(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5816375号
(P5816375)
(45)発行日　平成27年11月18日(2015.11.18)　(24)登録日　平成27年10月2日(2015.10.2)

(51)Int.Cl.　F I
G06F 21/55 (2013.01)　G06F 21/55 340
G06F 21/55 320

請求項の数 22　(全 12 頁)

(21)出願番号	特願2014-530908 (P2014-530908)
(86)(22)出願日	平成24年9月14日 (2012.9.14)
(65)公表番号	特表2014-530419 (P2014-530419A)
(43)公表日	平成26年11月17日 (2014.11.17)
(86)国際出願番号	PCT/US2012/055630
(87)国際公開番号	WO2013/040496
(87)国際公開日	平成25年3月21日 (2013.3.21)
審査請求日	平成26年4月21日 (2014.4.21)
(31)優先権主張番号	13/233,497
(32)優先日	平成23年9月15日 (2011.9.15)
(33)優先権主張国	米国(US)

(73)特許権者　505418238
マカフィー，　インコーポレイテッド
アメリカ合衆国、９５０５４　カリフォルニア州、サンタ　クララ、ミッション　カレッジ　ブールバード　２８２１
(74)代理人　110000877
龍華国際特許業務法人
(72)発明者　ブ、ジェン
アメリカ合衆国、９５０５４　カリフォルニア州、サンタ　クララ　ミッション　カレッジ　ブーレバード　２８２１　マカフィー、インコーポレイテッド内

最終頁に続く

(54)【発明の名称】脅威に対してリアルタイムでカスタマイズされた保護を行う方法、ロジック及び装置

(57)【特許請求の範囲】
【請求項１】
ネットワーク環境全体にわたって分散された複数のセンサーからの複数のレポートに関連する複数のイベント情報を脅威インテリジェンスクラウドで受信することと、
脅威を特定するように前記複数のイベント情報をイベント解析サブクラウドで相関付けることと、
前記脅威に基づいて前記複数のセンサーのそれぞれに、カスタマイズされたセキュリティポリシーを前記イベント解析サブクラウドから送出することと、
を含む、方法。
【請求項２】
前記脅威に基づいて前記脅威インテリジェンスクラウドがレピュテーションシステムにレピュテーションデータを送出することを更に含む、請求項１に記載の方法。
【請求項３】
前記脅威に基づいて前記脅威インテリジェンスクラウドがレピュテーションデータを受信することを更に含む、請求項１または２に記載の方法。
【請求項４】
前記複数のセンサーは、複数の侵入防止システムを備える、請求項１～３のいずれか１項に記載の方法。
【請求項５】
前記カスタマイズされたセキュリティポリシーは、前記脅威に感染したホストを隔離す

る、請求項１～４のいずれか１項に記載の方法。
【請求項６】
新しい前記脅威に基づいて前記脅威インテリジェンスクラウドがレピュテーションデータを受信することを更に含み、前記複数のセンサーは複数の侵入防止システムを備え、前記カスタマイズされたセキュリティポリシーは、前記新しい脅威に感染したホストを隔離する、請求項１に記載の方法。
【請求項７】
前記ネットワーク環境が有する複数のローカルネットワークに配置された前記複数のセンサーのそれぞれが、ローカルに調節されたポリシーを使用して前記複数のローカルネットワークのそれぞれのニーズに基づいて前記脅威に対する保護を提供すること、を更に含む、請求項１～６のいずれか１項に記載の方法。
【請求項８】
前記相関付けることは、特定の国、領域または業界内に設けられた前記複数のセンサーによってレポートされる前記複数のイベント情報を相関付けることによって、前記特定の国、領域または業界を標的とする脅威を特定することを含む、請求項１～７のいずれか１項に記載の方法。
【請求項９】
前記脅威は、グローバルな脅威を含む、請求項１～８のいずれか１項に記載の方法。
【請求項１０】
１つ又は複数の非一時的媒体内で符号化されるロジックであって、実行用のコードを含み、１つ又は複数のプロセッサによって実行されると、オペレーションであって、
ネットワーク環境全体にわたって分散された複数のセンサーからの複数のレポートに関連する複数のイベント情報を受信することと、
脅威を特定するように前記複数のイベント情報を相関付けることと、
前記脅威に基づいて前記複数のセンサーのそれぞれに、カスタマイズされたセキュリティポリシーを送出することと、
を含む、オペレーションを実施するように働く、ロジック。
【請求項１１】
前記オペレーションは、前記脅威に基づいてレピュテーションシステムにレピュテーションデータを送出することを更に含む、請求項１０に記載のロジック。
【請求項１２】
前記オペレーションは、前記脅威に基づいて脅威インテリジェンスクラウドにレピュテーションデータを送出することを更に含む、請求項１０に記載のロジック。
【請求項１３】
前記複数のセンサーは、複数の侵入防止システムを備える、請求項１０～１２のいずれか１項に記載のロジック。
【請求項１４】
前記カスタマイズされたセキュリティポリシーは、前記脅威に感染したホストを隔離する、請求項１０～１３のいずれか１項に記載のロジック。
【請求項１５】
前記複数のイベント情報は、脅威インテリジェンスクラウドから受信される、請求項１０～１４のいずれか１項に記載のロジック。
【請求項１６】
１つ又は複数のプロセッサを備える装置であって、
前記１つまたは複数のプロセッサがイベント解析サブクラウドに関連する命令を実行するように動作すると、前記装置は、
ネットワーク環境全体にわたって分散された複数のセンサーからの複数のレポートに関連する複数のイベント情報を受信し、
脅威を特定するように前記複数のイベント情報を相関付け、
前記脅威に基づいて前記複数のセンサーのそれぞれに、カスタマイズされたセキュリ

