(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7614715号
(P7614715)

(45)発行日　令和7年1月16日(2025.1.16)

(24)登録日　令和7年1月7日(2025.1.7)

(51)国際特許分類			FI		
G06F	*21/55*	*(2013.01)*	G06F	21/55	
G06N	*20/00*	*(2019.01)*	G06N	20/00	160
H04L	*51/00*	*(2022.01)*	H04L	51/00	

請求項の数　20　外国語出願　（全42頁）

(21)出願番号　特願2019-28818(P2019-28818)
(22)出願日　平成31年2月20日(2019.2.20)
(65)公開番号　特開2019-145107(P2019-145107A)
(43)公開日　令和1年8月29日(2019.8.29)
審査請求日　令和3年11月24日(2021.11.24)
審判番号　不服2023-16010(P2023-16010/J1)
審判請求日　令和5年9月22日(2023.9.22)
(31)優先権主張番号　62/632623
(32)優先日　平成30年2月20日(2018.2.20)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　16/278932
(32)優先日　平成31年2月19日(2019.2.19)
最終頁に続く

(73)特許権者　519059306
ダークトレース リミテッド
Ｄａｒｋｔｒａｃｅ Ｌｉｍｉｔｅｄ
イギリス， ＣＢ４ ０ＤＳ， ケンブリッジ， セントジョンズ イノベーション パーク， モーリス ウィルクス ビルディング
(74)代理人　100098899
弁理士　飯塚 信市
(74)代理人　100163865
弁理士　飯塚 健
(72)発明者　マシュー ダン
イギリス， ＣＢ７ ４ＢＥ， ケンブリッジシャー， イーライ， ブロードストリート ９２
最終頁に続く

(54)【発明の名称】　機械学習モデルを用いてｅメールネットワークを保護するサイバー脅威防御システム

(57)【特許請求の範囲】

【請求項１】

ｅメールシステムと関連付けられたｅメール活動およびユーザ活動の正常な挙動について訓練される１つまたは複数の第１機械学習モデルと、

前記ｅメールシステム内のサイバー脅威について訓練される１つまたは複数の第２機械学習モデルを使用するサイバー脅威モジュールであって、前記第１機械学習モデルを参照するように構成され、分析下の前記ｅメール活動およびユーザ活動の一連の１つまたは複数の非正常な挙動が前記第１機械学習モデルから得られた正常な無害の挙動から外れる可能性を考慮に入れた脅威リスクパラメータを決定する、サイバー脅威モジュールと、

前記サイバー脅威モジュールからの前記脅威リスクパラメータが、行動の指針となり得るしきい値に等しいかまたはそれより大きいとき、前記サイバー脅威を阻止するために取られるべき１つまたは複数の自律行動を引き起こすように構成された、行動を取る人間ではない、自律応答モジュールとを備える、装置。

【請求項２】

ｅメール自体およびその関連データに関する複数の特徴の理解を得ることについて訓練される１つまたは複数の第３機械学習モデルをさらに備え、

前記サイバー脅威モジュールが、前記第３機械学習モデルを参照して、分析下のｅメールが潜在的に悪意のある特徴を有するかどうかを決定することができ、次いで、この分析を前記脅威リスクパラメータの決定において考慮に入れることができる、請求項１に記載の装置。

