(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2015-535364
(P2015-535364A)
(43)公表日　平成27年12月10日(2015.12.10)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/57 (2013.01)	G06F 21/57 370	

審査請求 未請求　予備審査請求 未請求　（全 41 頁）

(21)出願番号	特願2015-533153 (P2015-533153)
(86)(22)出願日	平成25年9月18日 (2013.9.18)
(85)翻訳文提出日	平成27年5月18日 (2015.5.18)
(86)国際出願番号	PCT/US2013/060425
(87)国際公開番号	WO2014/182326
(87)国際公開日	平成26年11月13日 (2014.11.13)
(31)優先権主張番号	61/702,484
(32)優先日	平成24年9月18日 (2012.9.18)
(33)優先権主張国	米国 (US)

(71)出願人　592005010
ザ・ジョージ・ワシントン・ユニバーシティ
THE GEORGE WASHINGTON UNIVERSITY
アメリカ合衆国ワシントン，ディーシー　２００５２，アイ・ストリート・ノースウエスト　２１２１，ライス・ホール，スイート　６０１
(74)代理人　100102934
弁理士　今井　彰
(72)発明者　クレーン　アール　エヌ
アメリカ合衆国　ワシントン，ディーシー　２０００２，　フォーティーンス　ストリート　ノースイースト　２２４
最終頁に続く

(54)【発明の名称】創発的ネットワーク防御システム

(57)【要約】
複数のノードを備えたネットワークで使用するノードのシステム及び方法が開示される。ノードは、前記ノードからの所定の近さ範囲内の近隣ノードを識別するように構成されており、この近さは物理的近さ、論理的近さ、ネットワーク・ホップ、ネットワーク・リンク、又は頂点分析に基づく近さのいずれかによって測定される。ノードは自らのナーバスネスのレベルを判定し、ナーバスネスのレベルに関する情報を前記近隣ノードに送信及び／又は受信する。
【選択図】図１

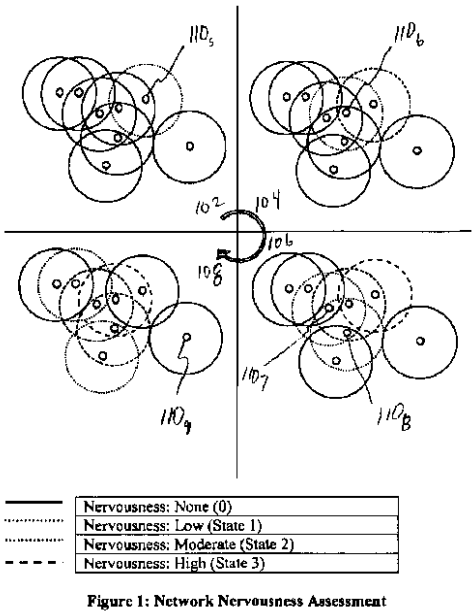


Figure 1: Network Nervousness Assessment

【特許請求の範囲】
【請求項１】
複数のノードを含むネットワークにおいて使用されるノードであって、前記ノードは、
前記ノードからの所定の近さ範囲内で少なくとも１つの近隣ノードを識別するように構成された処理装置を有し、前記処理装置はさらに、前記ノードのナーバスネスのレベルを判定して、前記ナーバスネスのレベルについて前記少なくとも１つの近隣ノードに送信及び／又は受信するように構成されている、ノード。
【請求項２】
請求項１において、前記ノードの所定の近さは、物理的近さ、論理的近さ、ネットワーク・ホップ、ネットワーク・リンク、又は頂点分析に基づく近さのいずれかによって測定される、ノード。
【請求項３】
請求項１において、前記ノードはさらに１又はそれ以上のデータ要素を具備し、前記処理装置は前記１又はそれ以上のデータ要素を制御する、ノード。
【請求項４】
請求項３において、前記１又はそれ以上のデータ要素はストレージセクタを具備する、ノード。
【請求項５】
請求項１において、前記ナーバスネスのレベルは、１又はそれ以上の情報セキュリティの健全性管理構成に基づくものであり、前記情報セキュリティの健全性管理構成は、
前記ノードがアプリケーション用の更新パッチを受信して適用した時点からの時間と、
前記ノードの保証ポリシーが構成管理サーバから現状の確認を得た時点からの時間と、
アドミニストレータが前記ノードの現状のローカルポリシー構成をチェックした時点からの時間と、
不審なイベントに対する警告を作動させる活動を実行したことと、
ローカルマルウェア又は不審な挙動に対する警告を作動させるシグネチャ又は発見的活動を実行したことと、
マルウェア又は脅威シグネチャが更新された時点からの時間とを含む、ノード。
【請求項６】
請求項５において、前記ナーバスネスのレベルはノードの健全性管理の増加に伴って減少し、ここでノードの健全性管理は、ノードの攻撃対象領域を含むノードの防御体制の現状状態を含み、ノードの健全性管理は、マルウェアシグネチャ又は脅威シグネチャに対する更新と、パッチ又は更新の適用と、システム構成の更新と、システムアドミニストレーションによる健全性管理の手動検証と、ノードの前記ナーバスネスのレベルを軽減させる沈静フェロモンの受信とのうちの少なくともいずれかを含む、ノード。
【請求項７】
請求項５において、前記ナーバスネスのレベルはノードの健全性管理の減少に伴って増加し、前記ノードの健全性管理の減少は、前記ノードがアプリケーション用の更新パッチを最後に受信して適用した時点と、前記ノードの保証ポリシーが構成管理サーバから現状の確認を得た時点と、アドミニストレータが前記ノードの現状のローカルポリシー構成を手動でチェックした時点と、前記ノードが不審なイベントに対する警告を作動させる活動を経験した時点と、ローカルマルウェア又は不審な挙動に対する警告を作動させるシグネチャ又は発見的活動が不審なイベントに対する警告を作動させる活動を実行した時点とのうちの少なくともいずれかから経過した時間の増加を含む、ノード。
【請求項８】
請求項１において、前記処理装置はさらに、前記少なくとも１つの近隣ノードから前記少なくとも１つの近隣ノードのナーバスネスのレベルを受信するように構成されている、ノード。
【請求項９】
請求項８において、前記ナーバスネスのレベルは前記少なくとも１つの近隣ノードの前

記ナーバスネスのレベルに基づく、ノード。
【請求項１０】
請求項９において、前記ナーバスネスのレベルは、フェロモンを受信した頻度または種類に基づく、ノード。
【請求項１１】
請求項８において、前記ナーバスネスのレベルはスティグマジと称される、直近の環境特性に基づく、ノード。
【請求項１２】
請求項１において、前記処理装置はパラノイア値を受信して、前記パラノイア値に基づき前記ナーバスネスのレベルを判定する、ノード。
【請求項１３】
請求項１において、前記処理装置は攻撃対象領域を決定するように構成されている、ノード。
【請求項１４】
複数のノードを備えたネットワークであって、各ノードは処理装置を有し、前記処理装置は所定の近さ範囲内の少なくとも１つの近隣ノードを識別するように構成されており、前記処理装置はさらに、前記ノードのナーバスネスのレベルを判定して、前記ノードの前記ナーバスネスのレベルを前記少なくとも１つの近隣ノードに伝達するように構成されている、ネットワーク。
【請求項１５】
請求項１４において、前記ナーバスネスのレベルはホストに属する複数の要素に基づいており、
重要なアプリケーション用の更新パッチを受信して適用した時点からの時間と、
前記ノードによってチェックされた保証ポリシーが構成管理サーバから現状の確認を得た時点からの時間と、
アドミニストレータが前記ノードの現状のローカルポリシー構成をチェックした時点からの時間と、
不審なイベントに対する警告を作動させるアクティビティを実行したことと、
ローカルＩＤＳ又はアンチウイルスマルウェア又は不審な挙動に対する警告を作動させるシグネチャ又は発見的活動を実行したことと、
マルウェア及び／又は脅威シグネチャに対する更新が行われた時点からの時間とのうちの少なくとも１つを含む、ネットワーク。
【請求項１６】
請求項１４において、前記ナーバスネスのレベルは、ノードの健全性管理の増加に基づき及び／又はナーバスネスが減少した近隣ノードからの入力に基づき減少する、ノード。
【請求項１７】
請求項１４において、前記ナーバスネスのレベルは、ノードの健全性管理の減少に基づき及び／又はナーバスネスが増加した近隣ノードからの入力に基づき増加する、ノード。
【請求項１８】
請求項１４において、ノードの状態は、近隣者からの入力に基づき、または、攻撃対象領域及び／又は健全性管理の増減に基づき変化する、ノード。
【請求項１９】
複数のノードを有するネットワークにおいて使用されるコンピュータに実装された方法であって、前記方法は、
前記複数のノードのうちの１つにおいて、前記複数のノードのうちの前記１つからの所定の近さ範囲内にある少なくとも１つの近隣ノードを識別するステップであって、前記所定の近さは物理的近さ、論理的近さ、ネットワーク・ホップ、ネットワーク・リンク、又は頂点分析に基づく近さのいずれかによって測定された近さである識別するステップと、
前記複数のノードのうちの前記１つにおいて、前記複数のノードのうちの前記１つのナーバスネスのレベルを判定するステップと、

前記複数のノードのうちの前記１つにおいて、前記ナーバスネスのレベルを前記少なくとも１つの近隣ノードに伝達するステップとを含む、方法。
【請求項２０】
複数のノードを含むネットワークにおいて使用されるノードであって、前記ノードは、
前記ノードからの所定の近さ範囲内の少なくとも１つの近隣ノードを識別するように構成された処理装置を備えており、前記所定の近さは物理的近さ、論理的近さ、ネットワーク・ホップ、ネットワーク・リンク、又は頂点分析に基づく近さのいずれかによって測定され、前記処理装置はさらに、ナーバスネスのレベルを少なくとも１つの近隣ノードから受信し、前記少なくとも１つの近隣ノードから受信したナーバスネスのレベルに少なくとも部分的に基づいて前記ノードのナーバスネスのレベルを判定するように構成されている、ノード。
【請求項２１】
請求項２０において、前記処理装置はさらに前記判定されたナーバスネスのレベルを前記少なくとも１つの近隣ノードに送信する、ノード。

【発明の詳細な説明】
【技術分野】
【０００１】
発明の背景
関連出願
本願は、２０１２年９月１８日出願の米国仮特許出願第６１／７０２，４８４号の優先権を主張し、そのすべての内容は参考として引用されて本明細書に含まれる。
【０００２】
本発明はネットワークセキュリティに関する。
【背景技術】
【０００３】
コンピュータ及びネットワークセキュリティに適用される情報セキュリティは伝統的に、独立したホスト単体に焦点を当てたものであり、ホスト単体のセキュリティに関する基本水準と規制とを定義し、ホストポリシーと構成とを集中管理するものである。しかしながら、このモデルは、移動電話、スマートグリッド、パーソナルコンピューティング装置及びネットワーク対応機器を含むネットワーク機器の急速かつ継続的な進展にはスケーラビリティが低い。
【０００４】
情報セキュリティ管理は、情報の記憶、処理及び伝達を行う情報システムの継続的使用の重要な一側面である。システム、技術、ユーザそして攻撃者の精巧さが増すにつれて、防御戦略と対応策とをこうした精巧さに見合うように進化させる必要が生じている。人的攻撃者と自動攻撃者の双方の数が千単位で増加し、ますます多くの情報システムを保護しなければならない防御者が数で圧倒されているため、コンピュータネットワーク防御（ＣＮＤ）の現行モデルはその管理が次第に困難になってきている。ＣＮＤの現行モデルは有効に機能していない。エンドポイントホストの特性を監視するためにエージェントを用いることは新規ではなく、また監視対象の創発的（emergent）挙動に対してエージェントを用いることもまた新規ではない。（S. A. Hofmeyr、『分散型検知の免疫学的モデル及びそのコンピュータセキュリティへの応用（An immunological model of distributed detection and its application to computer security）』、1999。）しかし、複雑な環境下において創発的セキュリティ指向型の挙動を生じさせるのに必要とされるシンプルでセキュリティ重視型の健全性管理特性（予防特性、衛生特性、hygiene characteristics）を評価しようと試みた文献は、今日に至るまでほとんど存在しない。（M. Mitchell、『分散型システムにおける自己認識及び制御（Self-awareness and control in decentralized systems）』、Presented at Metacognition in Computation、2005及び R. Dove、L. Shirey、『アジャイルなセキュリティパターンの発見及び表示について（On discovery an

d display of agile security patterns）、Presented at 8th Conference on Systems Engineering Research、2010を参照。）

【０００５】

ネットワークコンピュータシステムにおいて実体化されている今日のセキュリティ構造は、精巧かつ複雑なものとなっている。様々なパラダイムが、有壁要塞（walled fortress）型のセキュリティ手法、深層防御（layered defense-in-depth）型のセキュリティ手法、そして免疫システムモデリング型のセキュリティ手法を含むセキュリティ手法の概念化と発展をサポートしている。最初に要求されることは、侵入者が企業情報資産に不正アクセスするのを阻止することである。仮想プライベートネットワークなどの新しい可能性が出現し、また在宅勤務などの新しい操作パラメータが展開されるにつれて、システム単体であれば保護し得るという考え方は次第にほころびを見せている。クラウドコンピューティングの採用に伴って、このほころびの加速化が進んでいる。

【０００６】

発明者たちは、境界セキュリティに焦点を絞ることは有益ではあるが不十分であり、「外はカリカリ、中はモチモチ」的なシステムにつながるおそれがあると認識する。（Wadlow、『ネットワークセキュリティのプロセス：安全なネットワークの設計と管理（The process of network security: Designing and managing a safe network）』、2000。）このモデルが不十分であるのは、一人の攻撃者が、そのネットワークに侵入した際の防御すら提供できないばかりか、複数の攻撃者が、そのネットワーク境界内に残存し続けているときに防御を維持するための内部セキュリティを想定に入れていないからである。さらに、リモートユーザ、モバイルユーザ及び新規サービス用に外部から内部へのアクセスを許可させる必要から境界に開けられた仮想穴の数が増加しているが、これによってますます境界の多孔性が増加している。その結果として生じた企業境界の非防衛線化に伴い、従来型のセキュリティモデルの有効性は減じることとなった（Jericho Forum 2007）。安全保障の分野はますます賢くなり、こうした現実に対処し得る新しい手法を開発する必要がある、ということは広く理解されている（National Research Council 2007）。

【０００７】

これまでネットワーク上の個々のノードを、脅威を認識して対処できる程度にインテリジェントなものとしようとする試みがなされ、それが諸技術の発展に寄与した。その一例として、コンピュータシステム用の免疫システムを作成するニューメキシコ大学の研究があり、実現すればコンピュータが異質なソフトウェア要素を認識できるようになるというものである（Forrest et al., 1994）。免疫システムに触発されたこの研究は、多くの様々な探求の道をたどり続けている（Timmis et al., 2010；Greensmith et al., 2006）。

【０００８】

コンピュータシステム上でセキュリティソフトウェアを稼働させる際の運用上の課題は、セキュリティ関連のイベントの記録と分析とによって処理サイクルが占められ、その結果、企業運営などその他の用途での使用に供し得る容量が減少することである。コンピュータの性能が今日と比べてはるかに低かった頃には、このことは重大な問題であった。セキュリティ監視及び分析用のすべてのオプションを選択した場合にネットワークの速度が使用不能な程度にまで低下してしまうことは珍しいことではなかった（Kruegel et al., 2005）。この問題はコンピュータの速度と容量の改善によって幾分解消したものの、収集、関連付け及び分析の対象となるデータの量が膨大である超大型のシステムにおいては、依然として重大な課題であり続けている。

【発明の概要】

【０００９】

したがって、超大型で、不均一（異成分からなる、ヘテロジニアス）で、ネットワーク化された環境のシステムのセキュリティを管理する、拡張性の高いシステム及び方法が必要とされている。人間による介入は機械のスピードと比べれば遅いため、通常であれば、各ネットワークノードの管理に関与する人間はほとんどいない。マルウェア（悪意のあるソフトウェア）の感染はネットワークを介して驚異的なスピードで拡散する。無管理の又

は管理の不十分なネットワークノードの増加により構成や補修の基本的な健全性管理が維持できない。様々な現存のソリューションが、マルウェア拡散の抑制やシステムセキュリティの管理を支援しているが、その多くは、処理のオーバーヘッドとネットワークサイズとがトレードオフの関係となる。そのため、システム全体のセキュリティの管理を各ノードが支援するようにネットワークの諸要素を関わらせることによって、大規模ネットワークの管理がネットワーク運用の負担とならないようにする必要がある。

【００１０】

こうしたセキュリティ管理上の課題への対応をネットワーク内の各ノードが支援できるようにすることは、問題の完全なソリューションにはならないが、課題への対応は容易になる。具体的には、本発明は、動作環境を継続的に評価してその評価結果に基づき自らの動作に関する決定をなす能力を各ノードにおいて形成することによって、各ノードがセキュリティ管理上の課題対応に寄与できるようにすることに焦点を当てる。この決定プロセスは２つの要素、すなわち、近くの近隣ノードからの入力と、先験的な条件状態（a priori conditional states）に基づく自己評価とに基づくものである。この決定空間の最終産物は緊張性指数（神経質性指数、ナーバス指数、nervousness index）であり、各ノードはこの指数を用いて挙動の動作パターンを増減させる。本発明の説明のために、動作挙動パターン（運用行動様式）とは、グループ環境評価の結果に基づいて動作能力（攻撃対象領域（アタックサーフェス、attack surface））を自動的に削減することによって、ネットワークのセキュリティ管理を支援する各種処理のことを指すこととする。これは人間のアドミニストレータに、ネットワーク環境内で脅威が検出されたときに、それに対処するための追加時間とともにネットワークのセキュリティステート全体に関する価値ある情報を入力することを可能とする。攻撃対象領域の自動削減の実現はしばしば基礎的な情報セキュリティの健全性管理を実施することによりなされ、例えばサービスを停止させたり、パッチと構成とを最新版のレベルにすることである。