ティポリシーを送出するように構成される、装置。
【請求項１７】
前記脅威に基づいてレピュテーションシステムにレピュテーションデータを送出するように更に構成される、請求項１６に記載の装置。
【請求項１８】
前記脅威に基づいて脅威インテリジェンスクラウドにレピュテーションデータを送出するように更に構成される、請求項１６に記載の装置。
【請求項１９】
前記複数のセンサーは、複数の侵入防止システムを備える、請求項１６～１８のいずれか１項に記載の装置。
【請求項２０】
前記カスタマイズされたセキュリティポリシーは、前記脅威に感染したホストを隔離する、請求項１６～１９のいずれか１項に記載の装置。
【請求項２１】
前記複数のイベント情報は、脅威インテリジェンスクラウドから受信される、請求項１６～２０のいずれか１項に記載の装置。
【請求項２２】
脅威インテリジェンスクラウドと、
イベント解析サブクラウドと、
１つ又は複数のプロセッサと
を備える装置であって、
前記１つ又は複数のプロセッサが前記脅威インテリジェンスクラウド及び前記イベント解析サブクラウドに関連する命令を実行するように動作すると、
前記脅威インテリジェンスクラウドは、ネットワーク環境全体にわたって分散された複数のセンサーからの複数のレポートに関連する複数のイベント情報を受信するように構成され、
前記イベント解析サブクラウドは、脅威を特定するように前記複数のイベント情報を相関付け、前記脅威に基づいて前記複数のセンサーのそれぞれに、カスタマイズされたセキュリティポリシーを送出するように構成される装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本明細書は、包括的に、ネットワークセキュリティの分野に関し、より詳細には、カスタマイズされたリアルタイムの脅威保護のシステム及び方法に関する。
【背景技術】
【０００２】
情報システムが、世界的規模で人々及び事業者の日常生活に統合されてきており、情報セキュリティの分野が、また、今日の社会において益々重要になってきた。こうした広範囲にわたる統合は、同様に、悪意のあるオペレーターがこれらのシステムを悪用する多くの機会を提示してきた。悪意のあるソフトウェアがホストコンピューターを感染させることができる場合、悪意のあるソフトウェアは、ホストコンピューターからスパム又は悪意のあるｅメールを送出すること、ホストコンピューターに関連する事業者又は個人から機密情報を盗むこと、他のホストコンピューターに伝搬させること、及び／又は、分散してサービス妨害の攻撃を支援すること等、任意の数の悪意のある行為を実施し得る。さらに、幾つかのタイプのマルウェアの場合、悪意のあるオペレーターは、他の悪意のあるオペレーターにアクセス権を売るか又はその他の方法で与えることができ、それにより、ホストコンピューターの悪用をエスカレートさせる。そのため、安定したコンピューター及びシステムを効果的に保護し維持する能力は、コンポーネント製造業者、システム設計者、及びネットワークオペレーターにとって重大な課題を提示し続ける。
【発明の概要】