【請求項３】
前記ｅメールシステムに入る／前記ｅメールシステムから出るｅメールおよび分析下の１つまたは複数のｅメールについて知られているサイバーセキュリティ特徴のインボックススタイルビューを有するユーザインターフェースをさらに備え、前記ｅメールのインボックススタイルビューを有する前記ユーザインターフェースが、前記分析下の１つまたは複数のｅメールを表示する第１のウィンドウ、およびそれらの分析下の１つまたは複数のｅメールについて知られているセキュリティ特徴を伴う第２のウィンドウを有する、請求項１に記載の装置。
【請求項４】
サイバー脅威防御システムのための前記ユーザインターフェースが、前記第１のウィンドウ内の前記分析下の１つまたは複数のｅメールを、それらの１つまたは複数のｅメールについて知られている関連する前記セキュリティ特徴の隣で、カスタマイズし、かつターゲットとするために、前記ｅメールシステム内のｅメールがフィルタリング可能、検索可能、およびソート可能であることを許容するように構成され、このユーザインターフェースと同じディスプレイ画面上にそれらのそれぞれの情報を表示するこれらの２つのウィンドウが、分析下の前記ｅメールを分析するサイバー専門家に分析下の前記ｅメールを分析して、それら１つまたは複数のｅメールが実際にサイバー脅威であるかどうかを評価することを可能にする、請求項３に記載の装置。
【請求項５】
前記自律応答モジュールは、ｉ）知られている悪意のあるｅメールまたはｉｉ）少なくとも悪意の可能性があるｅメールがサイバー脅威モジュールによって決定されたとき、前記自律応答モジュールが前記サイバー脅威を阻止するために前記自律行動をいつ取るべきであるかを知るように構成され、前記自律応答モジュールは、前記脅威リスクパラメータがサイバー専門家によって選択可能である前記行動の指針となり得るしきい値に等しいかまたはそれより大きいこと、すなわち前記分析下の１つまたは複数のｅメールが少なくとも悪意の可能性があることを前記サイバー脅威モジュールが示すとき、前記自律応答モジュールに可能である行動のタイプおよび特定の行動を含む、前記自律応答モジュールが取ることができる自律行動が何であるかを設定するように、ユーザインターフェースを通じて構成可能な管理ツールを有する、請求項１に記載の装置。
【請求項６】
前記ｅメールシステムの特定のユーザへの混乱を回避するために、そのｅメールに対する全面的隔離またはブロックをするのではなくて、前記自律応答モジュールが、前記自律応答モジュールが実行可能であって、悪意のあるｅメールの特定のｅメール要素に対して自律的に行動するように構成され、かつ前記ユーザインターフェースを通じて選択可能である集中的な応答行動を含む、行動の応答行動タイプ及び特定の行動のライブラリを有する、請求項５に記載の装置。
【請求項７】
前記ｅメールシステムに関連付けられるネットワーク上の、ユーザ、デバイス、およびそれらの間のインタラクションの正常な挙動について訓練される１つまたは複数の第４機械学習モデルを有するネットワークモジュールをさらに備え、ユーザインターフェースが、ネットワークデータを表示するための１つまたは複数のウィンドウ、ならびに、同じユーザインターフェースを通じてディスプレイ画面上に、ｅメールおよびそれらのｅメールに関するサイバーセキュリティ詳細を表示するための１つまたは複数のウィンドウを有し、それにより、サイバー専門家が、１つのプラットフォーム内でネットワークデータとｅメールサイバーセキュリティ詳細との間でピボットし、それらを前記同じディスプレイ画面上の別個の領域ではなく、相互接続された全体として考えることが可能になる、請求項１に記載の装置。
【請求項８】
潜在的に非正常なネットワーク活動を決定するために利用される、前記ネットワークモジュールおよび前記第４機械学習モデルは、前記サイバー脅威モジュールへの情報の追加