【００１１】

さらに、問題への対処をより容易にするため、ナーバス指数の低減は主に、最小数の安全管理をある特定のノードに適用することによってなされる。攻撃対象領域の削減に用いられる基礎的な動作能力は「セキュリティの健全性管理（セキュリティの健全性管理度、セキュリティ衛生度、security hygiene）」としても知られており、最低限の許容可能な安全基本水準（security baseline）を維持するためにシステムに実装すべき最小限の安全管理がある。特にこの実装のため、我々は、「セキュリティの健全性管理」の最小限の管理（規制、制御）には、ノードポート、プロトコル、オペレーティングシステムのパッチレベル、アプリケーションパッチレベル、アンチウイルス及び侵入検知システムのソフトウェアのシグネチャ（署名的行動、痕跡、特徴）及びポリシーエイジ（policy age）、の管理、維持及び運用管理、システムがポリシー遵守状況につき最後にチェックされた時点からの経過時間、そして現行のシステム状態とシステム構成の基本水準と差、が含められると考える。これは、ノードの攻撃対象領域を管理する際に利用され得る、可能な制御（可能な規制）の、ある限られたセットである。安全管理を攻撃対象領域に影響を与える安全管理のサブセットのみに限定することで、システム全体の複雑性が軽減され、またこのコンセプトの有効性を示す良い例となる。

【００１２】

この最低レベルを上回る追加的管理を行うと、この機能の実装の厳格性とナーバス計算の精度が増すことにはなるが、緊張性（ナーバスネス、ナーバス性）と攻撃対象領域の管理という基本コンセプトの実現に大きな影響は与えない。しかしながら、本発明の用途は攻撃対象領域の削減のみに限定されるものではなく、セキュリティの健全性管理は最小限であっても堅牢であっても使用でき、他の要素がナーバスネス（ナーバス性）に影響を与えたり低減するものであってもよい。これらは、将来の攻撃および疑わしい不正ユーザの挙動の情報又は事前警告、外部の脅威緩和行動といった脅威による攻撃成功の可能性を減じるものを含むが、それに限定されるものではない。現行の攻撃対象領域を判断するリスク評価の一部は、一部の動作能力が他の動作能力よりも重要であると認識することを含む

。その一部の能力は追加サービスを提供するものであってもよく、それは、いっそうの有用性、機密性又は整合性を要求し、それらは攻撃対象領域を変更するものではないが、リスク評価を通じて判断される。その他の動作能力は、要求するセキュリティへの考慮がより少ないものであってもよく、そのため限られたリソースを、各ノードのセキュリティに関する最も重要な要素に集中できる。これが本発明の基礎的な動態（ダイナミクス）の１つであり、すなわち情報セキュリティリスクを測定し動的に処理し緩和する新しいメカニズムである。

【００１３】

複数のノードを含むネットワークで使用されるノードのシステムと方法が提供される。ノードはこのノードからの所定の近さ範囲内にある近隣の１または複数のノードを識別するように構成されており、この所定の近さは物理的、論理的、ネットワーク・ホップ、ネットワーク・リンク、又は頂点分析（vertices analysis）に基づく近さのいずれかによって測定される。ノードは自らの緊張性（神経質性、ナーバスネス）のレベルを判定し、ナーバスネスのレベルについて、近隣ノードに送信及び／又は受信する。

【００１４】

本発明の上記及びその他の目的、さらには本発明において意図されている利点の多くは、以下に記述する説明を添付の図面と併せて参照することで、さらに明白となるであろう。

【図面の簡単な説明】

【００１５】

【図１】ネットワークナーバスネス評価を示すダイヤグラムである。
【図２】創発的ネットワーク防御のシステミグラムである。
【図３】最も近い近隣者を抽象化して示す。
【図４】ナーバス状態の例を示す。
【図５】ブロック１の理論的コンテクストダイヤグラムである。
【図６】ステート変更を示す。
【図７】ブロック２の理論的コンテクストダイヤグラムを示す。
【図８】創発的挙動を示す３つの警告を示すスクリーンショットである。
【図９】ブロック３の理論的コンテクストダイヤグラムである。
【図１０】要求されるデータ要素を示す。

【発明を実施するための形態】

【００１６】

図面に示される本発明の好ましい実施形態を説明するに当たり、明りょう性を確保するため専門用語の説明を行うこととする。しかし本発明は、選ばれた特定用語に限定されることを意図しているものではなく、各専門用語は同様の目的を達成するために同様の仕方で動作するすべての技術的等価物を含むものと解されるべきである。

【００１７】

図示及び明確性確保の目的上、ただし本発明の限定を意図するものではないが、「ノード」という用語はここでは、固有の特性を有する個々の要素であって、他の近隣ノードと通信可能な環境下にあるものと一般に理解される。ノードは「ホスト」として実体化されるが、本実施形態は、ノードのアプリケーションが、定義された「ホスト」を超えることを制限することを意図したものではない。「ホスト」という用語は、近隣ノードと通信し、当該ノードのナーバスネスレベルを判定しナーバスネスのレベルについて、１または複数の近隣ノードに送信及び／又は受信するように構成された処理デバイスとしての特定の実施形態のノードのことを指す。「ローカル」という用語は、当該ノードと１または複数の近隣者との間の所定の近さ（closeness）のことを指し、この所定の近さは物理的近さ、論理的近さ、ネットワーク・ホップ、ネットワーク・リンク、又は頂点分析に基づく近さのいずれかによって測定される。「エージェント」という用語は、ノードとして動作するホスト上に存在するソフトウェアなどの特定の能力のことを指す。

【００１８】

本発明の目的の１つは、ネットワークノードにおいてローカル環境基本認識（local environmental primitive awareness）を使用することで、大規模ネットワークのセキュリティ管理の実効性と効率性をさらに高めることにある。実効的なセキュリティ管理とはリスクマネジメント処理のことであって、これは潜在的な攻撃がその最終目的を達成する確率を下げることを意味し、また、この計算のために攻撃対象領域を代替変数として用いる。効率的なセキュリティ管理とは、アクションが取られるスピードの代替変数と、人間であるオペレータに課題が通知されるスピードの代替変数とを用い、ローカル環境評価に基づく自動決定を通じて脅威への対応がより迅速になされ得ることを意味する。

【００１９】

本発明は、大規模な異機種ネットワークにおけるセキュリティ管理の手法を提供し、人間であるアドミニストレータが検出された脅威に対応する能力を向上させる。従来のセキュリティ管理は、集中制御型のホスト単体に焦点を置いており、それほど有効に機能しなくなっている。本発明は、ネットワーク環境の防御と障害対応を有効化するように総合的に機能する相互ネットワーク環境を形成するという課題に対処する。本発明のいくつかの非限定的な実施形態を以下に論じるが、そこでは、脅威の高度化し、防御の複雑性が増し、そして防御すべき攻撃対象領域が増加していることを念頭に置きつつ、大規模な異機種ネットワークにおけるセキュリティ管理を目的とした「セキュリティエコシステム（安全な生態系）」を構築することを論じている。セキュリティエコシステムにおいては、機械は機械時間において他の機械からの脅威に対処し、人間は人間時間において他の人間からの脅威に対処する。オートメーションは健全なサイバーエコシステム（仮想生態系）の第一の構造ブロックである（米国国土安全保障省、2011）。本発明は、ネットワーク上のデバイスの関与を有効化しかつ検出された脅威に対応する人間であるアドミニストレータの能力を向上させるためにはどのような特性が本質的に重要であるか、という点を考慮に入れた分散型モデルを提供する。

【００２０】

本発明は、フェロモンとスウォーム理論（swarm theory）を検討する。フェロモンとは、生物が放散する化学物質であり、群内の他者に対して極めて限定的でかつ特定のメッセージを伝達するためのものである。スウォーム挙動（swarm behavior）とは、刺激に呼応して生物の群が一斉に動くことである（New Oxford American Dictionary、2011）。スウォーム理論は、興味深い特性の出現を求めて群を観察するためにスウォーム挙動を用いる。フェロモンはその性質上極めて限定的なものではあるが、重要な情報を群の構成員に伝達し、この情報に基づき個々の及び群の挙動に変化をもたらすものである。コンピューティングシステムとの類似点は、フェロモンの類似物が極めて少ないリソースしか要求しないということであり、この点は本発明において、パフォーマンスの制約となる。スウォーム理論は、蟻や蜂のような真社会性の昆虫のインタラクションの組合せを通じて観察される群れのアクティビティのことである。群れのアクティビティのインパクトは個々のノードのアクティビティを超えるものであり、この場合、システムのインテリジェンスは個々のパーツのインテリジェンスの総和よりも大きい（C. G. Langton、『混沌の縁における計算：相転移と創発的計算（Computation at the edge of chaos: Phase transitions and emergent computation）』、Physica D 42（1-3）、pp. 12-37、1990; S. A. Kauffman、『秩序の起源：自己組織化と進化時の選択（The Origins of Order : Self Organization and Selection in Evolution）』、New York：Oxford University Press、1993; J. Kennedy および R. Eberhart、『粒子群最適化（Particle swarm optimization）』、Presented at Neural Networks、1995、Proceedings、IEEE International Conference、1995）。

【００２１】

フェロモンの類似物はナーバスネス（緊張性、神経質性）のレベルをネットワーク上のノード間で伝達するのに用いられる。このフェロモン類似物という表現は、ナーバスネスアセッサ（緊張性評価者）（ＮＡ）が生成するナーバス信号（ＮＳ）である。いずれのノードにおけるＮＡも、通信を行っている複数の近隣者から複数のＮＳを受信して統合する

。ＮＡは、ネットワークから１又はそれ以上のＮＳを受信すると、収容されていた情報を統合してノードの現行状態（カレントステート）のアセスメント（評価）に組み入れる。このアセスメントには、動作状態に関連する重要なノード特性が含まれる。最後に、ナーバスネスオペレータ（緊張性オペレータ、ＮＯ）はノードに働きかけて、例えば攻撃対象領域の増減といったような動作状態の変更を行わせる。

【００２２】

ナーバス信号（ＮＳ）は、ナーバスネス状態を、あるノードの最も近い複数の近隣者に伝達するものである。このコンセプトと類似するものは、大勢の人々の観察である。ある人が特定の挙動を示す（例えばある特定の方向を向くなど）と、そのアクティビティを観察していた最も近くの隣人たちもまた同じ方向を向くことになるであろうし、その場合、彼らの関心を引く価値のある何かが実際に存在している可能性もある。ここで留意すべき点は、人間は真社会性の動物ではないため、人間の挙動から創発的な特性（emergent characteristics）を類推することは確実とは言い切れないということである。

【００２３】

ナーバスネスアセッサ（緊張性評価者、神経質性評価者）（ＮＡ）は、ノードのナーバスネス状態を計算して、ナーバス信号の送受信を行う。ノードのナーバスネスの計算は、最も近い近隣者のナーバスネスと内部状態構成とを用いる。本発明の目的上、選択される内部状態特性は以下のものである：現状の攻撃対象領域、直前のナーバスネスレベル（緊張性レベル）、そして妄想性レベル（パラノイアレベル、paranoia level）である。この場合におけるパラノイアのコンセプト（妄想性概念）は、人間のオペレータが設定する可変の特性であり、そのためＮＡによる反応の仕方は運用環境の要求するところに基づいて設定できる。

【００２４】

ナーバスネスアセスメント（緊張性の評価、神経質性の評価）への反応は、この理論における行動的成分（挙動要素）に寄与する。ノードは環境からナーバス信号（ＮＳ）を受信し、ナーバスネスアセッサ（ＮＡ）は、個々のノードにおけるナーバスネス状態がどうあるべきかという点についてのアセスメントを生成する。その後、ＮＳは更新されたナーバス状態を伝達し、ＮＯは予め定義された挙動パラメータ（行動パラメータ）に基づいて動作する。この動作には、アクティブなポートの数を減らすことによって、適用されていないパッチをチェックすることによって、構成を最新のポリシーに更新することによって、人間であるアドミニストレータに警告を発することによって、又は完全にシャットダウンすることによって、内部の又はネットワークの攻撃対象領域を増減させることを含むものであってもよい。

【００２５】

この個別ノードの挙動（行動）は、システム内のより大きな挙動パターンに寄与する。本発明の実施形態では、個別ノードのナーバスネスが増すにつれてその近隣者にナーバスネスの増加が反映されることを示している。この挙動は、ナーバスネスの発生源という観点と、反応の拡散という観点とから観察可能である。以下にモデルを提示して、挙動がどのようにして発生し得るかを検証する。

モデル

【００２６】

形式モデルはノードナーバスネスA=< S,F >の２要素（２タプル）のステートマシンに依拠し、ここでSは１セットの状態（ステート）であり、F⊆Sは１セットのフィードバックステートである（ＳとＦは図２でさらに使用される）。ノードステートs∈Sはノードリソース（resources）をその構成（configurations）にマッピングしたものである：

【００２７】

【数１】

$$s : res_a \rightarrow conf_a$$

【００２８】

リソースには、ポート、サービス、そしてパッチングやシグネチャ更新やポリシー管理といったアドミニストレーション機能といったものなどが含まれる。構成とは、ブロックすべきポートやパッチ適用の頻度などのリソースに適用される設定のことである。概してノードステートsは、攻撃対象領域（アタックサーフェス、attack surface）を示し、そして内部攻撃対象領域とネットワーク攻撃対象領域の双方をこのモデル用の一測定単位として組み合わせたものを含む。

【００２９】

いずれかのノードにおけるナーバスネスを計算するため目的上、いずれかのノードにおけるナーバスネスアセスメント（ＮＡ）は、ローカルエリア内のナーバス信号（ＮＳ）のフィードバックとシステムの構成状態とにより生成される。

【００３０】

ネットワークナーバスネス（$Nerv_n$）は、ナーバスネス分析の各時間ステップにおいて反復される：

【００３１】

【数２】

$$Nerv_n : Nerv_n \rightarrow Nerv_{n+1}$$

【００３２】

ナーバスネス（緊張性、神経質性）とは、ローカライズされた環境における近隣者たちのナーバスネスであり、これは各ローカルノードmのナーバスネスを合計して、個別のノードロケーションにおけるローカライズされたネットワークナーバスネス（Network Nervousness）を計算したものである。

【００３３】

【数３】

$$Nerv_n = \sum_0^m Nerv_a$$

【００３４】

そしてシステムフィードバックFは、ネットワークナーバスネス（Network Nervousness）をノード倍率パラノイア（Paranoia）で乗じたものである。

【００３５】

【数４】

$$F : Nerv_n \cdot Par_a$$

【００３６】

各ステートにおいて取られるアクションは、環境の必要性に応じて変化させることができる。ステート１では、すべてのアクティビティが正常でありかつナーバスネスのステートが「沈静」であり、システムは、動作パラメータによって定義され、最も開放された状態に設定される。その後の各ステートにおいて、ステートの数は合計で３つを上回っても

よいが、動作ポリシーによって定義されるところのアクションは、より制約の多い構成を実装することによって攻撃対象領域を逐次減少させる。

【００３７】

次に、ステートマシンAのナーバスネスを、ノードの構成（configuration）とシステムのフィードバック（feedback）との組み合わせとしてモデル化する：

【００３８】

【数５】

$$A : s \cdot F$$

ここで

$$A = conf_a \cdot Nerv_n \cdot Par_a$$

【００３９】

sとしてモデル化されたノードステートの定義によって、個々の特性について検証を行うことができる。リソース（resources）の構成（configuration）を維持するための日々の更新サイクルを考慮すると、各ノードについて以下の変数が検討される：１日の平均動作時間o；構成のための１日の平均停止時間c；そしていずれかの時点における攻撃対象領域の相対的なサイズ、である。

【００４０】

２４時間の枠dの間で、構成の時間cを最小限として、以下のように指定できる：

【００４１】

【数６】

$$\mathrm{Conf_c} : \mathrm{Conf_M} \rightarrow \mathrm{Conf_{M+1}}$$

$$\mathrm{Conf_c} = d - o$$

【００４２】

変数は構成の安全性（構成セキュリティ）の様々な状態をもつ：

【００４３】

【数７】

$$Conf_{Low}$$

$$Conf_{Moderate}$$

$$Conf_{High}$$

【００４４】

攻撃対象領域を、ひいてはナーバスネスを減少させるための簡単な解答は、不必要なサービス、とりわけユーザがそれほど必要とせずあるいはそれほど頻繁には必要としないサービスを終了させることである（M. Howard、2004）。他のアプローチは、このモデルでは、ローカライズされたフィードバックとローカルポリシー（パラノイア）を介した動的フィードバックに基づきなされるポートの開放やパッチの更新などで、構成を徐々に増加することによって、攻撃対象領域のサイズを操作する。各構成状態は、構成と、ナーバスネスと、パラノイアとに基づき、攻撃対象領域のサイズについて、相異するが想定される結果をもたらす。このモデルによりユーザは、相対的なノードナーバスネスと従前のステートナーバスネスとを比較し、良好か否かの尺度にできる。