【０００３】
本開示並びに本開示の特徴及び利点のより完全な理解を提供するために、添付図面に関連して以下の説明に対して参照が行われる。添付図面では、同様の参照番号は同様の部分を示す。
【図面の簡単な説明】
【０００４】
【図１】本明細書による、カスタマイズされたリアルタイムの脅威保護のためのネットワーク環境の例示的な実施形態を示す略ブロック図である。
【０００５】
【図２】ネットワーク環境に関連することができる、考えられるオペレーションの略相互作用図である。
【０００６】
【図３】ネットワーク環境に関連することができる、考えられるオペレーションの略流れ図である。
【発明を実施するための形態】
【０００７】
概要
ネットワーク環境全体にわたって分散されたセンサーからの、レポートに関連するイベント情報を受信すること、及び、脅威を特定するためにイベント情報を相関付けることを含む方法が、１つの例示的な実施形態において提供される。カスタマイズされたセキュリティポリシーを、脅威に基づいてセンサーに送出することができる。より特定の実施形態では、イベント情報を、脅威インテリジェンスクラウドから受信することができる。更に他の実施形態では、レピュテーションデータを、同様に、脅威に基づいて脅威インテリジェンスクラウドに送出することができる。
【０００８】
例示的な実施形態
図１を考えると、図１は、カスタマイズされたリアルタイムの脅威保護のシステム及び方法をそこで実装することができるネットワーク環境１０の例示的な実施形態の略ブロック図である。ネットワーク環境１０は、脅威インテリジェンスクラウド１５、イベント解析サブクラウド２０、センサー２５ａ～センサー２５ｃ、及びホスト３０ａ～ホスト３０ｉを含む。センサー２５ａ～センサー２５ｃは、例えば、ファイル、ウェブ、メッセージを含む脅威ベクトル及びネットワーク脅威ベクトルに関するホスト３０ａ～ホスト３０ｉからの情報を集めるためにネットワーク環境１０全体にわたって分散された侵入防止システム、ゲートウェイアプライアンス、ファイアウォール、アンチウィルスソフトウェア、及び／又は他のセキュリティシステムを含むことができる。脅威インテリジェンスクラウド１５は、一般に、センサー２５ａ～センサー２５ｃから情報を受信し、その情報から導出されるリアルタイムレピュテーションベースの脅威インテリジェンスを送出するためのインフラストラクチャーを示す。イベント解析サブクラウドは、脅威インテリジェンスクラウド１５によって受信される情報を解析するためのインフラストラクチャーを示し、脅威情報更新及びポリシー構成更新をセンサー２５ａ～センサー２５ｃ及び／又はホスト３０ａ～ホスト３０ｉに提供できる更新サービス３５を提供することもできる。
【０００９】
図１の要素のそれぞれを、簡単なネットワークインターフェースを通して、又は、ネットワーク通信用の実行可能な経路を提供する任意の他の適した接続（有線又は無線）を通して互いに結合することができる。さらに、これらの要素の任意の１つ又は複数を、特定の構成ニーズに基づいて組み合わせるか又はアーキテクチャから除去することができる。ネットワーク環境１０は、ネットワークにおけるパケットの送信又は受信のための伝送制御プロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）通信が可能な構成を含むことができる。ネットワーク環境１０はまた、ユーザーデータグラムプロトコル／ＩＰ（ＵＤＰ／ＩＰ）、又は、適切である場合及び特定のニーズに基づいて、任意の他の適したプロ

トコルと連携して動作することができる。

【００１０】

図１のオペレーション及びインフラストラクチャーを詳述する前に、ネットワーク環境１０内で起こる場合がある幾つかのオペレーションの概要を提供するために、或る特定の文脈情報が提供される。こうした情報は、ひたすらまた教示のためだけに提供され、したがって、いずれの点でも本開示の幅広いアプリケーションを制限すると解釈されるべきでない。

【００１１】

典型的なネットワーク環境は、例えば、インターネットに接続されるサーバーによってホストされるウェブページにアクセスするため、電子メール（すなわち、ｅメール）メッセージを送受信するため、又は、インターネットに接続されるエンドユーザー又はサーバーとファイルを交換するために、インターネットを使用して他のネットワークと電子的に通信する能力を含む。ユーザーは、通常、ネットワーク環境に記憶されるデータが、容易に利用可能であるが、不正アクセスからセキュアであると期待する。ユーザーはまた、通常、通信が、信頼性があり、不正アクセスからセキュアであると期待する。しかし、悪意のあるユーザーは、通常のオペレーションに干渉し、機密情報にアクセスするための新しい方策を絶えず開発している。ウィルス、トロイの木馬（Trojan）、ワーム、ボット、及び他のマルウェアは、ネットワーク又はシステム内の脆弱性を悪用するために使用される手段の一般的な例であるが、不正アクセス、データの破壊、データの漏洩、データの改ざん及び/又はサービス妨害を通した、コンピューター又はネットワークの通常オペレーションに干渉するように設計された任意のアクティビティーは、「脅威」である。

【００１２】

ファイアウォール、侵入防止システム、ネットワークアクセス制御、及びウェブフィルタリングを含む幅広い範囲の対抗策が脅威に対して配備され得る。例えば侵入検出及び防止システム（ＩＤＰＳ：intrusion detection and prevention system）としても知られる侵入防止システム（ＩＰＳ：intrusion prevention system）は、悪意のある又はおそらく悪意のあるアクティビティーについてネットワークアクティビティー及び／又はシステムアクティビティーを監視し、警告を送出し得る。しかし、ＩＰＳ警告は、常に作動可能とすることができない。適した信頼度で攻撃を特定するのに単一イベントが十分でない場合があるため、たとえ観測されるイベントが悪意のあるアクティビティーを示しても、多くの警告は、警戒情報又は指針を提供するだけである。

【００１３】

ＩＰＳは、通常、パケットをドロップすること、接続をリセットすること、及び／又はソースからのトラフィックを遮断すること等によって、検出された侵入を積極的に遮断することができるようにインラインで設置される。ＩＰＳは、アプリケーション及びプロトコル異常検出アルゴリズム、シェルコード検出アルゴリズム、並びにシグネチャーを含む複数の検出方法を使用し得る。例えば、シグネチャーベース検出は、一般に、脅威を特定するために、シグネチャー（すなわち、既知の脅威に対応する任意のパターン）を、観測されるイベント又はアクティビティーと比較することを含む。例示的なシグネチャーは、ルートユーザーとしてリモート接続を確立する試みである。別の例は、既知の形態のマルウェアに特有のサブジェクトライン及びアタッチファイルを有するｅメールを受信することである。

