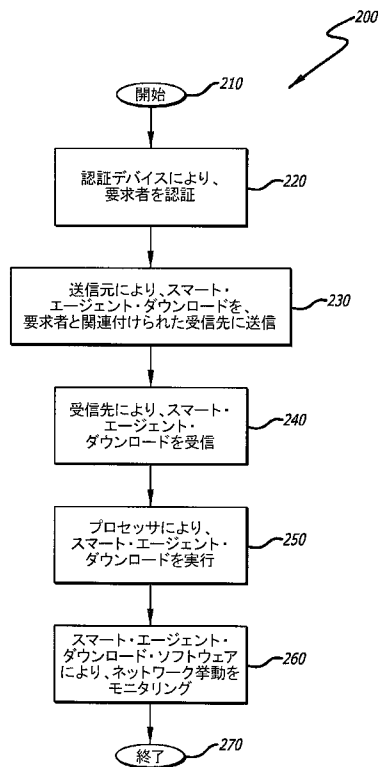


FIG. 14

【図 15】



【図 16】

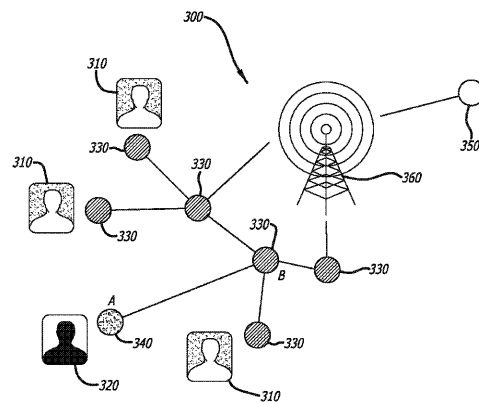
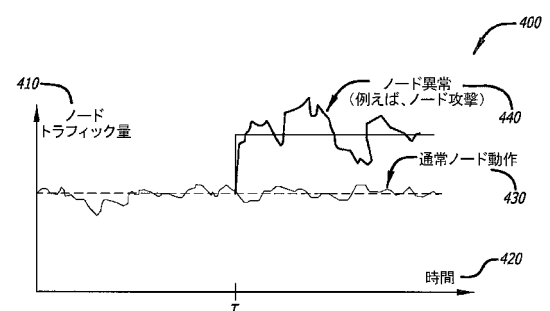
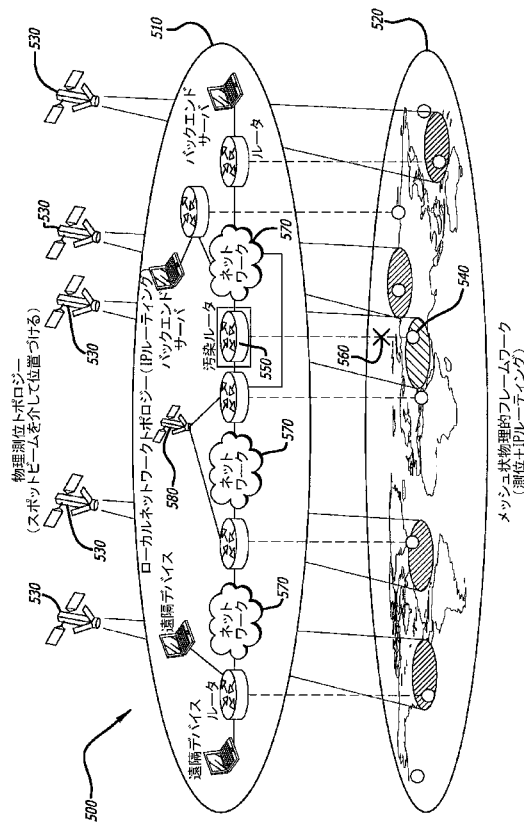