【００４５】

【数８】

$$A_n = conf_m \cdot Nerv_n \cdot Par_m$$

$$A_{n+1} = conf_m \cdot Nerv_{n+1} \cdot Par_m$$

ここで

$$A_n \leq A_{n+1} \text{ 又は } A_n \geq A_{n+1}$$

【００４６】

最後に、ノードナーバスネス（Ａ）は、ノード構成（攻撃対象領域）と、ナーバスネスと、パラノイアとの組合せであり、ノードの直近の環境に対する基本的（原始的）ローカル認識を用いて、個々の時点における直近のナーバスネスを計算できる。本発明において、この計算は、構成と、ナーバスネスと、パラノイアとを、均等加重で乗算する。

【００４７】

各ノードは、ノードナーバスネスA=< S, F >の２要素（２タプル）のステートマシンを有するが、この例はノード単体におけるナーバスネスを計算するものとする。上記のモデルに基づくと、システムステートsは、時間的な特定の各ステップにおける、０から１の

構成confが目安であり、これはポートとサービスの数、そして最後になされたパッチング、更新及びアドミニストレーションポリシープッシュからの経過時間に基づき計算される。この値が攻撃対象領域である。そしてシステムフィードバックfが、直近の近隣者のナーバスネスの合計で計算され、パラノイア倍率で乗算され、こうしてネットワークナーバスネスが計算される：

【００４８】

【数９】

$$Nerv_{m+1} = \sum_{A}^{E} Nerv_{m}$$

【００４９】

そして、これを個々のノードのパラノイア倍率（０～４）で乗じて、モデル化されたノードmのフィードバックを計算する：

【００５０】

【数１０】

$$F : Nerv_{m+1} \cdot Par_{m0}$$

【００５１】

最後に、システム構成の攻撃対象領域と、ネットワークナーバスネス、とホストのパラノイアとを乗算して、ノードナーバスネスを計算する：

【００５２】

【数１１】

$$A_{m+1} = conf_{m+1} \cdot Nerv_{m+1} \cdot Par_{m0}$$

又は

$$A_{m+1} = conf_{m+1} \cdot (Nerv_{A} + Nerv_{B} + Nerv_{C} + Nerv_{D} + Nerv_{E}) \cdot Par_{m0}$$

【００５３】

このモデルにおいては、パラノイアは、各ノードにつきそのライフサイクルを通じて固定されたままとされ、パラノイアの変更は可変独立変数の変更としてのみなされる。

【００５４】

本実施形態には、ナーバスネスを伝達するネットワークフェロモンはただ１つのみ含まれる。しかしながら、本発明は他の基本的（原始的）な伝達信号を含んでいてもよく、たとえば、「沈静」フェロモンであり、この信号は相互行動と挙動に対して発せられ得る。蟻の巣では、スティグマジ（stigmergy）、接触、相互行動の頻度及び集中度並びにフェロモンコミュニケーションなど多数の伝達メカニズムが用いられている。「沈静」又は「安全」信号は蟻の巣で見られるものであり、本発明においても用いることができ、複雑なコミュニケーション及び記憶保持をなすために、多数のフェロモン、そしてフェロモンの組合せを用いてもよい。本発明は、ネットワーク・スティグマジ（network stigmergy）を伴う多くの実施形態において使用することができ、ファイアウォールのルール、ネットワークのセグメント化、ルーティングルールの組合せ及び侵入検知システム（ＩＤＳ）の警告などといったネットワークデバイスルールの組合せを通じて、自らの周囲環境を動的に調整するノードを含めることができる。

応用

【００５５】

本発明は、ネットワーク環境アセスメントの基本構造を提供するものであり、広く応用可能である。本発明は、攻撃対象領域を削減して防御用ネットワーク態様（ネットワーク防衛、defensive network posture）を増加させる創発的システム（emergent system）を提供する。本発明は、近隣ノード間のナーバスコミュニケーション（緊張性の伝達、緊張性通信、神経伝達、nervous communication）を用いた多数の非限定的な例示的実施形態において使用することができる。

【００５６】

本発明が対処する課題の１つは、大規模、分散型、異機種接続（ヘテロジニアス）な環境下における可視性の欠如である。ネットワーク環境における可視性とは、自らの現状環境に対する状況認識をもたらすアドミニストレータの能力のことであり、言い換えると、アドミニストレータは自らの情報資産又はデバイスのロケーション及びそれら資産の現状のセキュリティステータスを知っているということである。これは、構成と、防衛（防御体制）と、攻撃対象領域とを変更するようホストに指示を出すために、現状のネットワーク管理下において必要とされる能力である。しかしながら、このことは、各ローカル環境がそれぞれ異なる種類のセキュリティ上の課題と脅威とを有している可能性もある大規模なネットワーク環境においては、ますます困難となっている。また本発明は、ホストが自らのローカル環境に基づき監視及び警告の発報をなすようにし、その結果はシステム全体の挙動の分析のために人間のアドミニストレータに報告として戻されるようにすることができる。防御の判断をホスト側により近付けることによって、本発明は、セキュリティの判断が、過去に報告されたイベントに基づく反応ではなく直近の、または進行中の脅威に先行できるように支援する。

【００５７】

コンピュータとネットワークセキュリティに適用される情報セキュリティは伝統的に、孤立したホスト単体に焦点を当てたものであり、ホスト単体におけるセキュリティ境界及びセキュリティ基本水準の制御を画定し、ホストポリシーと構成とを集中管理するものであった。しかしこのモデルは、移動電話、スマートグリッド、パーソナルコンピューティング機器、そしてネットワーク対応機器を含むネットワーク機器の急速かつ継続的な発展に伴って、それほど有効に機能しなくなっている。本発明は、ネットワークノードにおけるローカル環境の要素的認識（基本認識、primitive awareness）を用いて、大規模ネットワークにおけるセキュリティ管理の実効性と効率性を高めようとするものである。いくつかの非限定的な例示的実施形態を以下に論じるが、そこでは、脅威の高度化、防御の複雑性、そして防御すべき攻撃対象領域の増加を念頭に入れつつ、大規模でヘテロジニアスなネットワークにおけるセキュリティ管理を目的とした「セキュリティエコシステム」を構築することを論じている。セキュリティエコシステムでは、マシンはマシンタイムにおいて他のマシンからの脅威に対処する必要があり、人間は人的時間において他の人間からの脅威に対処する必要があるものと理解される。本発明においては、各ノードに、動作環境を継続的に評価してその評価結果に基づき各ノードの動作プロファイルに関する決定をなす能力を形成することによって、それぞれのノードがセキュリティ管理上の課題への対応に寄与できるようにする。さらに、攻撃対象領域を削減することにより、システム全体の複雑性を軽減する。

ネットワーク防御

【００５８】

１つの非限定的な例示的実施形態において、本発明はエンドポイント又はノードの管理に適用可能であり、エンドポイントが集中コマンド及び制御能力では制御も管理も受けていないときに、防御の警戒体制を増強できる。また、従来の集中型又は分散型のエンドポイント管理ソリューションが可視性の喪失によって崩壊しつつある大規模ネットワークにおいて、本発明をエンドポイント又はノード管理に利用することもできる。両シナリオにおいて、ネットワーク防御のための創発的挙動（emergent behaviors）は、他の分散型ネットワーク管理システムを支援はするが、その代替とはならない。この攻撃対象領域の自動削減は、しばしば、基礎的な情報セキュリティの健全性管理の実施、例えばサービスを

切断したり、パッチと構成とを最新版のレベルに確保したりすることによって達成される。

【００５９】

マイクロソフト社やアップル社などのオペレーティングシステムベンダを含め、大規模な非管理型ネットワーク環境内におけるアプリケーションは少なからずある。この大規模な非管理型ネットワーク環境には、インターネット対応モバイルデバイスを提供する移動電話キャリアも含まれる。これらのデバイスは、共有ネットワーク環境上で相互に接続されていて、中央管理サービスから更新データを受け取るが、最終的な管理上の決定はエンドユーザに委ねられている。例えば、インフラプロバイダとしてはベライゾン社、ＡＴＴ社そしてスプリング社、ソフトウェアプロバイダとしてはグーグル社、ＲＩＭ社そしてアップル社、ハードウェアプロバイダとしてはサムスン社、モトローラ社そしてアップル社が挙げられる。

【００６０】

さらに本発明は、多数の分散型ノードの管理に関わる、いかなるソフトウェア又はハードウェアベンダにも適用され、例えば、企業ネットワーク管理会社としてはＩＢＭ社、インターネットワーキング会社としてはシスコ社、エンドポイント管理ベンダとしてはエンドポイント社及びアルテリス社、そしてセキュリティ会社としてはマカフィー社及びシマンテック社がある。

【００６１】

エンドポイントがナーバスなネットワークを介して相互に通信を続けていても、凝集能力（aggregation capability）を通じて、セキュリティの健全性管理のレベルを継続的に集中監視することができる。このハイブリッドアプローチにより、リスクアセスメントを企業規模で判断できる。

【００６２】

本発明は、管理型コンピュータネットワーク環境、例えば分散型ネットワーク管理（ＤＮＭ）ソリューションを用いて中央集中型のノード補修及びポリシー管理を行う管理型コンピュータネットワーク環境に適用可能である。これは、マイクロソフトアクティブディレクトリなどオペレーティングシステム、アルテリス社又はビッグフィックス社のようなエンドポイント管理用のアドオンの組み込みソリューションに含められてもよく、マカフィー社又はシマンテック社のようなエンドポイント情報セキュリティソリューションに含まれてもよい。本発明は、ＤＮＭソリューションを補強しまたこれに代替することができる。さらに、そしてより重要なことに、本発明は、非管理型のコンピュータネットワーク環境のための、現行初期の機能に対する新しい機能または拡張として動作しうるものであり、ここでいう非管理型のコンピュータネットワークでは中央集中型のＤＮＭソリューションは用いられず、各ノードはいつ補修（パッチング）を行うか、そしてどのポリシーを配備するかを独立して選択する必要があるものである。これは、パーソナルコンピューティング機器、モバイルコンピューティング機器、個人所有機器、又はＤＮＭ配備の弱い大企業において通常用いられる。

【００６３】

この技術から生じるであろう主たる新しい所産は、拡張されたネットワーク管理機能であり、これは既存のネットワーク管理機能に統合され、情報システム管理者が、管理上の決定を人間のスピードの時間ではなくコンピュータのスピードでなすことが可能となるように支援する機能である。

【００６４】

ここで、ある民生用の移動電話ネットワークの実施例を挙げてみる。大抵の民生用の移動電話は、消費者が個人用機器として購入し保有する。消費者の責任は少なくとも、料金の支払い、機器の充電、ネットワーク上での電話機の登録、機器の物理的安全の確保、ファームウェア、オペレーティングシステム及びアプリケーションソフトウェアの更新、そして安全なセキュリティ上の行為の実施を含む。安全なセキュリティ上の行為は以下のことを含むがそれに限定されない：パスワードの選択と保存を適切に行うこと、自らの周囲

の状態に注意すること、自らが接続できてしまう他のネットワーク及び装置に配慮すること、そして自らの機器を適切に利用して以下のものに害を及ぼさないようにすること：自らの機器（マルウェア感染など）、自らと他者（ながら運転による交通事故など）、同僚や友人（マルウェアの共有又は悪意のあるコンテンツのソーシャルメディアへの投稿など）、そして使用するネットワークキャリア（ネットワークの悪用、サービス利用規約の違反など）。

【００６５】

しかしながら、消費者は、これらのそしてその他の必要なセキュリティアクティビティを実行するための技術も関心も有していない。結果として、これらのうちの一部をネットワークサービスプロバイダが実施し、またスマートフォン（アンドロイド、ｉＯＳ）などの場合はサードパーティのサービスプロバイダが限定された数のセキュリティサービス（バックアップ、パッチング、パスワード保護）を提供する。

【００６６】

会社所有のモバイル機器のような場合、上記の機能の一部を中央サーバが制御するが、ここで中央サーバは、ポリシーを設定し、パッチを当て、機器に入り及び機器から出る又は機器上に存在する悪意のあるアクティビティの有無をチェックし、そして会社のセキュリティポリシーに基づき機器の構成を行う。しかし、こうした環境下においても、各モバイル機器のあらゆる時点における直近の環境についての具体的な詳細を中央サーバが把握できない場合もあり得る。さらに、地理的要因（国外）や環境的要因（地下、混信）によってサーバ接続が失われることもあり得る。サーバが提供するいかなる応答も、利用状態や帯域幅による通信上のタイムラグを伴うことになる。

【００６７】

本発明を上記の移動電話の例に応用することで、これらの課題の多くが解消されるが、それは、人間であるアドミニストレータの警告に対応しやすくし、あるいは、環境認識と自動化とにより、人間であるユーザの介在を完全に不要にしたりすることによって、これらの課題への対応がより容易となるからである。

【００６８】

例えば、このネットワーク内で移動電話として具現化されるノードは、自らの周囲環境を認識する要素を有することになる。料金の支払いや機器の充電の他に、創発的ネットワーク（emergent network）上の移動電話は以下の機能を有する：

【００６９】

・移動電話がネットワークに登録されているよう確保する機能、又は、信号が喪失した場合、もしそのように構成されていてかつ他のネットワーク機器の範囲内にあるならば、網目状モバイルネットワークのピアデバイスを経由して通信を行う機能。近隣者が創発的ネットワークの一部をなしていないか、または、創発的ネットワークの近隣者が範囲内に存在しないため、いかなる近隣者も存在しない場合、その電話は、適切に、信頼できないピアとの通信を行わない。

【００７０】

・ＧＰＳ、加速度計、信号の強度及び近隣者との近さといった、直近の環境要因に基づき自らの物理的環境を認識する機能。これを用いることで、ある電話が盗難されたか否か、例えば普段その電話を使用しない又は使用を許可されない物理的領域内にあるか否かを示させることができる。

【００７１】

・創発的電話ノード（emergent phone node）は、ファームウェア、オペレーティングシステム及びアプリケーションの更新を、定期的なアップグレードアクティビティを待つのではなく、直近の環境要因に基づいて行う能力を有する。これは、複数の近隣ノードが現状の更新を行っていることを察知し、１つでも更新可能か否かをチェックする。これはまた、ナーバスの目安となる閾値に到達したか否かにより、攻撃対象領域削減のためにノードがアップデートをチェックすることを含む。

【００７２】

・安全なセキュリティ上の行動をユーザ側に強制することはできないが、創発的電話はユーザがより安全なセキュリティ上の決定をなすことを支援する。この決定には、セキュリティの弱い環境下において平文の送信を制限したり、パスワードの表示を制限（タイプ中に＊＊＊を表示するだけでなく）したりすることが含まれる。銀行口座の照会などセンシティブな活動は、他の創発的ノードが多数の近隣者の存在を示しているような、バス車内などの過密な公共エリアにいるときには、制限されることとしてもよい。

【００７３】

・おそらく移動電話の例において実現される最大の利点の１つは、他者の保護である。創発的ネットワーク（emergent network）は、健全なエコシステムを通じてなされるコミュニティが生き残ることに寄与する。その結果、創発的ネットワークは当然に自己保存（自己防衛）への欲求を有する。擬人化テクノロジーではないが、周囲環境を認識することによる生存活動は、容易に構成でき、実装できる特性である。例えば、創発的電話は、ユーザが車を運転しているときには動作させないでおくことができ、またツイーティングマルウェアなど他のユーザに伝播するおそれのあるマルウェアに感染したときにユーザが特定のサービスにアクセスすることを許可しないようにすることもできる。大量のダウンロードを行うようなネットワーク乱用ユーザはネットワークの過負担時には自己制限をかけることができ、あるいはピアはノードが自己制限をかけるべきであることを表示することができ、あるいはピアはノードに自己制限をかけさせることを選択できる。

【００７４】

最後に、創発的モバイルネットワークは、この例における移動電話のみに限定されない。ノードの例としては、移動電話の中継塔とバックエンド装置、無線ルータとスイッチ、Bluetooth（登録商標）対応デバイス、そして移動電話の通信を可能にする他のあらゆる技術が挙げられる。創発的モバイルネットワークは、スポーツイベントなどによる回線混雑時や自然災害などによるネットワーク可用性の低下時において、レート制限を行うといったさらなる利点を有する。これらの特性により、創発的モバイルネットワークは、不利な事態に直面したときでも障害対応力がより大きくて生き残り可能であり続けることができ、また状況に自動的に対応し、ノード又は優先度を与えられた特定のノードにより大きい使用能力を付与することができる。

ネットワークガバナンス

【００７５】

本発明はまた、近隣ノード間のナーバスコミュニケーション（神経伝達、緊張の伝送）による以下のような他の応用をも示す。

【００７６】

・評判（風評）の投票、信頼度の投票、又はさらなる回避（even shunning）。ノードは、自らの現状の環境認識について判断をなすに当たって、相手の信頼度を評価する評価メカニズムを提供する。一例として挙げられるのは、鈍感なドメインコントローラを備えたウィンドウズアクティブディレクトリ環境や、ブリッジド・ネットワークとの相互接続性を要求するピアツーピア通信システムなどの、制御サーバの選択と高度さである。これらのシナリオのいずれにおいても、ノードは他のノードについて値の判定を行い、その判定には、他のノードからのデータを回避又は無視することを選択することが含まれる。