【００１４】

シグネチャーベース検出は、既知の脅威を検出するときに非常に効果的であり得るが、未知の脅威又は更に既知の脅威の僅かな変形を検出するときに非効果的であり得る。さらに、ＩＰＳシグネチャーは、普遍的であり、ローカル環境についてカスタマイズされない傾向がある。脅威は、グローバルな視点なしで、ローカルに見られることができるだけである。グローバルに配備されるセンサーから収集される知識は、一般に、ローカルセキュリティポリシーを改善するためにレバレッジをかけることができない。ポリシーに対する手作業の調整もまた、しばしば必要とされ、感染が蔓延することを可能にするのに十分な

遅延を引き起こす場合がある。

【００１５】

本明細書で述べる実施形態によれば、ネットワーク環境１０は、グローバル脅威インテリジェンスとローカル脅威インテリジェンスとを相関付け、カスタマイズされたセキュリティポリシーを提供するシステム及び方法を提供することによって、これらの欠点（及び他の欠点）を克服し得る。

【００１６】

再び例証のための図１を参照すると、ホスト３０ａ～ホスト３０ｉは、ネットワーク要素とすることができ、ネットワーク要素は、ネットワークアプライアンス、サーバー、ルーター、スイッチ、ゲートウェイ、ブリッジ、負荷バランサー、ファイアウォール、プロセッサ、モジュール、又は、ネットワーク環境内で情報を交換するように働く、任意の他の適したデバイス、コンポーネント、要素、若しくはオブジェクトを包含するものとする。ネットワーク要素は、そのオペレーションを容易にする、任意の適したハードウェア、ソフトウェア、コンポーネント、モジュール、インターフェース、又はオブジェクトを含むことができる。これは、データ又は情報の効果的な交換を可能にする適切なアルゴリズム及び通信プロトコルを包含するものとすることができる。ホスト３０ａ～ホスト３０ｉは、デスクトップコンピューター、ラップトップ、又はモバイル通信デバイス（例えば、ｉＰｈｏｎｅ（登録商標）、ｉＰａｄ（登録商標）、Ａｎｄｒｏｉｄデバイス等）等の他の有線ネットワークノード又は無線ネットワークノードを示すものとすることもできる。

【００１７】

脅威インテリジェンスクラウド１５は、一実施形態においてはレピュテーションシステムであり、分散ファイルシステムクラスターとして実装することができる。一般に、レピュテーションシステムは、アクティビティーを監視し、その過去の挙動に基づいてエンティティにレピュテーション値又はスコアを割り当てる。レピュテーション値は、有益なものから悪意のあるものまでのスペクトルに対する異なるレベルの信頼性を示すことができる。例えば、接続レピュテーション値（例えば、最小リスク、未検証の高リスク等）を、アドレスによって行われる接続に基づくネットワークアドレス又はアドレスから発信するｅメールについて計算することができる。接続レピュテーションシステムは、悪意のあるアクティビティーに関連することが分かっているか又はその可能性があるｅメール若しくはＩＰアドレスによるネットワーク接続を拒否するために使用することができ、一方、ファイルレピュテーションシステムは、悪意のあるアクティビティーに関連することが分かっているか又はその可能性があるハッシュを有するファイル（例えば、アプリケーション）のアクティビティーを阻止し得る。脅威インテリジェンスクラウド１５は、ネットワーク全体にわたって分散されたセンサー（例えば、センサー２５ａ～センサー２５ｃ）からレポートを受信することができ、そのセンサーの一部は、別個のエンティティによって制御される別個の領域にあるとすることができる。収集モジュールは、脅威インテリジェンスクラウド１５にレポートを定期的に送出するようセンサーに要求することができ、例えば、レポートを、機密情報を保護するために匿名で送出することができる。レポートは、接続の発信元アドレス及び宛先アドレス、アクティビティーのタイプ、ダウンロードされるファイル、使用されるプロトコル等のようなイベント情報を含むことができ、また、作動可能である（例えば、さまざまな深刻度の警告）か、又は助言的である（例えば、単独では作動可能でない場合がある疑わしいアクティビティーに関する情報を提供する）とすることができる。

【００１８】

イベント解析サブクラウド２０は、歴史的にとほぼリアルタイムにとの両方で、イベントを記憶し、処理し、マイニングするためのクラウドインフラストラクチャーを示す。サブクラウド２０は、警告のデータマイニングを行うための発見的方法を実装して、ネットワーク環境全体にわたって分散されたセンサー（例えば、センサー２５ａ～センサー２５ｃ）からの情報を相関付け、新しい脅威を特定することができる。長期的及び短期的なプロファイリングアルゴリズムが実行されて、センサーによってグローバルに検出される蔓