入力を提供して、前記脅威リスクパラメータを決定する、請求項７に記載の装置。
【請求項９】
前記第１機械学習モデルを、訓練をするためのプローブからのデータを使用し、したがって、前記正常な挙動の基準線が何であるかを定期的に更新する、請求項１に記載の装置。
【請求項１０】
前記サイバー脅威を阻止するために取られるべき１つまたは複数の自律行動を引き起こすように、前記自律応答モジュールと連携して構成される前記サイバー脅威モジュールが、何らかの人間の介入を待たずに前記サイバー脅威に応答することを通じて、前記ｅメールシステム内のコンピューティングデバイスを、前記コンピューティングデバイスにおけるＣＰＵサイクル、メモリスペース、および消費電力を消費することからの前記サイバー脅威の影響を制限することによって、改善する、請求項１に記載の装置。
【請求項１１】
サイバー脅威防御システムのための方法であって、
前記サイバー脅威防御システムは、ｅメールシステムと関連付けられたｅメール活動およびユーザ活動の正常な挙動について訓練される１つまたは複数の第１機械学習モデルを備え、
前記ｅメールシステム内のサイバー脅威について訓練される１つまたは複数の第２機械学習モデルを使用するサイバー脅威モジュールであって、前記第１機械学習モデルを参照するように構成されたサイバー脅威モジュールが、分析下の前記ｅメール活動およびユーザ活動の一連の１つまたは複数の非正常な挙動が前記第１機械学習モデルから得られた正常な無害の挙動から外れる可能性を考慮に入れた脅威リスクパラメータを決定するステップと、
行動を取る人間ではない、自律応答モジュールが、前記サイバー脅威モジュールからの前記脅威リスクパラメータが、行動の指針となり得るしきい値に等しいかまたはそれより大きいとき、前記サイバー脅威を阻止するために取られるべき１つまたは複数の自律行動を引き起こすステップと、を含む、方法。
【請求項１２】
前記サイバー脅威防御システムは、ｅメール自体に関する複数の特徴およびその関連データの理解を得ることについて訓練される１つまたは複数の第３機械学習モデルを更に備え、
前記決定するステップでは、更に、
前記サイバー脅威モジュールが、前記第３機械学習モデルを参照して、分析下のｅメールが潜在的に悪意のある特徴を有するかどうかを決定することができ、次いで、この分析を前記脅威リスクパラメータの決定において考慮に入れることができる、請求項１１に記載の方法。
【請求項１３】
ユーザインターフェースが、前記ｅメールシステムに入る／前記ｅメールシステムから出るｅメールおよび分析下の１つまたは複数のｅメールについて知られているサイバーセキュリティ特徴のインボックススタイルビューを提示するステップであって、前記ｅメールのインボックススタイルビューを有する前記ユーザインターフェースが、前記分析下の１つまたは複数のｅメールを表示する第１のウィンドウ、およびそれらの分析下の１つまたは複数のｅメールについて知られているセキュリティ特徴を伴う第２のウィンドウを有する、提示するステップ、をさらに含む、請求項１１に記載の方法。
【請求項１４】
前記提示するステップでは、更に、
前記サイバー脅威防御システムのための前記ユーザインターフェースが、前記第１のウィンドウ内で前記分析下の１つまたは複数のｅメールを、それらの１つまたは複数のｅメールについて知られている関連する前記セキュリティ特徴の隣で、カスタマイズし、およびターゲットとするために、前記ｅメールシステム内のｅメールがフィルタリング可能、検索可能、およびソート可能であることを許容するように構成され、このユーザインターフェースと同じディスプレイ画面上にそれらｅメールのそれぞれの情報を表示するこれらの