【００７７】

・本発明は、自然災害、内戦、禁輸及び制裁などリアルタイムの地政学的シナリオ及び状況に基づきインターネットガバナンスに影響を与える新しいモデルなど、複雑なシミュレーションのモデル化を含む。一連の既存のルールに基づくさらに迅速なガバナンス判断は、このモデルや本発明からの恩恵を享受できる。

【００７８】

・本発明は、財務モデル化を含み、あるいは何らかの定義された基準群に従った動作最適化さえも含み、その際に、あるモデルを使用する。経済学や計量経済学では、費用便益トレードオフ分析と効率性の問題を考慮する。サイバネティックス理論の他に、ゲーム理論、ゼロサム／ノンゼロサムゲームの適用も可能である。リソース消費のレベルを最大化

することもできるし、あるいはゲーム理論の又は経済学の視点からセキュリティアクティビティを最適化することもできる：ただし、ネットワークフェロモンのプリミティブコミュニケーション（基本的な、原始的な通信）は、ネットワークリソース利用料金を必要とする。これには、ナッシュ均衡とともにゲーム理論及び経済分析に対するさらなる研究が含まれ、ゲーム理論は分散型ネットワーク管理エコシステムの費用便益トレードオフ分析と効率性分析とに適用できるように構築される。これの一例では、ノードは、データベース内での財務取引である。

【００７９】

・最後に、本発明は、欺瞞又は悪意のある内部者の内部脅威に対して考え、確かに、プリミティブネットワーク通信メカニズムは操作可能なものである。実際、生物系は、寄生生物、疾病及び奴隷化による、同様の脅威にさらされている（Franks & Sudd、1987）。設計上、今日のネットワーク通信メカニズムにはいかなる認証メカニズムも含まれていない。これによって、開放的で、たくましく、スケールフリーのネットワークが実現するが、信頼の乱用による脆弱性を含む。システムの規模が十分大きく、参加中のノードの数が十分であれば、悪意のある内部のノードであっても単体ではエコシステム全体を操作することは不可能であると考えられていた。しかし、ボットネットや他の大規模制御メカニズムの発展に伴い、この仮説は有効性を失っている。

【００８０】

本発明の実装は、アーキテクチャ（構造様式）や組織により異なることもあるが、基本要素は同じである。エンドポイントが、管理環境下ではサーバに対する問い合わせとなり、非管理環境下ではユーザフィードバックとなり、本発明に示される創発的機能（emergent capability）はこれらの所産に取り入れられて、防御的意思決定過程を改善することができる。重要なことに、本発明が最も必要とされているのは非管理型のエンドポイント環境であり、この環境では、現時点においてどのベンダも、ローカル環境の状況認識に基づいく、攻撃対象領域の動的な決定はなしてはいない。

システム

【００８１】

本発明は、ネットワーク上の各コンピュータノードが個々にネットワークのセキュリティの共同管理に貢献することを可能にする、自己組織化的なマルチエージェントシステムを提供する。本発明は一連の３つの構造ブロックにおいて説明され、ここで各ブロックは、機能と粒度（granularity）との点で他のブロックを基礎とするものである。ブロック１（図５に示す）はノード単体の特性を説明する。ブロック２（５個のブロック１の集合体として図７に示す）は、近隣者と通信を行う５個のノードのインタラクションを説明するが、このインタラクションにおいてネットワークフェロモンはまだ介在していない。ブロック３（ブロック２に示すように通信を行う１８個のブロック１の集合体として図９に示す）は、ネットワークフェロモンの使用を介してそれぞれ最も近い近隣者と通信を行う１８個のノードのインタラクションに基づく創発的特性を説明する。ブロック３の出力は、防御目的の創発的ネットワークである。

【００８２】

本発明は、ネットワークノードがネットワークセキュリティ管理に関与することを可能にするものであり、基本的自己認識（primitive self-awareness）が考慮され、あるノード自身が、その現状の安全体制とローカルネットワーク環境とを「ナーバスネス（緊張性、神経質性）」と称されるステート（状態）で表現する。各ノードは、「ネットワークフェロモン」と称される基本的通信（プリミティブコミュニケーション）を用いて、自らの現状のプロファイルと近隣者のプロファイルとを評価する。この評価では、アドミニストレータが設定した一群の所定の健全性管理ルールが用いられる。正常な応答はノードの状態（ステート）の変更を含み、自らの環境に応じて、ノード自らのナーバス状態を緩和するようにルールを通じてノードの状態は設定される。

【００８３】

図１（ネットワーク緊張性評価）は、プリミティブコミュニケーションメカニズム（基

本的通信の機構、原始的通信の機構）と、各ノードにおいて繰り返されるステート変更（状態変更）を示す。図示されるように、創発的ネットワーク（emergent network）は、４つのステップ（１０２、１０４、１０６、１０８）のナーバスコミュニケーションが繰り返される。図示されるように、ネットワークは８個のノード１１０（各ノードは図１において小円として記される）を有し、ここで各ノードはその周りに円を伴っており、この円は最も近い各近隣者からナーバスの影響を受けるエリアを示す。この図が示すのは、これらの８個のノードのうちの１個のノード（１１０_{5}）であり、この１個のノードは図６に示すように自らのナーバスネスのレベルをゼロ、弱、中、強のナーバス状態の間で変更する。各ノードは自らのナーバスネスのレベルを近隣者と共有し、その後、自らの攻撃対象領域を削減することで自らのナーバスネスのレベルを低減させる。ノードの周囲の円で示されるように、ノード（１１０_{5}）に近隣するのはただ１個のノード、すなわちノード（１１０_{6}）のみである。しかしノード（１１０_{6}）の方は、３個のノード、すなわちノード（１１０_{7}）とノード（１１０_{8}）とノード（１１０_{5}）に近隣する。ノード（１１０_{9}）はいずれの近隣者も有していない。

【００８４】

各ステップ（１０２、１０４、１０６、１０８）はステップごとのシミュレーションであり、各ステートは次のステップでステートが変更される（時間の経過に伴い）まで待つ必要があることに留意されたい。第一のステップ（１０２）において、ノード（１１０_{5}）のナーバスネスは低であり、ノード（１１０_{6}）のナーバスネスはゼロである。次にステップ（１０４）では、最も近い近隣ノード（１１０_{6}）は高いナーバスフェロモンを（１１０_{5}）から受信しており、自らのナーバス性を低に引き上げる。ノード（１１０_{6}）はナーバスネスが低に引き上げられて、自らのナーバスフェロモンを放出する。ノード（１１０_{5}）のナーバスネスも続いて中に引き上げられて、このノード（１１０_{5}）も自らのナーバスフェロモンを放出する。ステップ（１０６）において、元のノード（１１０_{5}）はナーバスネスが強に引き上げられて、ナーバスフェロモンの放出を続けており、これによってノード（１１０_{6}）のナーバスネスは中に引き上げられる。ノード（１１０_{7}）と（１１０_{8}）はノード（１１０_{6}）からナーバスフェロモンを受信しているが、ノード（１１０_{5}）からは受信しておらず（ノード１１０_{7}と１１０_{8}はノード１１０_{5}と近隣していない）、そしてこの時点でノード（１１０_{7}）と（１１０_{8}）のナーバスネスは低に引き上げられる。

【００８５】

最後にステップ４（１０８）において、元のノード（１１０_{5}）は何らかのアクション（パッチング、更新、サービスの終了）を実行して、自らのナーバスネスのレベルを引き下げる。ノード（１１０_{6}）からのナーバスフェロモン、そしてノード（１１０_{7}）と（１１０_{8}）の相互からのナーバスフェロモンにより、ノード（１１０_{7}）と（１１０_{8}）のナーバスネスの上昇している。しかしながら、ノード（１１０_{9}）は、ローカルの近隣者ではないため、ナーバスネスの変更はない。この例において、ホストの初期条件（攻撃対象領域、ナーバスネスのレベル）はすべて同一である。攻撃対象領域とは、システム内のセキュリティ上の問題が起こる可能性の大きさを示すために計算される代替変数のことである。これは、問題１つ１つを定義する必要なしにシステム内のセキュリティ制御と脆弱性について議論する１つの方法である。

【００８６】

上記の例で、次の期間のステップ５に続くと、ノード（１１０_{5}）は今やより高い防御を有しているため、ノード（１１０_{5}）が、ノード（１１０_{6}）がナーバスになったことよってナーバスネスを増すことは必ずしもない。ノード（１１０_{5}）がノード（１１０_{6}）を沈静させることはないが、ノード（１１０_{6}）のナーバスネスを、より高いナーバスレベルへと移行させるのではなく、現状レベルのまま維持させる要因となるかもしれない。

【００８７】

ホストの初期条件、インタラクションに影響を及ぼすのに用いられる変数、そしてイン

タラクションのパターン、これらすべてが創発的特性（emergent characteristics）に影響する。図２（創発的ネットワーク防御のシステミグラム）はシステミグラムを用いてこのコンセプトを図示したものであり、創発的ネットワーク防御のシステムを導くシステムエンジニアリングのデザインフローを記載している。システミグラムはシステムエンジニアリング機能のテキスト表記に基づくものであり、この図形は、１つのパラグラフを完全に表記したものとして読むことができる。図２に示すシステミグラムは、手順チェックリストや戦術的な説明を意図したものではなく、本発明の非限定的な例示的実施形態を提示するものである。この例におけるシステミグラムは、左上部から右下部の方向にグラフ表示されたものであり、多数のバリエーションを通覧でき、そして複雑で相互関連したシステムのダイナミクスモデルのグラフィカルコミュニケーションを可能とする（Boardman & Sauser、 2008）。すべての動作が環境の要素を定義するため、すべての動作はすべてのブランチに沿って同時に移動する。

【００８８】

理解をより容易にするためにシステミグラムの特性を一般化させることもできる。定義的要素１、２、１１、１９、２１、２３、２５、２７、３７及び４３はすべて、不連続な各時点におけるホストの特徴（特性）を定義するものである。これらの各要素は、保存され、判定されてもよく、周囲に指定された種々のエリアから生成されるものであってもよい。近隣者の数はシステムそれ自体に保存され、図８ではＳ６と記載されている。この数は、図１のノード円の範囲内にあるノードの数を数えることによって判定される。それはシステムで定義されるものである。ホストは、それらを、固定した状態として持ち、必要とし、あるいは受け取る。

【００８９】

Ｆ４：攻撃対象領域の楕円（１２）は、攻撃対象領域を表すのに用いられる基礎的運用能力を示す。攻撃対象領域（Ｆ４）は、Ｓ１、Ｓ２、Ｓ３、Ｓ４、Ｓ５を含む。これらは、「セキュリティの健全性管理（セキュリティ健全性管理度、セキュリティ衛生度、security hygiene）」として知られる最低限の許容可能なセキュリティの基本水準を維持するためにシステムに実装される最低限の安全規制（セキュリティコントロール）である。創発的特性（１０）は、ＳＡＲＥＰＨと称されるアジャイルなシステムの特性（機動的なシステムンの特性）の基本セットを表し、これはR. Dove氏が、『パターン適格と、次世代型アジャイルシステム－セキュリティ戦略の諸例（Pattern qualifications and examples of next-generation agile system-security strategies）』、Presented at Security Technology （ICCST）、2010 IEEE International Carnahan Conference、2010、において議論しているところであり、その全内容は参照することで本明細書に組み入れられる。

【００９０】

ＳＡＲＥＰＨアジャイルセキュリティパターン（ＳＡＲＥＰＨの機動的なセキュリティパターン）は以下のものを含む：（Ｓ）自己組織化、敵対的攻撃に対処するための最も重要なシステム特性；（Ａ）順応性のある戦術、攻撃に応じて再組織化及び再構成すること；（Ｒ）反応的障害対応力（反応的な回復力）、未知の世界で動作して対応し、攻撃のショックを吸収して対応すること；（Ｅ）進化可能な戦略、よりタイトな学習ループを通じて挙動を修正すること；（Ｐ）積極的イノベーション、新規で斬新な防御及び攻撃技術；そして（Ｈ）調和的動作、この調和的動作は利用可能かつ相乗的なセキュリティ特性を構築するものであり、ユーザと環境内の他のノードとのインタラクションを可能とする。これら６つの特性のそれぞれが存在することによって創発的システムが有効化される。

【００９１】

フィードバック要素Ｆ１、Ｆ２、Ｆ３及びＦ４は、フィードバックループを介してステートマシンを形成するために用いられる。データ要素Ｓ１、Ｓ２、Ｓ３、Ｓ４、Ｓ５、Ｓ６は、ホストのカレントステート（現状状態）を計算し、フィードバックループに入力を与えるために用いられる。図１０に示すように、各データ要素は、実装する際に様々な構造ブロックが用いられる。図１０は、ブロック１においては、Ｆ４、Ｓ１、Ｓ２、Ｓ３、Ｓ４及びＳ５のみが動作のために必要である。しかしながら、ブロック３においては、す

べてのデータ要素が動作のために必要である。また、それは、それぞれの定義を示す。

【００９２】

図５のブロック１を参照すると、ホストはプロセッサを含む。ホストは、Ｓ１：エージェントの存在（２０）、Ｓ２：システム防御の更新（２２）、Ｓ３：システム基本水準の更新（２４）、Ｓ４：インバウンドサービス（２６）の増減、そしてＳ５：アウトバウンドサービス（２８）の増減、に基づき、Ｆ４：攻撃対象領域を計算して操作する。また、ホストは、自らのＦ１：内部ナーバスネス（７）を、Ｆ３：パラノイア（３）とＦ２：ネットワークナーバスネス（５）に基づいて計算する。またブロック１は、Ｆ２：ネットワークナーバスネス（５）の入力が組み込まれているが、この入力は最も近い近隣者を有するネットワークに組み入れられるまでは無関係である。

【００９３】

図７のブロック２を参照すると、ホストはプロセッサを含み、このプロセッサは、ブロック１（図５）で実行されるすべての機能を計算し、加えてＳ６：近隣者（１５）からのネットワークフェロモンによってＦ２：ネットワークナーバスネス（５）を計算する。これはホスト単体の特徴を全て実現したものである。以下に論じるように、図７はブロック２の理論的コンテクストダイヤグラムであり、詳細をさらに示すものである。ブロック２は、ブロック１（図５）で学習された初期コンセプトに基づく完全なモデルの実装を示す。ブロック２は、完全モデルが自己触媒的（autocatalytic）である、つまり当該モデルが自続的（self-sustaining）である、といういくつかの初期特性を含む。

【００９４】

図９のブロック３を参照すると、ネットワークは、創発的ネットワーク防御（図２の１８）を形成する各ホストのインタラクション内に現れる創発的特性（図２の１０）を有する。これは、いかなるホスト単体にも現れず、このネットワークの創発的特性である。

【００９５】

図２に戻ると、システミグラム中に各要素の詳細な説明が記載されており、そこには各要素における機能の説明も含まれている。フィードバック要素Ｆ１、Ｆ２、Ｆ３そしてＦ４は、フィードバックループを介してステートマシンを形成するのに用いられる。データ要素Ｓ１、Ｓ２、Ｓ３、Ｓ４、Ｓ５、Ｓ６は、ホストのカレントステートの計算に必要なものであり、フィードバックループの入力となる。

【００９６】

要素（２００）は、ネットワーク上のホストなどのノード要素である。ノード要素（２００）は、例えばコンピュータやプロセッサを有する電子機器（移動電話やＰＤＡなど）である場合もある。ノード要素（２００）はデータ要素（保存領域など）である場合もあり、多数のデータ要素が１つのプロセッサ又はＣＰＵで制御できる。ノード要素（２００）は攻撃対象領域を有する。図２は、ホストが直近の環境において、最も近い近隣者とインタラクトするときにホスト上で起こる諸機能を示す。

【００９７】

定義要素（１）は、ホストが自らのステートマシン内で計算された変数としてのＦ１：内部ナーバスネスの性質を有する（１）の場合に適用される。定義要素（２）は、変数としてのＦ３：パラノイアの性質をホストが有する（２）の場合に適用される。

【００９８】

フィードバック要素Ｆ３：パラノイア（３）は倍数（係数）であり、ポリシーにより設定される変数である。このポリシーは通常、人間の管理者が、ノードが何をなすべきかについての関数として設定する。例えば、ノードはハイリスク環境下にあるのか、それともローリスク環境下にあるのか。脅威の蓋然性が低い閉鎖環境ではパラノイアが低であってもよく、一方、脅威が多い開放環境はより「危険」であり、より高レベルのパラノイアを要求されてもよい。パラノイアは、Ｆ１：内部ナーバスネスとＦ２：ネットワークナーバスネスとに同時に影響を与える。

【００９９】

フィードバック要素Ｆ３：パラノイア（３）はＦ２：ネットワークナーバスネスを乗算

して（４）、Ｆ２：ネットワークナーバスネスによって定量化される直近のネットワーク環境の重要性に合わせる。ネットワークナーバスネスのわずかな変化が、ほとんど問題にならないこともあれば大きな問題となることもあり、またそれゆえ、ネットワークナーバスネスの重み付けにわずかな影響を与えることもあれば大きな影響を与えることもある。さらにネットワークナーバスネスの重み付けは、創発的特性の展開の仕方に影響を与える。パラノイアが多いネットワークは常時高いナーバスである場合もあり、そのようなネットワークは麻痺しているため、システム変更のためアドミニストレータの注意を求め、パラノイアの軽減を要求する。