延している脅威を特定し、応答を自動化することができる。そのため、サブクラウド２０は、リアルタイム警告情報を収集し、センサーごとにカスタマイズされ得る高度な解析及び脅威相関を提供することができ、迅速でグローバルな脅威検出を容易にし得る。ライブ脅威情報が、脅威が発生すると、センサーに送り返され得る。サブクラウド２０は、脅威インテリジェンスクラウド１５（センサー２５ａ～センサー２５ｃから警告としてイベントを受信することができる）からイベントを取り出すことができるか、又は、センサー２５ａ～センサー２５ｃからイベントを直接受信し、脅威インテリジェンスクラウドが新しい脅威に関連するレピュテーションデータを調整することを可能にする結果を戻すことができる。さらに、サブクラウド２０はまた、更新及び新しい脅威インテリジェンスをセンサー２５ａ～センサー２５ｃ及び／又はホスト３０ａ～ホスト３０ｉに遠隔でかつほぼリアルタイムに自動的に提供することができる。顧客は、その後、これらの更新を迅速かつ積極的に実行し、サブクラウド２０の処理パワー及び発見的方法並びにグローバル脅威インテリジェンスにレバレッジをかけることによって顧客のシステムを保護することができる。サブクラウド２０はまた、ポリシー構成サジェスチョンを使用可能にする、ポリシー若しくはシグネチャーセット構成を自動的に調整する、及び／又は、他の応答アクションを使用可能にするため、新しいグローバル脅威が、より高い信頼度で（また、手作業の構成なしで）特定又は阻止され得る。

【００１９】

或る特定の実施形態において、脅威インテリジェンスクラウド１５及びイベント解析サブクラウド２０を、ともにクラウドインフラストラクチャーとして実装することができる。クラウドインフラストラクチャーは、一般に、サービスプロバイダーの最小の相互作用によって迅速に準備され（そしてリリースされ）得るコンピューティングリソースの供給プールに対するオンデマンドでのネットワークアクセスを使用可能にするための環境である。そのため、クラウドインフラストラクチャーは、コンピューテーションサービス、ソフトウェアサービス、データアクセスサービス、及び記憶サービスを提供することができ、それらのサービスは、サービスを提供するシステムの物理的場所及び構成についてのエンドユーザー知識を必要としない。クラウドコンピューティングインフラストラクチャーは、単一アクセス点として現れる場合がある、共有データセンタを通して提供されるサービスを含み得る。クラウド１５及びサブクラウド２０等の複数のクラウドコンポーネントは、メッセージキュー等の緩い結合メカニズムを通じて互いに通信し得る。そのため、処理（及び関連するデータ）は、指定された場所、既知の場所、又は固定的な場所である必要はない。クラウド１５及びサブクラウド２０は、既存の能力をリアルタイムに拡張し得る管理されホストされたどんなサービスも包含することができる。

【００２０】

ネットワーク環境１０に関連する内部構造に関して、脅威インテリジェンスクラウド１５、イベント解析サブクラウド２０、センサー２５ａ～センサー２５ｃ、及びホスト３０ａ～ホスト３０ｉのそれぞれは、本明細書で概説するオペレーションにおいて使用される情報を記憶するためのメモリ要素を含み得る。これらのデバイスは、任意の適したメモリ要素（例えば、ランダムアクセスメモリ（ＲＡＭ）、読出し専用メモリ（ＲＯＭ）、消去可能プログラム可能ＲＯＭ（ＥＰＲＯＭ）、電気的消去可能プログラム可能ＲＯＭ（ＥＥＰＲＯＭ）、特定用途向け集積回路（ＡＳＩＣ）等）、ソフトウェア、ハードウェア内に、又は、適切である場合及び特定のニーズに基づいて、任意の他の適したコンポーネント、デバイス、要素、又はオブジェクト内に情報を更に維持することができる。本明細書で論じるメモリアイテムの任意のメモリアイテムは、広義の用語「メモリ要素」内に包含されるものとして解釈されるべきである。脅威インテリジェンスクラウド１５、イベント解析サブクラウド２０、センサー２５ａ～センサー２５ｃ、又はホスト３０ａ～ホスト３０ｉによって追跡又は送出される情報は、その全てが任意の適した時間枠内で参照され得る任意のデータベース、レジスタ、テーブル、キュー、制御リスト、又は記憶構造内に設けられ得る。こうした任意の記憶オプションを、本明細書で使用される広義の用語「メモリ要素」に含むことができる。