２つのウィンドウが、分析下の前記ｅメールを分析するサイバー専門家に分析下の前記ｅメールを分析して、それら１つまたは複数のｅメールが実際にサイバー脅威であるかどうかを評価することを可能にする、請求項１３に記載の方法。
【請求項１５】
前記引き起こすステップでは、更に、
前記自律応答モジュールが、ｉ）知られている悪意のあるｅメールまたはｉｉ）少なくとも悪意の可能性があるｅメールがサイバー脅威モジュールによって決定されたとき、前記自律応答モジュールが前記サイバー脅威を阻止するための前記自律行動をいつ取るべきであるかを知るように構成され、
前記自律応答モジュールが、前記脅威リスクパラメータがサイバー専門家によって選択可能である前記行動の指針となり得るしきい値に等しいかまたはそれより大きいこと、すなわち前記ｅメール活動およびユーザ活動の前記一連の１つまたは複数の非正常な挙動が少なくとも悪意の可能性があることを前記サイバー脅威モジュールが示すとき、前記自律応答モジュールに可能である行動のタイプおよび特定の行動を含む、前記自律応答モジュールが取ることができる自律行動が何であるかを設定するように、ユーザインターフェースを通じて構成可能な管理ツールを有する、請求項１１に記載の方法。
【請求項１６】
前記引き起こすステップでは、更に、
前記ｅメールシステムの特定のユーザへの混乱を回避するために、そのｅメールに対する全面的隔離またはブロックをするのではなくて、前記自律応答モジュールが、前記自律応答モジュールが実行可能であって、悪意のあるｅメールの特定のｅメール要素に対して、自律的に行動するように構成され、かつ前記ユーザインターフェースを通じて選択可能な集中的な応答行動を含む、行動の応答行動タイプおよび特定の行動のライブラリを有する、請求項１５に記載の方法。
【請求項１７】
ネットワークモジュールが、前記ｅメールシステムに関連付けられるネットワーク上の、ユーザ、デバイス、およびそれらの間のインタラクションの正常な挙動について訓練される１つまたは複数の第４機械学習モデルを使用するステップと、
ユーザインターフェースが、ネットワークデータを表示するための１つまたは複数のウィンドウ、ならびに、同じユーザインターフェースを通じてディスプレイ画面上に、ｅメールおよびそれらのｅメールに関するサイバーセキュリティ詳細を表示するための１つまたは複数のウィンドウを提示するステップであって、それにより、サイバー専門家が、１つのプラットフォーム内でネットワークデータとｅメールサイバーセキュリティ詳細との間でピボットし、それらを前記同じディスプレイ画面上の別個の領域ではなく、相互接続された全体として考えることが可能になる、提示するステップ、
をさらに含む、請求項１１に記載の方法。
【請求項１８】
前記決定するステップでは、更に、
前記サイバー脅威モジュールが、潜在的に非正常なネットワーク活動を決定するために利用される、前記ネットワークモジュールおよび前記第４機械学習モデルから提供された情報の追加入力を考慮して、前記脅威リスクパラメータを決定する、請求項１７に記載の方法。
【請求項１９】
前記第１機械学習モデルを、訓練をするためのプローブからのデータを使用し、したがって、前記正常な挙動の基準線が何であるかを定期的に更新するステップ、をさらに含む、請求項１１に記載の方法。
【請求項２０】
１つまたは複数のプロセッサを用いて実行されるとき、前記サイバー脅威防御システムに請求項１１の動作を実行させる、実行可能な命令を含む非一時的コンピュータ可読媒体。
【発明の詳細な説明】