【０１００】

Ｆ２：ネットワークナーバスネスというフィードバック要素（５）は、ホストのローカル環境内におけるナーバスな近隣者のすべてのナーバスフェロモンから計算されたナーバスネスである。この実施形態の目的上、出願人は基礎的な加算及び乗算による計算を採用したが、実施に固有の他のモデル化や計算モデルを採用することとしてもよい。Ｆ２：ネットワークナーバスネス（５）への入力は、Ｆ３：パラノイア（３）とＳ６：近隣者（１５）のナーバスフェロモンである。集められた近隣者のフェロモンを乗算して、カレントネットワークナーバスネスを求める。内部ナーバスネスに影響を与えるのはこれであり、ネットワーク上にそれが存在していることによって創発的特性が有効化される。

【０１０１】

Ｆ２：ネットワークナーバスネスの計算（５）は、その後、Ｆ３：パラノイアとＦ２との計算からの重み付けを用いた所定の計算アルゴリズム（上記「モデル」の項に記載）を介してＦ１：内部ナーバスネス（７）に影響を与える（６）。Ｆ１：内部ナーバスネス（７）は、ホストが計算したナーバスネスのレベルを表す変数である。これは、Ｆ２：ネットワークナーバスネスとＦ３：パラノイアの双方を加味して、どの程度のナーバスをホストが「感じて」いるかを示す。ホストの目的は、攻撃対象領域を削減したり、リスク曝露を制限したりするなどの複数のメカニズムを通じて、Ｆ１：内部ナーバスネスを軽減することである。Ｆ３：パラノイア（３）もまた、ポリシーが設定した係数として、Ｆ１：内部ナーバスネスに影響を与える（８）。

【０１０２】

Ｆ１：内部ナーバスネスの計算（７）しナーバスネスを軽減を目的とすることは、中央集中型の制御がないノード単体内の単純な要素であり、これが他のホストと組み合わされた場合、スウォーム理論で定義されるように、創発的特性が有効化される（９）。これが本発明の基本原則であり、すなわちナーバスネスを示すことによって真社会性の動物のモデルが形成され、創発的ネットワーク防御が可能となる。

【０１０３】

創発的特性は要素１０として示される。ＳＡＲＥＰＨの機動的（agile）セキュリティパターンは以下のものを含む：（Ｓ）自己組織化（４０）、敵対的攻撃に対処するための最も重要なシステム特性；（Ａ）順応性のある戦術（３４）、攻撃に応じて再組織化及び再構成すること；（Ｒ）反応的障害対応力（４６）、未知の世界で動作して対応し、攻撃のショックを吸収して対応すること；（Ｅ）進化可能な戦略（４２）、よりタイトな学習ループを通じて挙動を修正すること；（Ｐ）積極的イノベーション（３６）、新規で斬新な防御及び攻撃技術；そして（Ｈ）調和的動作（４１）、この調和的動作は利用可能かつ相乗的なセキュリティ特性を構築するものであり、ユーザと環境内の他のノードの両者とのインタラクションを可能とする。いかなる自己組織化的なマルチエージェントシステムとも同様に、機動的特性（アジャイル特性）は、訓練されていない観察者の目には複雑なシナリオとして映る。

【０１０４】

ホストはまた、変数Ｓ１、Ｓ２、Ｓ３、Ｓ４、Ｓ５を伴う攻撃対象領域のプロパティを有する（１１）。Ｆ４：攻撃対象領域（１２）は、攻撃対象領域への入力を計算するために用いられるデータである。これらの特性においては、セキュリティ健全性管理要素は、攻撃対象領域の計算を支援するのに用いられる最低限の要素である。Ｆ４：攻撃対象領域

（１２）変数は、内部ナーバスネス（７）を計算する入力（１３）となり、その計算はＳ２、Ｓ３、Ｓ４及びＳ５、Ｓ２及びＳ４の平均を取ってなされて、「内部ステート平均領域露出度（internal state average surface exposure）」変数を定義する。Ｓ４とＳ５との平均は、「ネットワークステート平均領域露出度（network state average surface exposure）」変数を定義する。ネットワークステート平均領域露出度と内部ステート平均領域露出度との平均は、Ｆ４：攻撃対象領域の全域を定義する。これが意味するところは、内部ステートなど１つの変数が増加して、ネットワークステートなど別の変数が減少したとしても、平均な攻撃対象領域の露出度はその均衡が維持されるということである。上記で参照したモデルに続いて、ノードステートsは攻撃対象領域を示し、内部攻撃対象領域とネットワーク攻撃対象領域の両方を含み、組み合わされ、このモデルの１つの指針となり、リソースの構成（configuration of resources）を維持する。カレントセキュリティポスチャ（現状の安全体制、current security posture）は脅威入力を含まず、既知の状態であるので、攻撃対象領域（１２）はパラノイアからの影響（１３）を受けていないことに留意されたい。Ｓ１：エージェントの存在（２０）変数を介して判定されるエージェントの存在は攻撃対象領域の計算には含まれず、なぜならエージェントが存在していない場合にはノードは創発的ネットワークの構成員ではなく、そのためナーバス計算を実行することもネットワークフェロモンを共有することもできないからである。ナーバスネス計算は、脅威入力を考慮している。

【０１０５】

本発明の一実施形態において、創発的特性（１０）は全近隣者の間に（１４）存在しかつ全近隣者の間で共通でなければならない。このことはブロック３（図９）にも示されている。Ｓ６：近隣者データ要素（１５）は、同様のホスト間の最も近い近隣者であり、創発的特性を有効化させるためにはある程度の量で存在している必要がある。創発的ネットワーク防御を含む創発的特性が発生するのは、単に、相互に通信可能となって創発的特性を有効化させる（１６）ことを可能とするのに十分な数のホスト（好適には少なくとも１５個程度だが、用途に応じてこれを前後することもあり得る）が存在すればよい。ホストはそれ単独では一匹の蟻のようなものであり、弱く、つまらない存在であり、多数の脅威にさらされ、極めて脆弱で、そして高いリスク下にある。創発的特性を進展させて示すことが、創発的ネットワークを形成する（１７）ことである。創発的特性を有する同様のホストのネットワークが、防御用の創発的ネットワーク（１８）となる。その結果であるシステムは、構造ブロック１、２及び３すべてを通じた創発的特性を具現化している。

【０１０６】

ホスト（２００）は、その内部ステートを計算するためにローカルに設置されたエージェント又は計算要素を有して（１９）いなければならない。カレントステートを計算する要素はＳ１：エージェントの存在（２０）変数であり、この変数がホストを創発的ネットワークの一部として識別する。ホスト（２００）は、群れの一部であって、ナーバスネスを計算するために、エージェントを有していなければならない。エージェントを有しないホスト（２００）は認識されないが、これは他のホストからの通信が遮断されていることを意味してもよい。ある場合には、エージェントを有しないホストは、強制的にエージェントをインストールさせられ、あるいはエージェントがインストールされるまで検疫され、あるいはネットワーク内の他のすべてのホスト及び制御ポイントから除去または隔離される。自ら及び最も近い近隣者におけるエージェントの存在（又はその不存在）は、攻撃対象領域の計算および内部ナーバスネスへの入力である。

【０１０７】

ホストはシステム防御を必要とする（２１）。Ｓ２：システム防御更新（２２）は、セキュリティデバイス及びセキュリティポリシーに対するシグネチャ更新を含む。これはアンチウイルス、侵入検出及びその他のシグネチャ（痕跡、署名的行動）、セキュリティツール、そしてシステム及びアプリケーションのパッチレベルを含む。ホスト構成は維持される必要がある（２３）。Ｓ３：システム基本水準の更新のデータ要素（２４）は、事前構成されたホストポリシーと現状のホスト構成との差を判定し、ここで現状のホスト構成

の例としては、インストールされた現状のソフトウェア、有効化された機能などの現状のアプリケーション構成、ハードドライブの暗号化などの現状のシステム構成、ジオロケーション、許可されたユーザの数、実行されたユーザアクション、ファイアウォール構成とアンチウイルス感度などのシステム防御のカレント構成、そして他の多くのシステム基本水準の構成がある。これらは通常、最新のパッチレベルやシグネチャに依存するものではないことから、システム防御としては考えられておらず、むしろ予め定義されたポリシーに基づく定常構成として考えられている。

【０１０８】

ホスト（２００）は、他のホストが自らに接続することを許可するが、これによって自らの攻撃対象領域が増加する（２５）。Ｓ４：インバウンドサービスのデータ要素（２６）はポート、プロトコルおよびアプリケーションを含み、ホストがオープンして、他のホストがアクセス、問合せ及び接続のを許可する。これらは、クライアントホスト上でのピアトゥピア・ネットワーク探索、又はウェブサーバ上で稼働中のサービスを含んでもよい。インバウンドサービスは一般的であるが、ポート上で稼働中のアプリケーションの個々の特性、例えば特定ユーザによる、限定されたアプリケーション情報のみに対するアクセスを許可することなどを含んでもよい。これはインバウンドサービスを「オン」と「オフ」とで切り替える二進法的な決定ではなく、レート制限、特定データへのアクセス制限、ホストへの要求の誤り、ミスリーディング、欺瞞的なデータ又は悪意のあるデータの供給、そして他の多数の通常使用される防御的戦術を含む、一連の選択肢の間で動的に変更し得るものである、ということに留意することは重要である。誤りとは１００％正しいデータではないことを示す；ミスリーディング（誤解）とは、事実としては正しいがその提示が別の結論に到達するような仕方でなされた故意に修正されたデータのことである；欺瞞とは、故意に不正確にされたデータであって、ユーザを騙して他のサービスに誘導するよう意図されたデータのことである；そして悪意とは、リモートホストに取り込まれてある機能を実行するよう意図されたデータのことであり、ビーコン（案内役）であることもあり、破壊的であることもある。

【０１０９】

ホストは他のホストに接続し、そしてＳ４（２６）及びＳ５（２８）が認識するところの自らの攻撃対象領域を増加させる（２７）能力を有する。Ｓ５：アウトバウンドサービス（２８）は、直近の環境及びローカルネットワークにおいて、対内及び対外の両方でなされる様々なサービスへのアクセスを有するポート、プロトコル、アプリケーションを含む。

【０１１０】

Ｆ１：内部ナーバスネス（７）は、S2:システム防御更新（２２）の更新周期の時間を決める。通常のシステム防御は定期的なスケジュール（時間、日、週）に基づいて更新を行う（２９）が、このスケジュールは内部ナーバスネス（７）によって操作される。Ｆ１：内部ナーバスネス（７）は、また、現状のS3:システム基本水準構成（２４）の変更を行う（３０）。メンテナンスのスケジュールの変更の他に、現状のシステム基本水準を動的に変更することで攻撃対象領域を削減することができる。これは、ジオロケーション、現状のユーザ、インストール又は構成された現状のアプリケーション、ホスト上で及びホストを介して保存又は送信された現状のデータ、システム防御ツールからの現状（現行）のアラート、そしてホスト及びサーバポリシーツールによって構成され得る他のポリシー要素に基づくホストポリシーの変更を含む。また、Ｆ１：内部ナーバスネス（７）は、Ｓ４：インバウンドサービス（２６）の可用性（利用性）を減少させる（３１）。制限は、ポートへの又はアプリケーション上の特定の要素へのアクセスが認められる帯域や地理的位置、ホストされた単複のアプリケーションの異なるインスタンスに異なるユーザがアクセスできるようにする帯域や地理的位置に対する制限を加え、異なるデータを異なるユーザに示すといった制限を含んでもよい。この点は、上記モデルの項において、ノードリソースをノードリソース自身の構成にマッピングすることを示すノードステートs∈Sとして論じられている。この場合、リソースは上述の制限（帯域、ポート）を含むが、これらの

例のみに限られるというわけではない。制限は、現状の環境に適し、適用可能である各Ｓ１：エージェント（２０）内で定義されるいかなる要素を含むこともできる。ノード構成がナーバスオペレータ（ＮＯ）を通じて変化するにつれて、各ノードは、図６に示すように構成セキュリティのステート$Conf_c$：$Conf_M \rightarrow Conf_{M+1}$を、$Conf_{Low}$から$Conf_{Moderate}$、$Conf_{High}$に変化させる。

【０１１１】

Ｆ１：内部ナーバスネス（７）は、また、同じアルゴリズム（上記モデルの項参照）を用いて、アウトバウンド方向に認められたサービス（２８）の数を減少させ（３２）、それによって、ナーバスオペレータ（ＮＯ）を介してリソースを構成にマッピングし、ナーバスネスアセスメント（ＮＡ）に基づいて攻撃対象領域（１０）を変更する。これは、現状の動作環境に適用でき、ホストを特定のウェブサイトへのアクセス、特定の電子メールの送信、そして特定のプロトコルを介した通信に限定できる。しかしながら、アウトバウンドサービスを更に減少させる選択肢としては、システムの基本水準の更新と関連するが、例えば、ボットネットの緩和などでホストの出力を制限したり、イーサネット（登録商標）、ワイファイ、WiMax、BlueTooth（登録商標）及びその他のレイヤ１のプロトコルなどの通信プロトコルを限定することを含む。

【０１１２】

Ｓ４：インバウンドサービス（２６）と、Ｓ５：アウトバウンドサービス（２８）との両方を操作することにより、ホストは自らの攻撃対象領域を、Ｓ２：システム防御（２２）と、Ｓ３：システム基本水準（２４）とを更新するよりも速く、迅速な仕方で、動的に調整する（３３）ことができる。ホストの入出力の許可を動的に操作することによる迅速な対応により、防御目的の順応性のある戦術（３４）が形成される。順応性のある戦術：ホスト（３４）は、それらの防御体制と防御アクティビティを決定する単純なルールを用いて、防御体制を修正することができる。これらが含むことは、特定のサイト又はアドレスのブロッキング、サービスの無効化、そして、更新サイクルの増加であり、これらはネットワークナーバスネスを介した近隣ホストからの入力に基づき、これらのベクトルに関する脅威についての具体的な知識が存在していなくてもよい。

【０１１３】

攻撃対象領域を動的に変更することによって、ホストは自らの特性を迅速に変更（３５）できるようになり、このことは革新的な防御メカニズムの発展を積極的に支援する。例えば、ナーバスオペレータ（上記モデルの項参照）を用いて、ノード構成は自らの攻撃対象領域のスコアを自主的に増減させることができる。内部攻撃対象領域（Ｓ２、Ｓ３）とネットワーク攻撃対象領域（Ｓ４、Ｓ５）とを平均することで、Ｆ４：攻撃対象領域（１０）が求められる。これが意味するところは、内部攻撃対象領域が増加しても、ネットワーク攻撃対象領域を減少することにより攻撃対象領域（１０）全体としては減少できるということである。このようなケースが発生し得る例としては、ノードがレガシーシステムの一部をなしていて、システムの更新及びパッチングが既存のシステムを破壊してしまう恐れがあり、現状のパッチレベルへの更新が不可能な場合が挙げられる。期限が切れたＳ２：システム防御更新とＳ３：システム基本水準更新とによる脆弱性は、アドミニストレータがネットワークトラフィックなど他のセキュリティ制御を増加させることによって緩和されるであろう。創発的ネットワーク防御を用いると、ノード上のエージェントは、攻撃対象領域を、特にこの場合であればノードネットワーク攻撃対象領域を減少させることによって、ノードナーバスネスを減少させようと試みるであろう。攻撃対象領域を操作するこの例は、上記で説明したように、人間の管理者からの入力なしに、プロセス（上記モデルの項参照）の一環として自動的に発生し、攻撃対象領域全体を減少するであろう。これは、創発的シナリオにおける革新的な防御メカニズムの例であり、創発的ネットワークが、おそらく未だかつて考えられていなかった新しいユニークな方法で、知られざる脅威から自らを防御することを可能にする。また、創発的シナリオにおけるホストは、スタンドアロンのノードと比べて、注入された攻撃に対する障害対応力と回復力が大きく、相互に迅速に警告し合う近隣者の能力によるものであり、自らのノードが攻撃の標的となる前

に防御体制を強化することができる。これらは積極的イノベーション（３６）及び防御の例である。積極的イノベーション（３６）とは、ネットワークナーバスネスを用いることにより、システムが自らの反応と応答時間とを遅くし、その結果として、システムにパッチを適用したり、又はその他の方法で修復するまで、ネットワークとの通信を厳しく制限したり、ネットワークから切断したりすることができる。これは、ブロック２（図７）に示される１つの創発的特性である。

【０１１４】

ホスト（２００）はまた、自らの近隣者から受信したナーバスフェロモンを数える（３７）。ホストは近隣者からのナーバス信号を受信できるようになっている必要がある。各近隣者が１つのナーバス信号を同時に放出していれば、ホストは自身が何個の近隣者を有する（数えられる）のかを知ることになる。ネットワークフェロモンは共通の放送媒体を介して最も近い近隣のホストに集められ（３８）、近隣のホストもフェロモンの数を数える。各ホストはナーバスフェロモンを数えて、上述のようなアルゴリズムを介してＦ２：ネットワークナーバスネス（５）を計算するための入力とする。