【００２１】
さらに、脅威インテリジェンスクラウド１５、イベント解析サブクラウド２０、センサー２５ａ～センサー２５ｃ、及びホスト３０ａ～ホスト３０ｉは、本明細書で論じるアクティビティーを実施するためのソフトウェア又はアルゴリズムを実行し得る幾つかのプロセッサを含むことができる。プロセッサは、メモリ要素に関連する任意のタイプの命令を実行して、本明細書で詳述されるオペレーションを達成し得る。一例では、プロセッサは、要素又は物品（例えば、データ）を１つの状態又は物事から別の状態又は物事に変換し得る。
【００２２】
或る特定の例示的な実装形態において、本明細書で概説される機能を、１つ又は複数の有形の媒体（例えば、ＡＳＩＣ内に設けられる埋め込み式ロジック、デジタル信号プロセッサ（ＤＳＰ）命令、プロセッサによって実行されるソフトウェア（おそらくはオブジェクトコード及びソースコードを含む）、又は他の同様の機械等）内で符号化されるロジックによって実装することができ、１つ又は複数の有形の媒体が、非一時的媒体を含むものとすることができることに留意されたい。これらの事例の一部では、メモリ要素は、本明細書で述べるオペレーションのために使用されるデータを記憶し得る。これは、本明細書で述べるアクティビティーを実施するために実行されるソフトウェア、ロジック、コード、又はプロセッサ命令を記憶することができるメモリ要素を含む。別の例において、本明細書で概説されるアクティビティーを、固定ロジック又はプログラム可能ロジック（例えば、プロセッサによって実行されるソフトウェア／コンピューター命令）によって実装することができ、本明細書で特定される要素は、幾つかのタイプのプログラム可能プロセッサ、プログラム可能デジタルロジック（例えば、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、ＥＰＲＯＭ、ＥＥＰＲＯＭ）、若しくは、デジタルロジック、ソフトウェア、コード、電子命令、又は任意の適したそれらの組合せを含むＡＳＩＣであり得る。本明細書で述べる、考えられる処理要素、モジュール、及び機械の任意のものが、広義の用語「プロセッサ」内に包含されるものとして解釈されるべきである。
【００２３】
図２は、サブクラウド２０がＩＰＳセンサーからのイベントを解析するのに専用であるネットワーク環境１０の例示的な実施形態に関連することができる、考えられるオペレーションの略相互作用図である。２００にて、ＩＰＳセンサー（例えば、センサー２５ａ）は、埋め込み式ＪＡＶＡＳＣＲＩＰＴ（登録商標）タグを有するＰＤＦ文書をホスト３０ｂがダウンロードすること等の、脅威を示すアクティビティーを観察することができる。２０５にて、ローカルＩＰＳは、脅威を阻止することができる、及び／又は、ローカル警告を送出することができる。２１０にて、イベントを、脅威インテリジェンスクラウド１５に同様にレポートすることができる。２１５にて、脅威インテリジェンスクラウド１５は、サブクラウド２０内でのイベント解析にとってイベントが重要であるかどうかを判定することができる（例えば、レポートがＩＰＳから受信される）。サブクラウド２０内での解析にとってイベントが重要である場合、脅威インテリジェンスクラウド１５は、２２０にて、イベント情報をサブクラウド２０に送出できる。種々の解析発見的方法（例えば、時間、測位、レピュテーション等に基づく）を使用して、２２５にて、サブクラウド２０は、グローバルな脅威を特定するべく、イベントを、ネットワーク環境１０全体にわたって分散される他のセンサーからレポートされるイベント（又は、帯域外トラフィックの予期しない増加等の、同じセンサーからの後続のイベント）に相関付けることができる。
【００２４】
例えば、低深刻度の警告を、ＪＡＶＡＳＣＲＩＰＴ（登録商標）タグを有するポータブル文書フォーマット（ＰＤＦ：portable document format）ファイルをダウンロードすることについて設定することができる。ローカルポリシーは、低深刻度の警告であるため、こうしたイベントを無視することができる。しかし、こうしたＰＤＦのレピュテーション及びソースを、ネットワーク全体を通した複数のセンサーから受信されるレポートに基づいて決定することができる。分散センサーからレポートされるイベントのデータマイニン

グを行い、特定の国、領域、又は業界内のセンサーによってレポートされるイベントを相関付けることによって、ＰＤＦ文書を、その国、領域、業界を標的にする脅威として特定することができる。悪いレピュテーションを有する疑わしいアドレスからこのＰＤＦファイルをダウンロードしたホストもまた特定され得る。サジェスチョン、指針、及びポリシー変更推奨が、その後提供され得る。

【００２５】

２３０にて、サブクラウド２０は、グローバル脅威情報を生成し、また、ネットワーク環境１０内の又はネットワーク環境１０の（例えば、特定の国に関連する）特定のセグメント内の全てのＩＰＳに脅威情報を知らせるとともに、脅威相関に基づいて、それらの全てのＩＰＳに、カスタマイズされたセキュリティポリシー／構成サジェスチョンを提供することができる。カスタマイズされたセキュリティポリシーは、管理者からの介入なしでネットワーク環境１０を保護するきめ細かい（granular）応答アクションを含み得る。例えば、更新サービス３５は、感染したホスト（例えば、ホスト３０ｂ）をアドレスによって特定し、（もしあれば）データ喪失のタイプを特定し、感染したホストを隔離するカスタムセキュリティポリシーをセンサー２５ａに提供することができるか、又は、更新サービス３５は、阻止されるべきである特定のアドレスを特定することができる。２３５にて、サブクラウド２０はまた、結果を脅威インテリジェンスクラウド１５に提供して、他のレピュテーションデータを増大させることができる。

【００２６】

図３は、ネットワーク環境１０の或る特定の実施形態に関連することができる、考えられるオペレーションを示す略フローチャート３００である。特定の実施形態において、こうしたオペレーションを、例えば、イベント解析サブクラウド２０によって実行することができる。３０５にて、イベント情報を受信することができる。イベント情報を、例えば、脅威インテリジェンスクラウド１５からプッシュ又はプルすることができる。幾つかの実施形態において、イベント情報は、ネットワーク環境（例えば、ネットワーク環境１０）にわたって分散されるセンサーによってレポートすることができる。イベント情報を、３１０にて相関付けることができる。３１５にて、相関が脅威を明らかにする場合、３２０にて、カスタマイズされたセキュリティポリシーを、センサーの少なくとも１つのセンサーに送出することができる。カスタマイズされたセキュリティポリシーは、部分的又は全体的に３１５にて特定された脅威に基づき得る。レピュテーションデータ（同様に、部分的又は全体的に３１５にて検出された脅威に基づくことができる）を、３２５にて送出することができる。例えば、イベント情報の相関は、特定のネットワークアドレスに関連する脅威を特定することができ、サブクラウド２０は、ネットワークアドレスのレピュテーションの更新を脅威インテリジェンスクラウド１５に送出できる。