【技術分野】
【０００１】
著作権の通知
【０００２】
本開示の一部分は、著作権保護の対象となる資料を含む。著作権者は、著作権保護の対象となる資料の他者による複製について、米国特許商標庁の特許ファイルまたは記録に登場する場合には異存はないが、そうでない場合には、何であろうとも全著作権を保有する。
関連出願
【０００３】
本出願は、米国特許法第１１９条の下、２０１８年2月２０日出願の"Ａ　ｃｙｂｅｒ－ｔｈｒｅａｔ　ｄｅｆｅｎｓｅ　ｓｙｓｔｅｍ　ｗｉｔｈ　ｖａｒｉｏｕｓ　ｉｍｐｒｏｖｅｍｅｎｔｓ"と題される仮特許出願第６２／６３２，６２３号に対する優先権およびその利益を主張するものであり、その全体が参照により本明細書に組み込まれる。
【０００４】
本明細書に提供される設計の実施形態は、概して、サイバー脅威防御システムに関する。一の実施形態において、人工知能が、ｅメールに由来するおよび／またはｅメールと関連付けられたサイバーセキュリティ脅威を分析する。
【背景技術】
【０００５】
サイバーセキュリティ環境においては、ファイアウォール、エンドポイントセキュリティ法、ならびにＳＩＥＭおよびサンドボックスなどの他のツールが、特定のポリシーを実行するため、および特定の脅威に対する保護を提供するために展開される。これらのツールは現在、組織のサイバー防御戦略の重要な部分を形成するが、それらは、新時代のサイバー脅威においては不十分である。
【０００６】
ｅメール脅威を含むサイバー脅威は、巧妙であり、迅速にネットワークに危害を加え得る。自動化された応答を有することにより、これらの脅威に迅速に対抗することが可能になる。
【発明の概要】
【０００７】
一の実施形態において、サイバー脅威防御システムは、ｅメールおよび／もしくはｅメールシステムに由来するならびに／またはそれらと関連付けられたサイバー脅威からシステムを保護する。１つまたは複数の機械学習モデルは、ｅメールシステムと関連付けられたｅメール活動およびユーザ活動の正常な挙動、ならびにｅメールの対象とする受信者の、それら受信者の正常なネットワーク挙動から把握されるような、正常な挙動について訓練される。正常なネットワーク挙動は、ｅメールインタラクションの外側で動作する他のシステムから得ることができる。サイバー脅威モジュールは、ｅメールシステム内のサイバー脅威、または受信者のネットワーク上に存在し得るサイバー脅威について訓練される１つまたは複数の機械学習モデルを有し得る。サイバー脅威モジュールは、ｅメールシステムと関連付けられたメール活動およびユーザ活動の正常な挙動について訓練されるモデルを参照し得る。サイバー脅威モジュールは、分析下のｅメール活動およびユーザ活動の一連の１つまたは複数の非正常な挙動が、得られた正常な無害の挙動から外れる可能性を考慮に入れた脅威リスクパラメータを決定する。プローブが、ユーザ活動およびｅメール活動を収集し、次いで、その活動をサイバー脅威モジュールにフィードして、ｅメールシステム内のｅメール活動およびユーザ活動の理解を引き入れる。行動を取る人間ではない、自律応答モジュールは、サイバー脅威モジュールからの脅威リスクパラメータが、行動の指針となり得るしきい値に等しいかまたはそれより大きいとき、サイバー脅威を阻止するために取られるべき１つまたは複数の自律行動を引き起こすように構成される。
【０００８】
本明細書に提供される設計のこれらおよび他の特徴は、図面、明細書、および請求項を

参照してより良く理解することができ、それらのすべてが、本特許出願の開示を形成する。
【図面の簡単な説明】
【０００９】
図面は、本明細書で提供される設計のいくつかの実施形態に言及する。
【００１０】
【図１】図１は、少なくともｅメールシステムと関連付けられたｅメール活動およびユーザ活動の正常な挙動について訓練される機械学習モデルを参照するサイバー脅威モジュールを有するサイバー脅威防御システムであって、サイバー脅威モジュールが、「分析下のｅメール活動およびユーザ活動の一連の１つまたは複数の非正常な挙動が、得られた正常な無害の挙動から外れる可能性」、したがって悪意のある挙動である可能性が高いことを考慮に入れた脅威リスクパラメータを決定する、サイバー脅威防御システムの一実施形態のブロック図である。
【００１１】
【図２】図２は、ｅメール活動およびネットワーク活動を監視し、このデータをこれらの活動間の相互に関連した因果関係にフィードし、この入力をサイバー脅威分析に供給する、サイバー脅威防御システムの一実施形態のブロック図である。
【００１２】
【図３】図３は、一連の非正常な挙動が、潜在的なサイバー脅威にどのように相関するか、ならびに「分析下のｅメール活動およびユーザ活動のこの一連の１つまたは複数の非正常な挙動が、得られた正常な無害な挙動から外れる可能性」、したがって悪意のある挙動であることを考慮に入れた脅威リスクパラメータを決定するサイバー脅威モジュールの一実施形態のブロック図である。
【００１３】
【図４】図４は、ｅメールおよびそのメタデータのプロパティを分類することを含む、ｅメール自体の複数の特徴およびその関連データの理解を得ることについて訓練される１つまたは複数の機械学習モデルを参照するサイバー脅威防御システムの一実施形態のブロック図である。
【００１４】
【図５】図５は、分析下のその他のネットワークに関連してｅメールについての例となる一連の非正常な挙動の一実施形態のブロック図である。
【００１５】
【図６】図６は、ｅメールシステム内のｅメールが、フィルタリング可能、検索可能、およびソート可能であるようにするための、サイバー脅威防御システムのユーザインターフェースの例となるウィンドウの一実施形態のブロック図である。
【００１６】
【図７】図７は、例となる自律行動であって、人間がその行動を開始することなく、自律的迅速応答モジュールが取るように構成され得る例となる自律行動の一実施形態のブロック図である。
【００１７】
【図８】図８は、特定のユーザの、それらユーザのｅメール活動に結び付けられたネットワーク活動を連携するｅメールモジュールおよびネットワークモジュールの一実施形態のブロック図である。
【００１８】
【図９】図９は、例となるネットワークを保護するサイバー脅威防御システムの一例を示す図である。
【００１９】
【図１０】図１０は、コンピュータのネットワーク活動を、そのコンピュータのユーザがそのネットワーク活動に関係のあるコンテンツを含むｅメールを受信するより前に、ｅメールモジュールに通知するネットワークモジュールの一例を示す図である。
【００２０】