【０１１５】

Ｆ２：ネットワークナーバスネスのフィードバック要素（５）は計算され、ホストステートマシンに取り込まれ、最も近い近隣者の間で創発的特性（１０）を有効化し（３９）、それらは各々の内部ナーバスネスを共有する。

【０１１６】

自己組織化特性（４０）とは、中央集中型のポリシー制御なしに、ホスト（２００）のノードが自らの環境下においてローカルインタラクションを通じて自己組織化アクティビティを実行することである。このシステムは、人間又は中央集中型管理システムが実行する場合と比べて、攻撃又は環境変化により迅速に対応する。調和的動作の特性（４１）は、同一セットの単純なルールに従うことにより、組織的なポリシーの定めた、良好な健全性管理の趣旨を反映し、ノード同士が共有のセキュリティ目標及びルールのセットを持ち、伝達することである。蟻と同様に、中央集中型の制御を持たないが、すべて同じ目標を有し、それは安定と、障害対応力と、調和の取れた環境が実現することである。

【０１１７】

進化可能な戦略特性（４２）とは、更新サーバを過負荷状態にさせないために、従来型のセキュリティ管理モデルでは、多くのホストが更新周期を２４、４８、７２時間又はそれ以上ずらし、あるいは大規模ネットワークがホスト更新を順次行うようにしている。しかしながら、あるホストが最近の更新によって自らのシステム上でマルウェアを検出した場合でも、他のホストは直ちにサーバをチェックして自らの最新の更新情報を得るわけではない。これは、重要な（クリティカルな）更新が利用可能になったときにパッチングの周期を低減できることである。このことは本発明を通じて、パッチングの周期を低減することにより、攻撃対象領域の露出度を低減することによって示される。

【０１１８】

ホストを標的（４３）とする脅威（４４）には、自然の脅威（洪水、火事、地震、リスなど）と人間による脅威（ハッカー、窃盗、スパイ行為、破壊工作など）の両方がある。脅威が存在しなければ、セキュリティの必要性はなくなるであろうから、脅威＞０であるはずである。本発明は、既知のそして未知の脅威、存在するそして存在しない脅威、自然の脅威、人間による脅威、コンピュータによってそして人間からの指令によって引き起こされる脅威（４４）に対処する。多くのセキュリティ上の失敗の根源をなすのは、システムの状態及びリスク管理が根本原因ではなく、具体的な脅威への対処である。本発明は、ネットワークノードにおけるローカル環境の基本的認識に注目し、大規模ネットワークのセキュリティ管理の実効性と効率性を向上させるものである。実効的なセキュリティ管理とは、潜在的な攻撃がその最終目的を達成する可能性がより低いことを意味し、この計算のために（１）攻撃対象領域を代替変数として用いる。効率的なセキュリティ管理は、自動決定によって脅威への対応がより迅速になされ得るということを意味し、この自動決定は、（２）アクションが取られるスピードを表す代替変数と（３）人間のオペレータに課

題が通知されるスピードを表す代替変数を用いてなされるローカル環境評価（ローカル環境アセスメント）に基づく。これは、上記モデルの項で詳細に説明したように、創発的特性をノードに適用することによって達成される。

【０１１９】

これらの脅威に対処するため、本発明は、反応的障害対応力（４６）機能で対応（４５）して、攻撃やセキュリティ侵害に直面したとしても、正常な動作を可能にする。反応的障害対応力の特性（４６）とは、群れの中のホストが、攻撃対象領域の増加に伴うナーバスネスの増加に対する認識を有し、その結果、ホストの防御体制を動的に変更することである。例えば、攻撃者が既知のシグネチャを作動させることはないが、攻撃対象領域を増加すると複数のホストを通じてネットワークナーバスネスが増加し、ナーバスネスのレベルを上昇させ、それによって防御体制を強化する。防御体制が強化されるにつれて、ナーバスネスのレベルは低下し、システムは定常状態に戻る。攻撃が明確に識別されないこともあり得るが、ナーバスネスのレベルは防御体制を強化し未知の攻撃を緩和する。ナーバスな近隣者に反応する感度は、ホストの「パラノイア」レベルを変更することによって修正できる。パラノイア（３）は、ノードがどの程度自らの近隣者のナーバスネスを考慮して自らの世界の計算をするのかを示す倍率である。パラノイア特性は、ホストがどの程度近隣者に反応するかに影響する。ホストは、プリミティブコミュニケーションを用いて自らと自らのローカルネットワークのナーバスネスとを比較し、カレントステート（現状状態）を共有し、自らをできるだけ健全に維持し、自らのパラノイアのレベルに基づき近隣者からの影響を考慮する。

【０１２０】

１つの非限定的な例示的実施形態において、システミグラムは次のように読み取ることができる：ホスト（２００）は、あるレベルのＦ１：内部ナーバスネス（７）を有し（１）、あるレベルの（２）Ｆ３：パラノイア（３）を有し、このＦ３：パラノイア（３）でF2:ネットワークナーバスネス（５）を乗算（４）してＦ１：内部ナーバスネス（７）に影響を与える（６）。上述のように、ナーバスネスは計算値であり、パラノイアはポリシーベースの性格（属性）を持つ。例えば、パラノイア（３）は機密情報を扱う施設ではアドミニストレータが「高」に設定でき、一方でパラノイアは幼稚園では「低」に設定できる。午前３時に道を歩いているときのパラノイアは午後３時よりもはるかに高くなるであろうし、ナーバスネスが同じで計算すれば、ナーバスネスの計算結果も高くなる。さらにＦ３：パラノイア（３）は、Ｆ１：内部ナーバスネス（７）に影響を与え（８）、創発的特性（１０）を有効化する（９）。ホスト（２００）はＦ４：攻撃対象領域（１２）を有しており（１１）、このＦ４：攻撃対象領域（１２）はＦ１：内部ナーバスネス（７）に影響を与え（１３）、またこのＦ１：内部ナーバスネス（７）もまた創発的特性（１０）を有効化する（９）。これらの創発的特性（１０）はＳ６：近隣者（１５）の間に（１４）存在しており、このＳ６：近隣者（１５）もまたこれらの創発的特性（１０）を有効化し（１６）、最終的には創発的ネットワーク防御（１８）を形成する（１７）。これらの特性はすべて存在しており、つまりこれらの特性は上述のアクティビティから生じるということである（すなわち創発的挙動：複数のエンティティがプリミティブ機能性を伝達し合うときに協同的挙動が生じる）。

【０１２１】

別の例では、ある１つのドキュメントがＳＡＲＥＰＨ（１０）フレームワークから示された創発的性質を含むことができ、またドキュメントの創発的ネットワークを作成してドキュメントを防御できる。ドキュメントは、暗号化や、開く、コピーする、印刷するなどのユーザの権限及び特権などのセキュリティ属性をますます帯びるようになっていて、そうしたドキュメントをネットワークデータの送受信に用いることができる。創発的ネットワーク防御システム用の同じシステミグラムをたどるのであれば、ドキュメントを開くプログラムがこれらの創発的性質をサポートする限り、ドキュメントが攻撃対象領域のプロパティを有していればよい。これは、ドキュメントを暗号化し、特定のプログラム（Microsoft Word、Adobe Acrobat）のみにドキュメントの開封を許可することにより容易に対

処できる。防御的更新とベースライン更新は、アプリケーションのバージョンのレベルとドキュメント使用に関するポリシーとを含む。インバウンドサービスとアウトバウンドサービスは、ユーザと他のサービスとが、開く、コピーする、印刷する、参照する、リンクする、データを抽出するなど、どのようにしてドキュメントとインタラクトするかを示す。ドキュメントは、自らの直近のローカル環境に基づいてナーバスネスを理解できる、すなわち、ドキュメントが既知のネットワーク又はホスト内にあるのか、あるいは創発的性質を有する既知のホストもドキュメントも他に存在しない未知のネットワーク内にあるのか。基本的に、ドキュメントにアクセスするソフトウェアが創発的性質をサポートしている限りにおいて、このコンセプトは、創発的ネットワーク防御用のいかなるネットワーク対応のエージェントベースのシステムにも適用し得る。

【０１２２】

このシステミグラムは、前述の創発的モバイルネットワークなど、いかなる創発的ノード用の各用途について適用し得る。考えられる用途の一例は以下のとおりであり：移動電話（２００）が、前述した脆弱性の各パラメータからなるＦ４：攻撃対象領域（１２）を有する（１１）。これらは、物理的なセキュリティと、ファームウェア、オペレーティングシステム及びアプリケーションの更新と、安全なセキュリティ上の行為の実施を含む。この例においては、移動電話（２００）は、まず、創発的ネットワークの一部をなす当該電話上において、Ｓ１：エージェントの存在（２０）を有して（１９）いる必要がある。このエージェントは、ファームウェア、オペレーティングシステム、又はインストールされたアプリケーションの一部であってもよい。このエージェントは、図５のナーバスステートアセスメントを可能にする。移動電話（２００）はまた、安全なセキュリティ上の行為を奨励するために機能及び能力に制限を加えるなどのＳ２：システム防御更新（２２）をも必要とする（２１）。ここで、各システムが定期的なメンテナンスを必要とする点に留意されたい。例えば、あなたのコンピュータ上でアンチウイルスソフトウェアが稼働しているとしよう。アンチウイルスソフトウェアの有効性は、あなたがアンチウイルスディクショナリを最後に更新したときの状態のままである。このことは、ユーザが注意を払ってソフトウェアを更新するのを待つのではなく、企業が更新をプッシュし始めるまでは、問題であった。「必要性」（２１）の判定がなされるのは、（ａ）タイマーが切れたとき、そして（ｂ）更新が取得可能になったときである。創発的システム下では、「必要性」の判定はナーバスネスによってなされ、その判定の時点においてノードは更新の有無をチェックする。更新が見つからなかった（１は存在するが２は存在しない）場合、ノードは他のアクションを取って（例：ポートを閉じる）、攻撃対象領域を、ひいてはナーバスネスを減少させる。

【０１２３】

移動電話の例を続けると、移動電話（２００）はＳ３：システム基本水準の更新（２４）をも必要としており（２３）、これは構成、ファームウェア、オペレーティングシステム又はアプリケーションの更新を含む。ホストは、自らの基本水準の構成の更新を必要とする（２３）。取得可能になると更新（３０）がなされる。ナーバスネスのレベルに応じて、ノードは基本水準の更新の有無をチェックし、又はナーバスネスを減少させるように自らの基本水準を操作する。移動電話ではなくパーソナルコンピュータの例の場合、コンピュータは、セキュリティパッチを含む定期的なソフトウェアメンテナンスを必要とする。ウィンドウズ（登録商標）の場合、このメンテナンスがなされるのはせいぜい月に一度である。マッキントッシュの場合、更新はこれよりも頻繁ではないが、それでもパッチをダウンロードしてインストールし、ハッカーがシステム上における無パッチ状態の脆弱性を利用することを防ぐ必要があることに変わりはない。内部ナーバスネスの計算は、その一部は、定期メンテナンスが実行されてからどれくらいの期間が経過したのかについての評価に基づきなされる。

【０１２４】

最後に、時間の経過とともに、移動電話（２００）上のエージェントは、ユーザが取得可能となったＳ４：インバウンドサービス（２６）の量を増加させ（２５）ることによっ

て、ユーザが、（例えば、移動電話がテキストメッセージを受信できる環境下にある場合に）新たに取得可能となったサービスを介してより多くのデータと接続を受けられるようにする。これらが含むサービスは、例えば、どの種類の無線ネットワークに移動電話が接続しようとしているか、移動電話が接続を許可しようとしている機器（ペアリングされていないBluetooth（登録商標）のスキャンなど）、移動電話上で稼働するサービスであって他のノードに移動電話への接続を許可するサービス、そしてＳＭＳ、ＭＭＳ、ウェブ、電子メール及び電話など、どの型式のメッセージを移動電話が受信するか、である。具体的には、ユーザはＳＭＳメッセージを、ユーザのネットワークに待機させて電話機で受信できる状態にすることができるが、電話機上のエージェントは、ナーバスネスが攻撃対象領域を十分に減少させて、ＳＭＳメッセージの受信をＳ４：インバウンドサービス（２６）に許可できる状態になるまでは、これらのメッセージの受信と表示を許可しない。このことが今日発生するのは、移動電話が地下のように信号のない環境下にあるとき又は電話の電源が切れているときである。別の例として、ローカルのBluetooth（登録商標）機器が電話への接続用に使用可能である場合があり得るが、電話上のエージェントは、ナーバスネスが攻撃対象領域を十分に減少させて、Bluetooth（登録商標）の接続をＳ４：インバウンドサービス（２６）に許可できる状態になるまでは、Bluetooth（登録商標）からの接続を許可しない。

【０１２５】

これらの例が実装されるのは、移動電話やパーソナルコンピュータのような、具体的なホストの環境に依存する、個別の、粒的なインスタンスにおいてである。移動電話（２００）上のエージェントは、ユーザに開放されるＳ５：アウトバウンドサービス（２８）の量を増加させ（２７）、それによってユーザは、新規に取得可能となったサービスを介してより多くの接続を開始し、また、より多くのデータを送信することが可能となる。このサービスの例としては、どのウェブサイトにユーザが訪問する可能性があるか、ユーザが送信する可能性のあるメッセージの種類、そして移動電話が接続先として選択する無線ネットワーク及び無線機器の種類などである。具体的には、移動電話は、その移動電話が十分にパッチングされておりかつ、ナーバスネスが十分に低く、よりリスクの高い無線接続を許可してネットワーク攻撃対象領域を増加させてもよいレベルを確保していない場合、公共の暗号化されていないWiFiなど特定の無線ネットワークへの接続を制限されることがある。電話が、エージェントによって承認されたレベルまでナーバスネスを減少させた状態になると、パラノイアの現状レベルが設定された後、ユーザはリスクのある無線接続先への接続を許可される。

【０１２６】

これまでＦ１：内部ナーバスネス（７）、Ｆ２：ネットワークナーバスネス（５）、Ｆ３：パラノイア（３）及びＦ４：攻撃対象領域（１２）のホストフィードバックアクティビティについて論じてきた。以下では、Ｓ２、Ｓ３、Ｓ４及びＳ５を介してＦ４：攻撃対象領域（１２）の操作という対応挙動が、Ｆ１：内部ナーバスネス（７）にどのように影響する（１３）のかについて論じることにする。上述したように、攻撃対象領域は、ネットワーク攻撃対象領域と内部攻撃対象領域の集合変数であり、そのため、システムパッチの有無を最後にチェックしたときからの時間の増加と、インバウンド及びアウトバウンドコミュニケーションへの制限とによる攻撃対象領域露出度に関連する。攻撃対象領域は、良好なセキュリティの健全性管理が確立した基本水準からの分散値として測定することができ、これは、直近の更新、最新のパッチ、そして最も制限されたインバウンド及びアウトバウンドサービスを含む。攻撃対象領域が良好な健全性管理から逸脱すると、Ｆ１：内部ナーバスネス（７）の増加を通じてノードナーバスネスのレベルに影響を与える（１３）。これは、現状の攻撃対象領域の構成をＦ２：ネットワークナーバスネス（５、６）のレベルをＦ３：パラノイア（３、８）の倍率で乗算することで求められる。これは上記モデルの項において、ノードＡのナーバスネス$An = conf_m \cdot Nerv_n \cdot Par_m$として計算されている。

【０１２７】

例えば、ノードのパラノイアが１であり、ネットワークナーバスネスが４１０であり、そして攻撃対象領域の構成が０．１７であるとき、ノードナーバスネスは６９．７となる（すなわち、４１０×０．１７＝６９．７）。移動電話の例に限ると、移動電話のパラノイアが１、そしてネットワークナーバスネスが４１０と比較的高い値で設定されるとき、その移動電話は、自らの攻撃対象領域を減少させて自らのナーバスネスを減少させ、ＭＭＳメッセージではなくＳＭＳメッセージを許可する。

【０１２８】

さらに一般的には、Ｆ１：内部ナーバスネス（７）は、次に、シグネチャの更新など、現状のＳ２：システム防御更新（２２）を更新する（２９）。また、Ｆ１：内部ナーバスネス（７）は、現状の基本水準ポリシー（ベースラインポリシー）に対して得られるＳ２：システムベースライン更新（２４）をも更新する（３０）。また、Ｆ１：内部ナーバスネス（７）は、Ｓ４：インバウンドサービス（２６）とＳ５：アウトバウンドサービス（２８）の変数をも減少させて（31、３２）、上述のように、時間の経過とともに生じるサービス可用性の増加（２５、２７）に対応できるようにする。これらのサービス間のバランス調整によって、環境変化に自動的に対応して、所望のレベルのナーバスネスを、ひいてはセキュリティを維持する順応性のある戦術（３４）が作成される（３３）。またＦ４：攻撃対象領域（１２）の計算は、最小化関数として攻撃対象領域を動的に監視して調整することによって、脅威への積極的かつ革新的な対応（３６）のサポート（３５）も行う。