FIG. 16

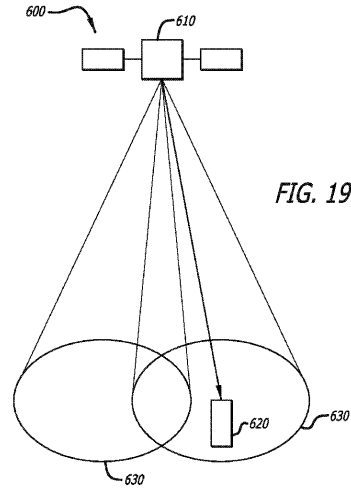
【図 17】



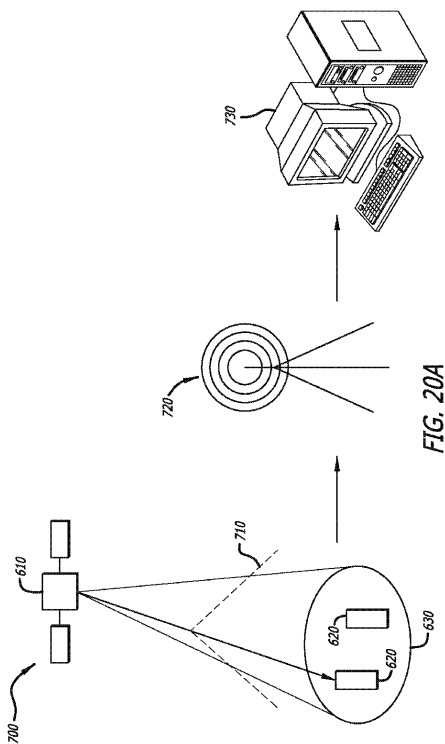
【 図 1 8 】



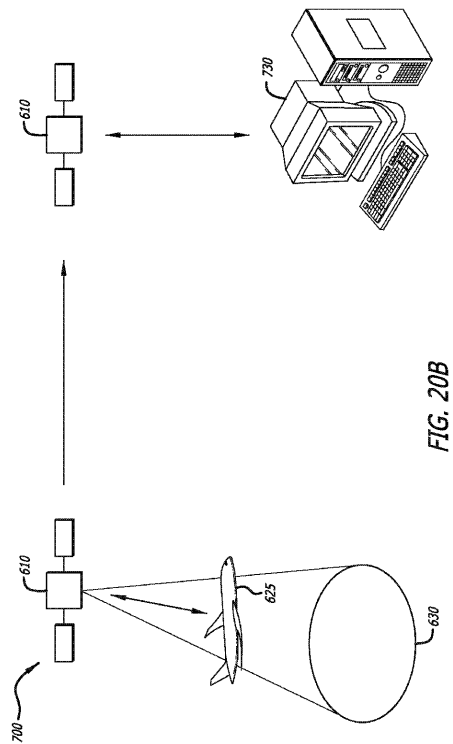
【 図 1 9 】



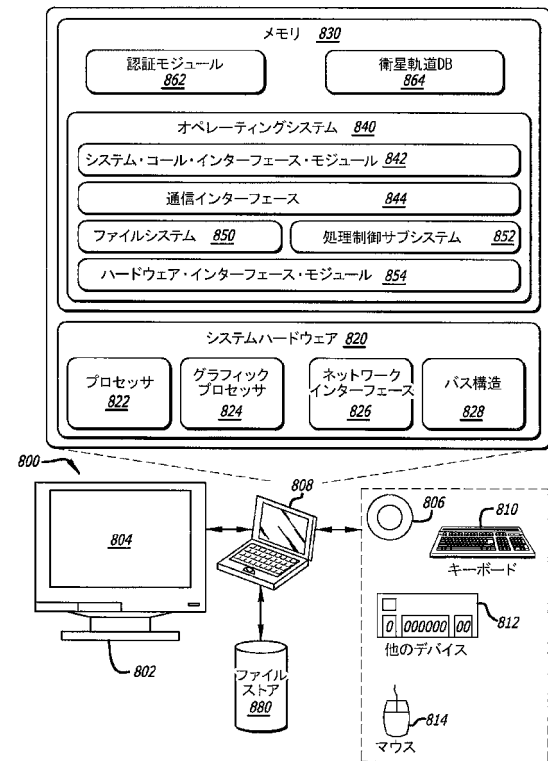
【 図 2 0 A 】



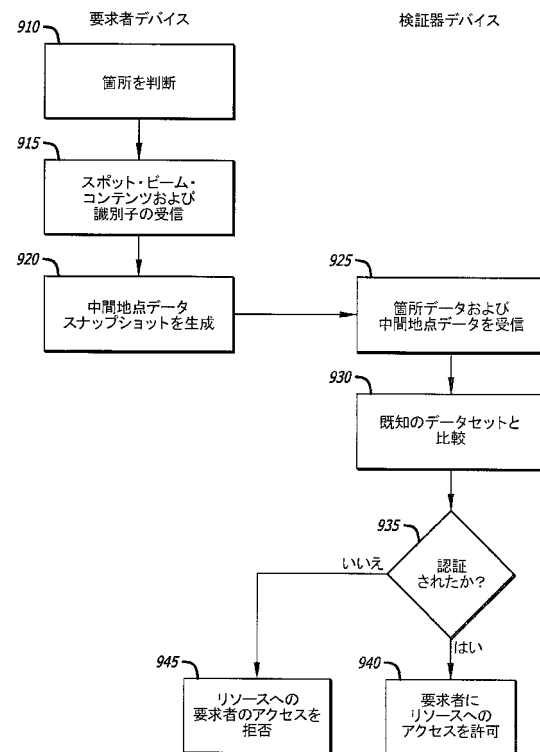
【図 2 0 B】



【図 2 1 A】



【图 2 2】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/072388

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L29/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CA 2 531 410 A1 (SNIPE NETWORK SECURITY CORP [CA]) 23 June 2007 (2007-06-23) abstract page 1, line 25 - line 26 page 2, line 1 - page 3, line 24 page 4, line 5 - line 19 page 4, line 27 - page 5, line 1 page 5, line 6 - line 7 page 5, line 12 - line 13 page 6, line 1 - line 8 page 6, line 22 page 6, line 27 - line 29 page 7, line 3 - line 9 page 7, line 15 - line 17 ----- -/--	1-27

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

26 February 2014

Date of mailing of the international search report

05/03/2014

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax (+31-70) 340-3016

Authorized officer

Oliveira, Joel

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2013/072388