【００２７】

そのため、ネットワーク環境１０は、その一部が既に述べられた有意の利点を提供することができる。より詳細には、ローカルセキュリティ対抗策は、ローカルに調節されたポリシーを使用して、ローカルネットワークのニーズに基づいて脅威に対する保護を提供することができ、また、ネットワーク環境１０は、ローカルセンサー（すなわち、センサー２５ａ～センサー２５ｃ）のそれぞれを接続して、１つのグローバル脅威インテリジェンスネットワークにすることができる。ネットワーク環境１０では、ローカルセキュリティ対抗策は、もはや最新の脅威に反応するだけではない。新しい脅威に関するインテリジェンスを、管理システムに自動的にプッシュすることができ、管理システムがネットワークを積極的に保護することを可能にする。さらに、ネットワーク環境１０は、積極的な調節のためにクラウドベースインフラストラクチャーにレバレッジをかけることによってセキュリティ対抗策についての総所有コストを大幅に低減することができる。

【００２８】

先に提供された例によって、２つ、３つ、又は４つのネットワーク要素の観点から相互作用を述べることができることに留意されたい。しかし、これは、明確さ及び例だけのために行われた。或る特定の場合には、制限された数のネットワーク要素を参照することだ

けによって所与のフローのセットの機能の１つ又は複数を述べることがより容易である場合がある。ネットワーク環境１０（及びその教示）が、容易にスケーラブルであり、多数のコンポーネント並びにより複雑な／精緻な配置及び構成に対処し得ることが認識されるべきである。ＩＰＳの特定の文脈において本明細書で述べる原理を、ゲートウェイ、ファイアウォール等のような他のタイプのネットワーク要素に、又は、アンチウィルスシステム等のホストシステムに容易に拡張することができることも認識されるべきである。したがって、提供される例は、無数の他のアーキテクチャにおそらくは適用されるため、ネットワーク環境１０の範囲を制限すべきではないか、又は、ネットワーク環境１０の広義の教示を禁じるべきではない。さらに、オペレーションが所与のネットワーク要素に関連することができる特定のシナリオを参照して述べたが、これらのオペレーションは、外的に実装され得る、又は、任意の適した方式で統合及び／又は組み合わされ得る。或る特定の事例では、或る特定の要素を、単一の独占的なモジュール、デバイス、ユニット等内に設けることができる。

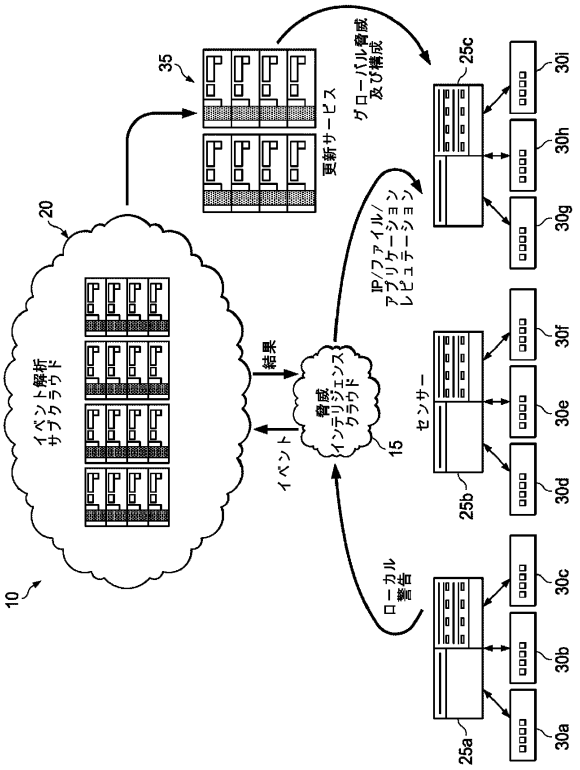
【００２９】

添付図面のステップが、ネットワーク環境１０によって又はネットワーク環境１０内で実行することができる、考えられる信号送信シナリオ及び信号送信パターンの一部だけを示すことに留意することも重要である。これらのステップの一部を、適切である場合、削除若しくは除去することができる、又は、これらのステップを、本明細書で提供される教示の範囲から逸脱することなくかなり修正又は変更することができる。さらに、幾つかのこれらのオペレーションは、１つ又は複数の更なるオペレーションと同時に又はそれと並列に実行されるものとして述べられた。しかし、これらのオペレーションのタイミングを、かなり変更することができる。先行するオペレーションフローは、例及び議論のために提供された。任意の適した配置構成、時系列（chronology）、構成、及びタイミングメカニズムを、本明細書で提供される教示から逸脱することなく提供することができる点で、かなりの柔軟性がネットワーク環境１０によって提供される。