【０１２９】

最後に、図９のブロック３に示したように、創発的特性（１０）の残りの要素は、創発的ネットワーク防御（１８）の能力を発展するものである。（我々の例では）第１に、移動電話（２００）は、自らのローカルのＳ６：近隣者（１５）の数を数え（３７）、その集合（３８）を用いてF2：ネットワークナーバスネス（５）を計算しなければならない。このフィードバックは、フィードバックループを形成して、またナーバスネットワークの自己組織化（４０）を可能にすることによって、創発的特性（１０）を有効化する（３９）。これが意味するところは、ナーバスネットワークは外部からの案内や指示を受けることなしに、独自にインタラクションを行って情報を交換することができるということである。さらに、ナーバスネットワークは、調和的に動作（41）する必要があり、同一の単純なルールのセットに従い、伝達し合い共有されたセキュリティ目標及びルールのセットを有し、そして、厳格なルールではなく、直近の状況に基づいたナーバスネスのレベルなどの動的な変数を介して、進化可能な戦略（４２）が用いられる。最後に、移動電話（２００）は脅威（４４）の標的になる（４３）ものである。そうした脅威は、窃盗のような物理的脅威やハッカーのようなデジタルな脅威であってもよく、有効なＦ４：攻撃対象領域（１２）のいずれの要素を標的としてもよい。

【０１３０】

しかしながら、脅威（４４）の如何に関わらず、移動電話（２００）は、弾力的に反応する（４６）ことが求められる（４５）。移動電話にとって、既知及び未知の脅威への弾力性のある対応（４６）が、ある移動電話が動作期間全体にわたり有効かつ継続して機能する特定の特性を携帯電話に与える基本的な手段である。例えば、移動電話は、バックアップシステムと、他の機能が動作できるようにシャットオフされる非必須の機能とを有する。例えば、移動電話において９１１番にダイヤルする能力は、キャリアや定期購読サービスの如何に関わらず、常に存在していなければならない。しかしながら、創発的移動電話ネットワークは、緊急通話（９１１）、優先通話（ＧＥＴＳ－政府緊急通信サービス（Government Emergency Telecommunication Service））及びＷＰＳ（無線優先サービス（Wireless Priority Service））をサポートするために、許容されるネットワークデータと輻輳（混雑状態）の量を削減することもある。障害対応力（回復力）に関わるその他の問題としては、Bluetooth（登録商標）、近距離無線通信（Near Field Communications）及びピアツーピアWiFiなどの予め定義された非必須のサービスを無効化することが挙げられる。また反応的回復力は、状況に応じて必須のアプリケーションと非必須のアプリケー

ションとを識別することも含む。非必須のアプリケーションの例にはゲームがあり、必須のアプリケーションの例には電話、ステムサポート（stem support）、ＧＰＳ、そしてTwitterやFacebookなど特定のメッセージング機能がある。この例示をさらに続けると、反応的障害対応力により電話で可能になればであるが、テキストのみの機能（画像なし）をサポートすることによりFacebookのアプリケーションに障害対応力を持たせてもよい。

【０１３１】

このように、反応的対応力（４６）では、Ｓ６：近隣者（１５）のF４：攻撃対象領域（１２）に対する注目が高くなることにより移動電話（２００）のナーバスネスが上昇し、その結果、移動電話（２００）の防御行動に動的な変更がなされてもよい。例えば、脅威（４４）が既知のシグネチャを作動させることはないが、すべてのＳ４：近隣者（１５）におけるF４：攻撃対象領域（１２）の増加は、ネットワーク状況認識に対し、より集合された（３８）見方を提供し、ひいてはＦ２：ネットワークナーバスネス（５）に影響を与えることになる。ホスト（２００）の数が多ければ多いほど、ネットワークを通って反応を検出したり共有する機会が増え、Ｆ２：ネットワークナーバスネスのレベルが上昇し、創発的特性（１０）が有効化される（３９）ため、最終的には、創発的ネットワーク防御（１８）の形成（１７）によって防御体制が強化される。

【０１３２】

「ローカル」という用語は、前記ノードと近隣者との間の所定の近さのことを指し、この所定の近さは物理的近さ、論理的近さ、ネットワーク・ホップ、ネットワーク・リンク、又は頂点分析（vertices analysis）に基づく近さのいずれかによって測定される。図４（ナーバス状態の例）に示すように、センターノードと５個の最も近い近隣者（Ａ、Ｂ、Ｃ、Ｄ、Ｅ）の例を検討する。破線は、物理的近さに基づく「近隣者」の任意の判断基準を示す。センターノードは、Ａ、Ｂ、Ｃ、Ｄ及びＥから集められたネットワークナーバスネスに基づき、自らの内部ナーバスネスを計算する。Ａ、Ｂ、Ｃ、Ｄ及びＥをリンクする具体的なネットワークアーキテクチャは、この例では考慮されていない。

【０１３３】

しかしながら、図３は、ネットワーク近さ（network closeness）の測定基準としてのネットワーク・ホップ又はネットワーク・リンク又は頂点解析を用いる。この図が示すのは、２つのアーキテクチャ表現であり、一方はネットワーク近さに基づき、他方はもっとも近隣者の計算のための抽象的近さに基づくものである。物理的な近さ（距離）を最も近い近隣者の近さの代わりに用いたとしても、本発明の適用対象を特定型式のネットワークアーキテクチャに限定しようとしているわけではない。むしろこの抽象化は、本発明がいかなるアーキテクチャにも適用可能であることを示している。階層的アーキテクチャ（１２０$_1$）におけるセンターノードは５個の近隣者を有する；部分接続メッシュアーキテクチャ（１２０$_2$）におけるセンターノードは２個の近隣者を有する；リングアーキテクチャ（１２０$_3$）におけるセンターノードは２個の近隣者を有する；完全接続メッシュアーキテクチャ（１２０$_4$）におけるセンターノードは２個の近隣者を有する；スターアーキテクチャ（１２０$_5$）におけるセンターノードは２個の近隣者を有する；バスアーキテクチャ（１２０$_6$）におけるセンターノードは２個の近隣者を有する；無線アーキテクチャ（１２０$_7$）におけるセンターノードは３個の近隣者を有する。抽象化されたアーキテクチャは、この実施例及び実施形態の目的上、同じニーズに応える。抽象アーキテクチャ１２０$_8$の近隣者は０個であり、抽象アーキテクチャ１２０$_9$の近隣者は２個であり、抽象アーキテクチャ１２０$_{10}$の近隣者は４個であり、抽象アーキテクチャ１２０$_{11}$の近隣者は５個である。

【０１３４】

このダイヤグラムは、ネットワークアーキテクチャにおいて、地理的近さと論理的近さは必ずしも同じではないということを示す。そのため、一般的な意味において抽象化すると、この実施形態は地理的近さに基づいた位置関係を示すのに対し、具体的に実装する場合は論理的近さが用いられる。このシミュレーションにおいては、ネットワーク・リンクの具体的な数は検討もモデル化もされておらず、それゆえリンクの解析は除かれているが

、その代わりに、各ノードの半径内にある最も近い近隣者の数が代替変数として用いられている。

【０１３５】

図５のブロック１の一部として識別されるノードの能力及び特性の一部を以下に説明する。ノード能力の推定はノードの健全性管理の特性に基づいてなされ、ここでナーバスネスと攻撃対象領域は、図７のブロック２で計算されているようにノードのステートマシンを用いてモデル化される。これらの能力と特性は、図５のブロック１のモデルに適用され、このモデルにおいて、各ノードは自らの周囲環境からナーバスネスの入力情報を受信して、個別ノードのナーバスネスレベルに関するローカライズされた判断をなす。このナーバスネスのレベルは、他のどのノードがこのナーバスネスの入力情報を受信できるかについては考慮することなく、ローカル環境と共有される。

【０１３６】

ブロック１（図５）を参照すると、ノードは、自らのカレントステートアセスメント（現状の状態評価）（５００）に基づき、ナーバスを増減させる。このステートアセスメントは、ホストステート（５０２）を計算するための算法である（上記モデルの項参照）。ホストステートは、攻撃対象領域と、ネットワークナーバスネスと、倍率としてのパラノイアとの組合せである。攻撃対象領域を求めるためになされるホストステート（５０２）の計算は下記の特性に基づく：（ａ）ホストが最後に手動で更新された時点からの、又は重要なアプリケーションへのパッチを得るために中央パッチサーバを自動的にチェックした時点からの経過時間が増えるにつれて、ノードのナーバスネスは増していき、ここで重要なパッチとしては、ファームウェアのパッチ、オペレーティングシステムのパッチ、アプリケーション固有のパッチ、アンチウイルス更新、及び侵入検知システムのシグネチャの更新がある；（ｂ）ホストが最後に構成管理サーバをチェックして、又はアドミニストレータが最後に手動でホストにログインして、現状のローカルポリシー構成につきチェックした時点からの経過時間が増えるにつれて、ノードのナーバスネスは増していく。構成チェックは、許可された及びブロックされたポート、プロトコル、サービス及びアプリケーションを含んでもよい。構成チェックはさらに、誰がログインしてよいのか、ログインした者がどの機能を実行してよいのか、ログインした者がどのデータを送信してよいのか、そしてログインした者がそのデータをどこに送信してよいのか、についての制限を含んでもよい。（ｃ）不審なイベントに対する「警告」を発報するアクティビティによって、ノードのナーバスネスは増加する。そうした不審なイベントの例には、ユーザが、アクセスが許可されていないファイル、ブロックされているサイト、制限されている共有データへのアクセス、通常の業務時間外のアクセス、そして通常使用されていないロケーションからのアクセスを試みることが含まれる。（ｄ）ローカルＩＤＳ（侵入検知システム）の又はアンチウイルスの警告を作動させるシグネチャ又はヒューリスティック・アクティビティによって、ノードのナーバスネスは増加する。（ｅ）ノードが設定された時間枠内にパッチと更新を受信すると、あるいはパッチが用意されていないことの確証を受信すると、ノードのナーバスネスは減少する。ノードは、最新のマルウェア及び脅威シグネチャに対し更新されると、そのナーバスネスが減少する。

【０１３７】

最初に攻撃対象領域を推定する際は、総合的な視点を得るために、すべてのノードについて攻撃対象領域を集めている。本発明は、攻撃ベクトルを一般化して、シミュレーション環境における使用のために汎用エンドポイント構成をモデル化し、共通エンドポイントセキュリティ能力の縮小セットを求める。代替変数は、内部攻撃対象領域とネットワーク攻撃対象領域とからなる１つの攻撃対象領域で近似できる。例えば、時間関連の１つの変数は、オペレーティングシステム（ＯＳ）及びアプリケーション用のパッチ更新、アンチウイルス（ＡＶ）及び侵入検知システム（ＩＤＳ）用のシグネチャ更新、そしてポリシー更新を示し、内部攻撃対象領域群の特性となる。ネットワークサービス関連の１つの変数は、ホスト上で稼働中のサービス（インバウンド・クエリ）と、ローカルホスト上での行き先アドレスの制限（アウトバウンド・リクエスト）を表していた。

【０１３８】
次に、ネットワークナーバスネスの計算は、近隣ノードから受信したナーバス信号（５０３、５０４、５０５、５０６）の合計に基づいてなされ、このナーバス信号は抽象的で非特異的なデータを含む。これらの信号は、無線ネットワーク内のアソシエート信号としてEthernet（登録商標）ネットワークのブロードキャスト・ドメイン上で送信されてもよく、ローカルで近くの他の一般的なキャリア信号を介して送信されてもよい。ブロードキャスト・ドメインが必要とするのは、物理的であると論理的であるとを問わず、ネットワークの近さ又はローカリティ（位置関係）を示すことだけである。信号は、３つのナーバス信号（５０３、５０４、５０５）と１つのＯＫ信号（５０６）と加算であり、これらをすべて合わせると、発生し得る４つのナーバスネスレベルのうちの３つに等しくなる。これを攻撃対象領域及びパラノイアのレベルとステートアセスメント（５０１）とで乗算して、ホストステート（５０２）を求める。この場合、ホストはナーバスであり、自らのナーバス信号（５０７）を送信する。
【０１３９】
１つのステートから他のステートへのステート変更を図６（ステート変更）に示しており、ここでステート１（６０１）は沈静で通信に開放されており、ステート２（６０２）はある程度のナーバスを示しており、ステート３（６０３）は極めてナーバスであり、ナーバスネスが減少するまでシステムが一時的にほとんどの又はすべての通信を遮断する。
【０１４０】
ブロック２（図７）はより堅牢な環境におけるブロック１のモデルを示しており、図７において５個のノード（７０１）を示す。このブロックは、NetLogo内での完全に実装され、１０００個のノードを用いて本発明を具現化するものである。このモデルの第２ブロックは、ローカル認識に基づき、影響を受けたノードステートにより規定された、多数のノード間のインタラクションを示す。システムフィードバックは、特定の物理的距離内にある最も近い近隣者と共有されたナーバスネスのレベル（７０２）の伝達と、パラノイア（７０３）と呼ばれる近隣者のナーバスネスに対する感度のレベルを含む。
【０１４１】
図７はブロック２用の理論的コンテクストダイヤグラムであり、詳細な内容を含む。ブロック２は、ブロック１（図５）で学習された初期コンセプトに基づく完全モデルを実装したものである。ブロック２は、完全モデルが自己触媒的である、つまり当該モデルが自続的である、といういくつかの初期特性を含む。ブロック２において、パラノイア変数は、ナーバスネスに影響を与える倍率から、各ノードが自ら所属する近隣者ネットワークナーバスネスのナーバスネスをどの程度ファクタとしているかを示す重み付け乗数へと再定義された。
【０１４２】
シミュレーションにおいて使用される変数とパラメータは、エージェントベースの変数と環境変数との間で分化したものである。エージェントベースの変数は個別ノードに固有のものであり、そして環境変数はシミュレーションの範囲内にあるすべてのノードに平等に適用される。表１：エージェントベースの変数と、表２：環境変数は、どの変数とパラメータとがエクスポートされるのか、そしてそれに対応するデータ要素を示す。
【０１４３】

【表１】

エージェント変数	定義	エクスポート
主体（デフォルト設定）	各個別ノード用の一意的な識別子	はい
ネットワーク	ネットワーク攻撃対象領域のレベル、０～１の範囲。Ｓ４、Ｓ５の代替変数。ネットワーク攻撃対象領域は、ノードがどの程度迅速にネットワークポートとサービスとアドレスとを開閉させるかの指標の設定に応じて、様々な量で増減し得る。	はい Ｓ４、Ｓ５
ナーバスネス	単一ノードにおけるナーバスネスのレベル、０～１００。ナーバスネス＝攻撃対象領域＊Ｆ２のネットワークナーバスネス＊パラノイア。	はい Ｆ１
ナーバスステート	ナーバスネスのステートの定義：（１）沈静；（２）ナーバス；（３）最大。ノードが（３）最大に到達すると、ノードはサーバにパッチを適用してポートを閉じることでナーバスネスを減少させようとするか、あるいはナーバスネスが減少するまで通信を停止させようとするかのいずれかを行う。	いいえ
内部	内部攻撃対象領域のレベル、０～１の間。Ｓ１、Ｓ２、Ｓ３の代替変数。内部攻撃対象領域は、最後にパッチを適用されたときから定常的に増加し、その後、（１）アドミニストレータが設定した、又は（２）ナーバスネスのレベルに基づいて設定された、又は（３）検出されたアラートに基づいた定期スケジュールに基づいてパッチを適用される。	Ｓ１、Ｓ２、Ｓ３
Ｆ２ネットワークナーバスネス	各ノードの半径内にあるノードのナーバスネスのレベル、ローカルＦ２ノードの代替変数。設定に応じて、平均（mean）又はアベレージ（average）によって計算される。	はい Ｆ２
警告検出	警告検出の手動注入（manual inject）、これによって更新が強制的になされて、ノードが最高レベルのナーバスネスに設定される。	いいえ Ｆ５
攻撃対象領域	ノード攻撃対象領域全体の変数。内部攻撃対象領域の変数＋ネットワーク攻撃対象領域の変数からなる。０～１の間。	はい Ｆ４
自らの近隣者	ノードの半径内にある近隣者の数	はい Ｓ６

表１：エージェントベースの変数

【０１４４】

【表２】

環境変数	定義	エクスポート
ティック	環境内におけるタイムステップの増量	はい
パラノイア	すべてのノードに適用されるパラノイアの設定レベル	はい Ｆ３
半径	すべてのノードに適用される位置関係を定義する半径の設定レベル	はい
ネットワークナーバスネス計算	すべての近隣ノードナーバスネスの加算値（Additive）又は平均値（Mean）であるネットワークナーバスネスの計算メカニズム	いいえ
ネットワークナーバスネス	シミュレーション中のすべてのノードのナーバスネスのシミュレーション平均値	いいえ
シミュレーション世界	水平及び垂直境界線上におけるワールドラップ（World wrap）	該当なし