【図１１】図１１は、コンピュータのウェブ閲覧活動に関する推定生活パターン情報を、そのコンピュータのユーザがその生活パターンと一致していないコンテンツを含むｅメールを受信するより前に、ｅメールモジュールに通知するネットワークモジュールの一例を示す図である。

【００２１】

本設計は、様々な修正形態、等価物、および代替形式の対象となるが、それらの特定の実施形態は、図面内の例を用いて示されており、これより詳細に説明されるものとする。本設計は、開示される特定の実施形態に限定されず、それどころか、その特定の実施形態を使用するすべての修正形態、等価物、および代替形式を網羅することが意図されるということを理解されたい。

【発明を実施するための形態】

【００２２】

以下の説明において、本設計の徹底的な理解を提供するために、特定のデータ信号、名前の付いたコンポーネント、システム内のサーバの数などの多数の特定の詳細事項が明記される。しかしながら、当業者には、本設計がこれらの特定の詳細事項なしに実践され得ることは明らかである。他の例において、周知のコンポーネントまたは方法は、詳細には説明されておらず、本設計を不必要に不明瞭にすることを回避するために、むしろブロック図で説明されている。さらに、第１のサーバなど、特定の数字による参照が行われ得る。しかしながら、特定の数字による参照は、文字通りの順番と解釈されるべきではなく、むしろ、第１のサーバは第２のサーバとは異なると解釈されるべきである。したがって、明記される特定の詳細事項は単に例にすぎない。また、１つの実施形態において実装される特徴は、論理的に可能な場合には別の実施形態に実装され得る。特定の詳細事項は、様々であり得、依然として、本設計の精神および範囲内にあることが企図され得る。結合されるという用語は、コンポーネントに直接的、または別のコンポーネントを通じてコンポーネントに間接的、のいずれかで接続されることを意味すると定義される。

【００２３】

一般に、人工知能が、サイバーセキュリティ脅威を分析する。サイバー防御システムは、ｅメールシステムと関連付けられたｅメール活動およびユーザ活動の正常な挙動について訓練されるモデルを使用することができる。サイバー脅威モジュールは、メール活動およびユーザ活動の正常な挙動について訓練されるモデルを参照し得る。分析下のｅメール活動およびユーザ活動の一連の１つまたは複数の非正常な挙動が、得られた正常な無害の挙動から外れる可能性を考慮に入れた脅威リスクパラメータが決定される。自律応答モジュールは、行動を取る人間ではない、サイバー脅威モジュールからの脅威リスクパラメータが、行動の指針となり得るしきい値に等しいかまたはそれより大きいとき、サイバー脅威を阻止するために取られるべき１つまたは複数の自律的迅速行動を引き起こすために使用され得る。