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GARCIA-TEODORO P ET AL: "Anomaly-based network intrusion detection: Techniques, systems and challenges", COMPUTERS & SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 28, no. 1-2, 1 February 2009 (2009-02-01), pages 18-28, XP025839371, ISSN: 0167-4048, DOI: 10.1016/J.COSE.2008.08.003 [retrieved on 2008-08-27] page 18, column 2, line 13 - page 19, column 1, line 5 page 19, column 1, line 21 - line 32 page 19, column 2, line 29 - line 39 page 20, column 1, line 8 - line 11 page 20, column 1, line 17 - column 2, line 2 Section 2.3 Machine learning-based A-NIDS schemes -----	1-27

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2013/072388

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
CA 2531410	A1	23-06-2007	CA 2531410 A1
		US 2007245420 A1	23-06-2007
			18-10-2007

フロントページの続き

(81)指定国 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US

(特許庁注：以下のものは登録商標)

1. B L U E T O O T H
2. Z I G B E E
3. F A C E B O O K
4. イーサネット
5. U N I X
6. L i n u x
7. A N D R O I D

- (72)発明者 アルン・アヤガリ
アメリカ合衆国・イリノイ・60606-2016・シカゴ・ノース・リヴァーサイド・プラザ・
100・ザ・ボーイング・カンパニー
- (72)発明者 ティモシー・エム・アルドリッチ
アメリカ合衆国・イリノイ・60606-2016・シカゴ・ノース・リヴァーサイド・プラザ・
100・ザ・ボーイング・カンパニー
- (72)発明者 デイヴィッド・イー・コーマン
アメリカ合衆国・イリノイ・60606-2016・シカゴ・ノース・リヴァーサイド・プラザ・
100・ザ・ボーイング・カンパニー
- (72)発明者 グレゴリー・エム・グート
アメリカ合衆国・イリノイ・60606-2016・シカゴ・ノース・リヴァーサイド・プラザ・
100・ザ・ボーイング・カンパニー
- (72)発明者 デイヴィッド・エー・ウィーラン
アメリカ合衆国・イリノイ・60606-2016・シカゴ・ノース・リヴァーサイド・プラザ・
100・ザ・ボーイング・カンパニー

Fターム(参考) 5B089 GA11 GA32 GB02 KA17