表２：環境変数

【０１４５】
第３ブロック（図９）は、ブロック１（図５）及びブロック２（図７）の要素を含み、ノードナーバスネスとネットワークナーバスネスのレベルに基づき、ノードとネットワークのプロパティによって規定される、ネットワーク防御のための創発的挙動を示す。これはシステム挙動の分析を通じて実行されており、創発的ネットワーク防御に関する価値ある情報を提供する。図８の「創発的挙動を示す３個の警告」は、この創発的挙動を示し、アンチウイルス警告検出マルウェアなどによって１つの警告がノード（１１０）に対して発せられる様子が見られる。図８に示すソフトウェアは、例えばアドミニストレータによる使用のためにノード又はセントラルロケーションに設置されることとしてもよく、また、このソフトウェアは上述のアルゴリズムに基づくものである。警告（８０４）の際に、ホストがエージェントにパッチングを行い、それによって攻撃対象領域が減少し、ナーバスネスのレベルが減少する（（８０４）における隙間が示すように）ことに留意されたい。その後、時間の経過に伴い、システムは定常状態に戻り、次の警告と対応を待つ。上のチャートは、１つのエージェントにおける内部露出度、ネットワーク露出度、ナーバスネス及び攻撃対象領域を示す。下のチャートは、ネットワークナーバスネスと、ネットワーク全体に関連する様々なエージェントを示す。このシミュレーションの終わりには、出力（８０８）におけるエージェント０の攻撃対象領域の値は０．１７と、最大値１を下回っていた。信号（８０６）は、ネットワークナーバスネスの変化が安定状態に戻ることを示す（Ｙスケールにおいて約２０～３０）。
【０１４６】
最後に各ホストは、図９（ブロック３の理論的コンテクストダイヤグラム）に示すように、各ホストのローカルネットワーク内で他のホストと通信する。この図では、表示された範囲では、すべてのホストが他のすべてのホストのローカルの近隣者である。
【０１４７】
上記の説明に加えて、本発明は以下の文書にも記載されている。（ａ）創発的ネットワーク防御（Emergent Network Defense）という題の論文、（ｂ）ネットワーク防御のための環境プリミティブ認識（Environmental Primitive Awareness for Network Defense）

（論文）、（ｃ）ナーバスネットワーク：理論及びモデル（A Nervous Network: Theory and Model）（共著）、（ｄ）ナーバスネットワーク：理論及びモデル（A Nervous Network: Theory and Model）（単著）、及び（ｅ）ネットワーク防御のための環境プリミティブ認識（Environmental Primitive Awareness for Network Defense）（以下「論文」と称す）。これらの論文はすべて仮出願の一部をなしており、その全体は参考として引用されて本明細書に含まれる。論文は、本明細書の一部をなして、本発明の典型的な実施形態を開示する。

【０１４８】

本発明は、プロセッサ又はコントローラを各エンドポイント又はノードにおいて使用して、有限ステートマシンモデルに基づく様々な機能及び動作を実行する。各エンドポイントにおけるプロセッサは、例えば、コプロセッサ、レジスタ、データ処理機器及びサブシステム、有線又は無線通信リンク、入力機器、モニター、メモリ又は、データベースなどのストレージ機器を含む、多種さまざまな部品又はサブシステムの１又はそれ以上を備えることとしてもよい。システム及び処理のすべて又は一部は、コンピュータ可読媒体に保存でき又はコンピュータ可読媒体から読み出すことができる。システムは、記載された処理を実行させるためにマシン実行可能な命令を保存してある、ハードディスクなどのコンピュータ可読媒体を含むことができる。

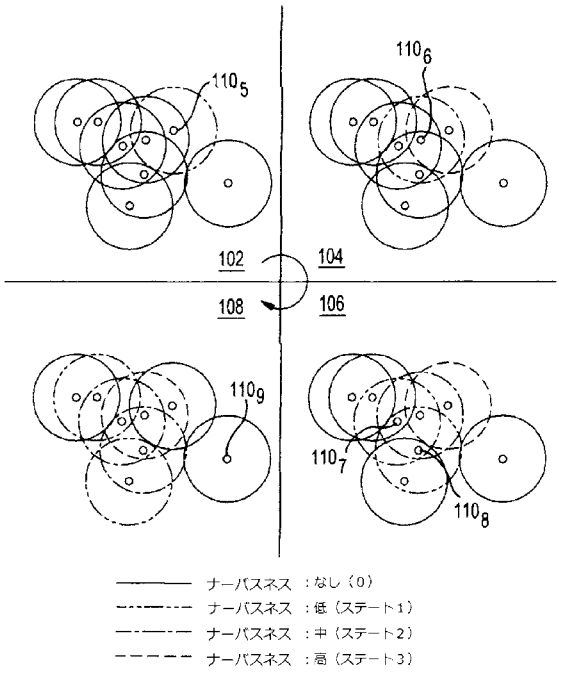
【０１４９】

例えば、ノード（ホストとも称される）プロセッサは、図２に示すように、上記で実行したすべての動作を実行でき、図２では、上にノードの動作を示し、下に創発的特性１０とネットワーク動作を創発的特性１０として示す。さらに、動作に必要なデータは、メモリ又はデータベースなどのストレージ機器に保存することができる。また、さらに、すべての動作は連続的かつリアルタイムで発生するため、システムは脅威に直ちに反応することができる。そして、本発明を中央集中型プロセッサに統合することで、ネットワークの状況を中央監視することができ、それにより１又はそれ以上のノードが中央ロケーションと通信を行う。

【０１５０】

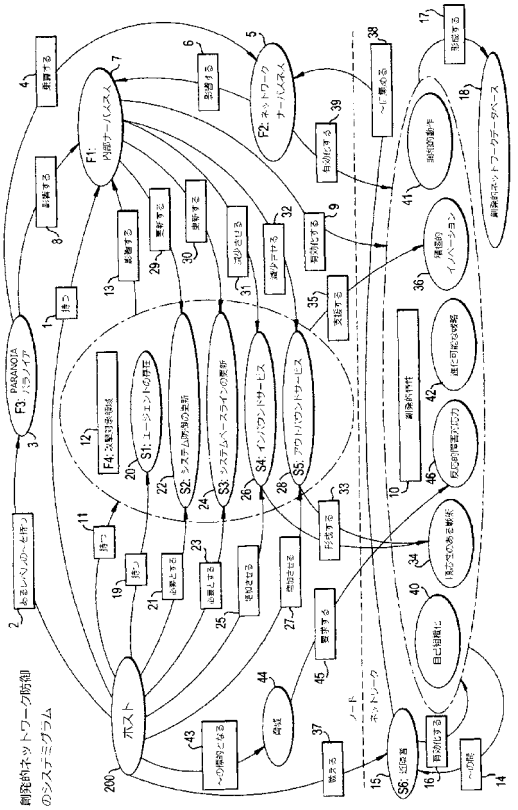
本明細書中で記載した参考文献は、参照することによって本明細書に組み入れられる。上記論文において記載された本発明の詳細な説明及び図面は、本発明の原理のみを示す例示的なものとして理解されるべきである。本発明は、様々な仕方で構成し得るものであって、好ましい実施形態によって限定されることは意図していない。本発明の数多くの応用は当業者によって容易に着想されるであろう。したがって本発明を、開示された特定の実施例や、図示及び説明された当の構造及び動作に限定することは所望されていない。むしろ、あらゆる適切な応用例及び等価物を本発明の範囲内に該当するものとして主張することができる。

【図１】

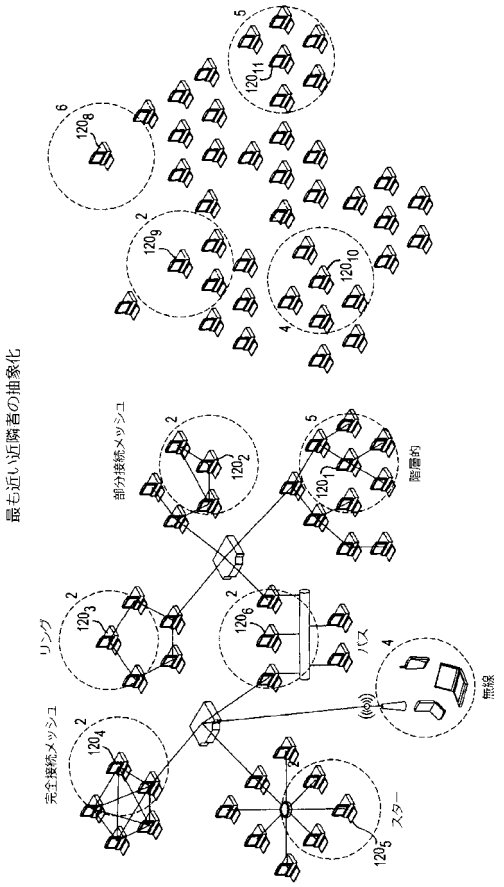


ネットワーク ネーバスネス アセスメント

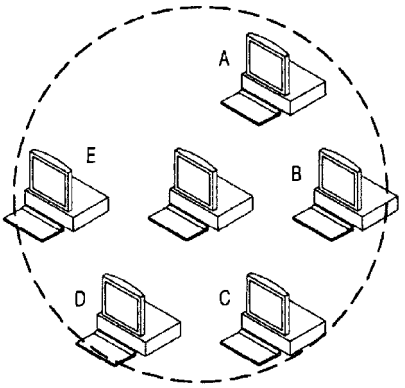
【図２】



【図３】

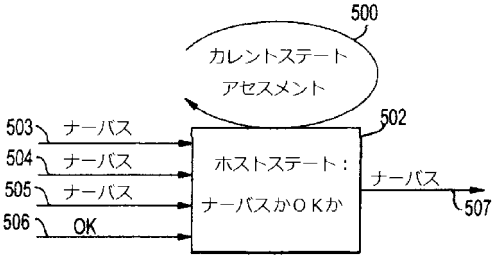


【図４】



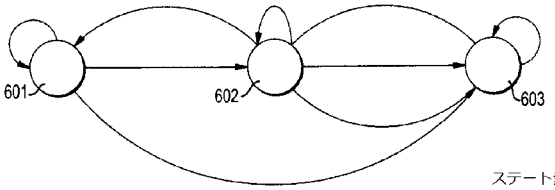
ナーバスの例

【図５】



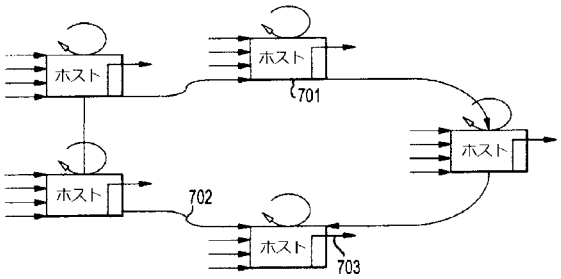
ブロック１の理論的コンテクストダイヤグラム

【図６】



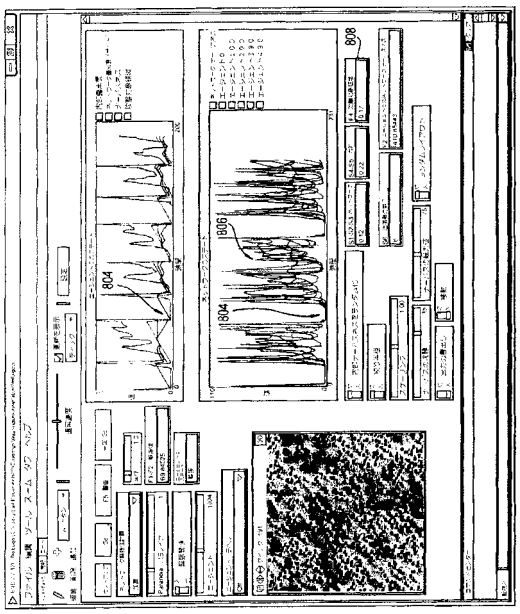
ステート変更

【図７】

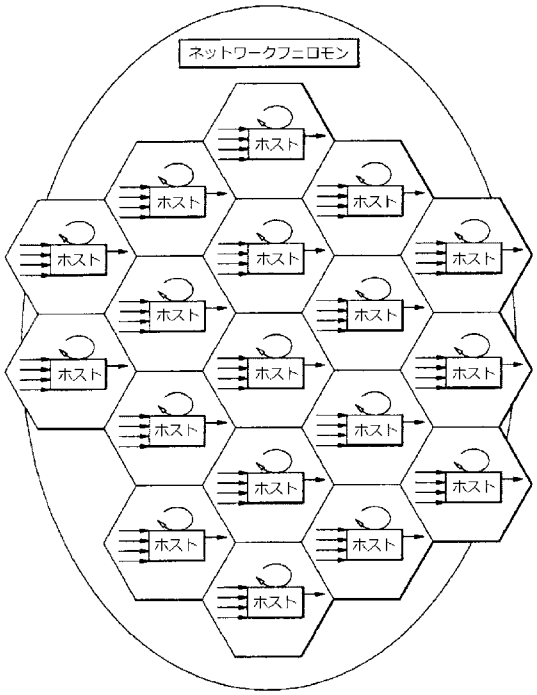


ブロック２の理論的コンテクストダイヤグラム

【図８】



【図９】



ブロック３の理論的コンテクストダイヤグラム

【図１０】

フィードバックデータ：	ステートデータ：
Ｆ１：内部ナーバスネスのレベル	Ｓ１：エージェントがノード上に存在する
Ｆ２：ネットワークナーバスネスのレベル	Ｓ２：最新のシグネチャレベルにおけるシステム防御（ＨＢＳＳ、ＡＶ、ＩＤＳ）
Ｆ３：パラノイアのレベル	Ｓ３：最新のパッチ／構成レベルにおけるシステム基本水準（ＯＳ、アプリケーション）
Ｆ４：攻撃対象領域	Ｓ４：制限されたインバウンドサービス（制限されたサービス、ブロックされたポート）
	Ｓ５：制限されたアウトバウンドサービス（ブロックされたＩＰ、サブネット、ＵＲＬ）
	Ｓ６：近隣者の数

	Ｆ１：内部ナーバスネスのレベル	Ｆ２：ネットワークナーバスネスのレベル	Ｆ３：パラノイアのレベル	Ｆ４：攻撃対象領域	Ｓ１：エージェントがノード上に存在	Ｓ２：最新のシグネチャレベルにおけるシステム防御	Ｓ３：最新のパッチ／構成レベルにおけるシステム基本水準	Ｓ４：制限されたインバウンドサービス	Ｓ５：制限されたアウトバウンドサービス	Ｓ６：近隣者の数
ブロック１：エンドポイント攻撃対象領域の特性				×	×	×	×	×	×	
ブロック２：エンドポイントノードが「ナーバスネットワーク」を介してセキュリティステートを共有	×	×	×		×					×
ブロック３：ノードシステムが自らの攻撃対象領域とノードナーバスステートを入力に基づき変更	×	×	×	×	×	×	×	×	×	×

要求されるデータ要素

【国際調査報告】

61500540008

PCT/US2013/060425 22.06.2015

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 130761-00521	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US 13/60425	International filing date *(day/month/year)* 18 September 2013 (18.09.2013)	(Earliest) Priority Date *(day/month/year)* 18 September 2012 (18.09.2012)
Applicant THE GEORGE WASHINGTON UNIVERSITY		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 2 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the language, the international search was carried out on the basis of:

☒ the international application in the language in which it was filed.

☐ a translation of the international application into _____ which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

b. ☐ This international search report has been established taking into account the rectification of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).

c. ☐ With regard to any nucleotide and/or amino acid sequence disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (see Box No. II).

3. ☐ **Unity of invention is lacking** (see Box No. III).

4. With regard to the title,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the abstract,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the drawings,

a. the figure of the drawings to be published with the abstract is Figure No. 1

☒ as suggested by the applicant.

☐ as selected by this Authority, because the applicant failed to suggest a figure.

☐ as selected by this Authority, because this figure better characterizes the invention.

b. ☐ none of the figures is to be published with the abstract.

Form PCT/ISA/210 (first sheet) (January 2015)

15. 9. 2015

2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 13/60425

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 19/00 (2015.01), G06F 15/173 (2015.01)
CPC - H04L43/00
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)
CPC: H04L43/00; IPC(8): G06F 19/00 (2015.01), G06F 15/173 (2015.01); USPC: 709/224

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
CPC: H04L29/08072, H04L29/06, H04L43/00, H04L12/2602, H04L41/22, H04L63/1441; USPC: 726/25, 726/13, 709/224, 726/26, 726/4, 709/225 (keyword limited; terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PatBase; Google Scholar
Search Terms: node, network, graph, computer, machine, neighbor, proximity, adjacent, closeness, nervous, anxious, paranoia, transmit, spread, notify, stigmergy, pheromone

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/0132166 A1 (SAFFRE) 16 June 2005 (16.06.2005), entire document, especially abstract and para [0009], [0026], [0045]-[0050], [0059], [0064]-[0065], [0067]-[0071], [0076]-[0079], [0090]-[0091], [0093], [0095]-[0096], [0099]-[0103], [0109], [0111]-[0113], [0119], [0121], Fig. 1, Fig. 2, claim 1, claim 21.	1-21
A	US 2005/0149728 A1 (SAFFRE) 07 July 2005 (07.07.2005), entire document.	1-21
A	US 2003/0142851 A1 (BRUECKNER et al.) 31 July 2003 (31.07.2003), entire document.	1-21

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

* 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	Date of mailing of the international search report
18 May 2015 (18.05.2015)	22 JUN 2015
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

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,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,UZ

（特許庁注：以下のものは登録商標）
１．アンドロイド
２．ＴＷＩＴＴＥＲ
３．ＦＡＣＥＢＯＯＫ

(72)発明者 クレーン サラ エム
アメリカ合衆国 ワシントン, ディーシー ２０００２, フォーティーンス ストリート ノースイースト ２２４
(72)発明者 ライアン ジュリー シー エイチ
アメリカ合衆国 ワシントン, ディーシー ２００５２, ジーストリート ノースウエスト １７７６