【００２４】

図１は、少なくともｅメールシステムと関連付けられたｅメール活動およびユーザ活動の正常な挙動について訓練される機械学習モデルを参照するサイバー脅威モジュールを有するサイバー脅威防御システムであって、サイバー脅威モジュールが、「分析下のｅメール活動およびユーザ活動の一連の１つまたは複数の非正常な挙動が、得られた正常な無害な挙動から外れる可能性」、したがって悪意のある挙動である可能性が高いことを考慮に入れた脅威リスクパラメータを決定する、サイバー脅威防御システムの一実施形態のブロック図を示す。

【００２５】

サイバー脅威防御システム１００は、ｅメールシステムならびにそのネットワークからのサイバーセキュリティ脅威に対して保護し得る。サイバー脅威防御システム１００は、ｉ）トリガモジュール、ｉｉ）収集モジュール、ｉｉｉ）データストア、ｉｖ）ネットワークモジュール、ｖ）ｅメールモジュール、ｖｉ）ネットワーク＆ｅメールコーディネータモジュール、ｖｉｉ）サイバー脅威モジュール、ｖｉｉｉ）ユーザインターフェースお

よび表示モジュール、ｉｘ）自律応答モジュール、ｘ）ｅメール自体の特徴およびその関連データについて訓練される第１の人工知能モデルと、潜在的なサイバー脅威について訓練される第２の人工知能モデルと、各々が異なるユーザ、デバイス、システム活動、およびシステム内のエンティティ間のインタラクション、ならびにシステムの他の態様について訓練される１つまたは複数の人工知能モデルとを含む、１つまたは複数の機械学習モデル、ならびにｘｉ）サイバー脅威防御システム内の他の同様のコンポーネントなどのコンポーネントを含み得る。

【００２６】

トリガモジュールは、Ｉ）非正常なもしくはＩＩ）疑わしい挙動／活動から１つまたは複数のｉ）イベントおよび／またはｉｉ）アラートが発生していることを示すタイムスタンプ付きのデータを検出し得、次いで何か非正常なことが起きていることをトリガする。したがって、収集装置モジュールは、ｉ）異常な挙動、ｉｉ）疑わしい活動、およびｉｉｉ）それら両方の任意の組み合わせの特定のイベントおよび／またはアラートによってトリガされる。インラインデータは、トラフィックが観察されるときにデータストアからデプロイメント上に収集され得る。この場所で利用可能なデータの範囲および幅広いバリエーションは、分析のために良好な品質のデータを結果としてもたらす。収集されたデータは、サイバー脅威モジュールに渡される。

【００２７】

収集装置モジュールは、分析されるイベントおよび／またはアラートについて形成される特定の仮説に応じて各々がデータの異なる側面を見る複数の自動データ収集装置からなり得る。可能性のある仮説の各々のタイプに関連するデータは、追加の外部および内部ソースから自動的に引き出される。いくつかのデータは、各々の可能性のある仮説について、収集装置モジュールによって引き出されるか、または取得される。連携のフィードバックループが、収集装置モジュール、ｅメール活動を監視するｅメールモジュール、ネットワーク活動を監視するネットワークモジュール、およびサイバー脅威モジュールの間で発生し、このプロセスの異なる側面について訓練される１つまたは複数のモデルを適用する。典型的な脅威、例えば、人間のユーザのインサイダ攻撃／不適切なネットワークおよび／またはｅメール挙動、悪意のあるソフトウェア／マルウェア攻撃／不適切なネットワークおよび／またはｅメール挙動の各々の仮説は、データの様々な支点、およびその可能性のある脅威と関連付けられた他のメトリックを有することができ、また、機械学習アルゴリズムは、データの関連点を見て、疑わしい活動および／または異常な挙動が関連することについての各々の仮説について、どんな疑わしい活動および／または異常な挙動が関連するかの特定の仮説を支持するか、またはそれに反証する。ネットワークは、収集され得る豊富なデータおよびメトリックを有し、その後、大部分のデータは、収集装置によってデータの重要な特色／顕著な特色にフィルタリングまたは集約される。