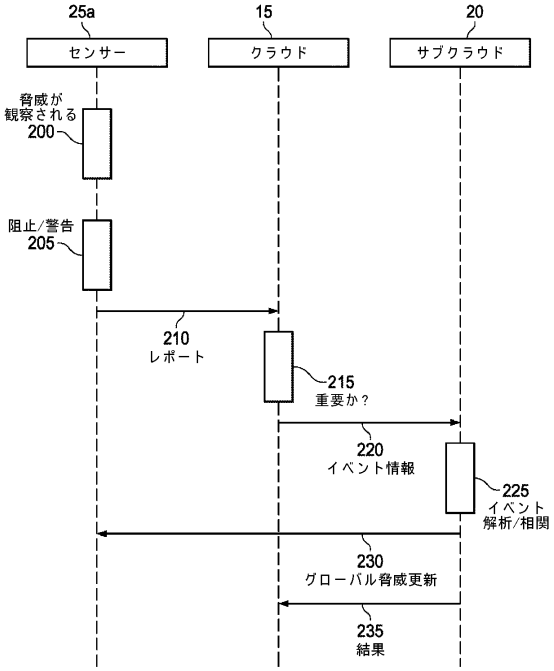
【００３０】

多数の他の変更、置換、変形、代替、及び修正を、当業者が確認することができ、本開示が、添付の特許請求の範囲内に入る全てのこうした変更、置換、変形、代替、及び修正を包含することが意図される。米国特許商標局（ＵＳＰＴＯ）、またさらに、本出願に関して発行される任意の特許の任意の読者が、添付の特許請求の範囲を解釈するのを補助するために、（ａ）「ための手段（means for）」又は「ためのステップ（step for）」という用語が特定の請求項において具体的に使用されなければ、添付特許請求項のいずれの特許請求項も、本明細書の出願日に存在している米国特許法第１１２条第６段落（paragraph six(6) of 35 U.S.C. section 112）を援用することを意図せず、また、（ｂ）本明細書のどの記載によっても添付特許請求の範囲に反映されない限り本開示を制限することは意図しないことに、本出願人は言及しておきたい。

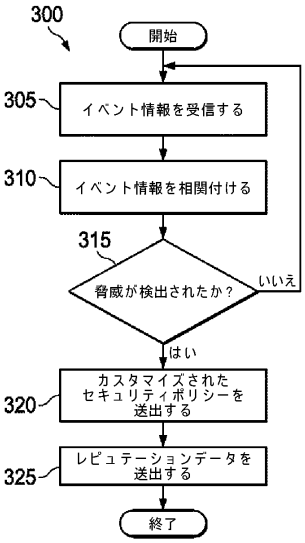
【図１】


35
更新サービス
グローバル脅威及び構成
25c
30i
30h
30g
IP/ファイル/アプリケーションレピュテーション
20
イベント解析サブクラウド
結果
イベント
脅威インテリジェンスクラウド
15
センサー
30f
30e
30d
25b
ローカル脅威
30c
30b
30a
25a
10

【図２】


25a
センサー
15
クラウド
20
サブクラウド
脅威が観察される
200
阻止/警告
205
210
レポート
215
重要か？
220
イベント情報
225
イベント解析/相関
230
グローバル脅威更新
235
結果

【図３】


300
開始
305
イベント情報を受信する
310
イベント情報を相関付ける
315
脅威が検出されたか？
いいえ
はい
320
カスタマイズされたセキュリティポリシーを送出する
325
レピュテーションデータを送出する
終了

フロントページの続き

(72)発明者 カシャップ、ラウール チャンダー
アメリカ合衆国、９５０５４ カリフォルニア州、サンタ クララ ミッション カレッジ ブーレバード ２８２１ マカフィー、インコーポレイテッド内
(72)発明者 リン、イーチョン
アメリカ合衆国、９５０５４ カリフォルニア州、サンタ クララ ミッション カレッジ ブーレバード ２８２１ マカフィー、インコーポレイテッド内
(72)発明者 マ、デニス ロク ハン
アメリカ合衆国、９５０５４ カリフォルニア州、サンタ クララ ミッション カレッジ ブーレバード ２８２１ マカフィー、インコーポレイテッド内

審査官 岸野 徹

(56)参考文献 特開２００８－０８３７５１（ＪＰ，Ａ）
特開２００５－０３８１１６（ＪＰ，Ａ）
特開２００７－１７９１３１（ＪＰ，Ａ）
宗像 誠之，徹底取材，日経コンピュータ ｎｏ．７７６ NIKKEI COMPUTER，日本，日経ＢＰ社 Nikkei Business Publications,Inc.，２０１１年 2月１７日，pp.108～111
染谷 征良 Masayoshi SOMEYA，クラウド時代のＩＴセキュリティ戦略，Ｇ－ＣＬＯＵＤ Ｍａｇａｚｉｎｅ，日本，（株）技術評論社，２０１０年 9月１０日，pp. 142～153

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／５５