【００２８】

実施形態において、ネットワークモジュール、ｅメールモジュール、およびネットワーク＆ｅメールコーディネータモジュールは、サイバー脅威モジュールの部分であり得る。

【００２９】

サイバー脅威モジュールはまた、ｅメールシステム内のサイバー脅威について訓練される１つまたは複数の機械学習モデルを使用し得る。サイバー脅威モジュールは、ｅメールシステムと関連付けられたメール活動およびユーザ活動の正常な挙動について訓練されるモデルを参照し得る。サイバー脅威モジュールは、これらの様々な訓練された機械学習モデル、ならびにネットワークモジュール、ｅメールモジュール、およびトリガモジュールからのデータを参照することができる。サイバー脅威モジュールは、一連の非正常な挙動が、潜在的なサイバー脅威にどのように相関するか、ならびに「得られた正常な無害な挙動から外れる、したがって、悪意のある挙動である、分析下のｅメール活動およびユーザ活動のこの一連の１つまたは複数の非正常な挙動の可能性が何であるか」を考慮に入れた脅威リスクパラメータを決定することができる。

【００３０】

１つまたは複数の機械学習モデルは、教師なし学習を使用し、かつシステムの異なる側面、例えば、ｅメールシステムと関連付けられたｅメール活動およびユーザ活動の正常な挙動について訓練される、自己学習モデルであり得る。正常な挙動の自己学習モデルは、定期的に更新される。正常な挙動の自己学習モデルは、新規の入力データが受信され、それが正常な挙動の範囲内と見なされるときに更新される。正常な挙動しきい値は、コンピューティングシステムについての正常な生活パターンに対応するパラメータの変動する基準としてモデルによって使用される。正常な挙動しきい値は、コンピュータシステム内の更新された変更に従って変動し、変動する基準によって設定されるパラメータから外れるコンピューティングシステム上の挙動をモデルが見分けることを可能にする。

【００３１】

図１０は、ユーザネットワーク上の分析されるメトリック、ならびに、自己学習機械学習モデルによって使用されるコンピューティングシステムの正常な生活パターンに対応するパラメータのそれらのそれぞれの変動する基準、および対応する潜在的なサイバー脅威と比較されるコンピュータ活動およびｅメール活動を比較するサイバー脅威モジュールの一実施形態のブロック図を示す。サイバー脅威モジュールは、次いで、分析されるメトリック、および何が正常な挙動と見なされるかの変動する基準に従って、サイバーサイバー脅威の可能性を示す脅威リスクパラメータを決定することができる。

【００３２】

サイバー脅威防御システム１００はまた、ｅメールおよびそのメタデータのプロパティを分類することを含む、ｅメール自体の複数の特徴およびその関連データの理解を得ることについて訓練される１つまたは複数の機械学習モデルを含み得る。

【００３３】

サイバー脅威モジュールはまた、ｅメール自体およびその関連データについて訓練される機械学習モデルを参照して、分析下のｅメールまたはｅメールのセットが潜在的に悪意のある特徴を有するかどうかを決定することができる。サイバー脅威モジュールはまた、このｅメール特徴分析を脅威リスクパラメータのその決定において考慮に入れることができる。

【００３４】

ネットワークモジュールは、ｅメールシステムに関連付けられるネットワーク上のユーザ、デバイス、およびそれらの間のインタラクションの正常な挙動について訓練される１つまたは複数の機械学習モデルを有し得る。ユーザインターフェースは、ネットワークデータを表示するための１つまたは複数のウィンドウ、ならびに、同じユーザインターフェースを通じてディスプレイ画面上に、ｅメールおよびそれらのｅメールに関するサイバーセキュリティ詳細を表示するための１つまたは複数のウィンドウを有し、それにより、サイバー専門家が、１つのプラットフォーム内でネットワークデータとｅメールサイバーセキュリティ詳細との間でピボットし、それらを同じディスプレイ画面上の別個の領域ではなく、相互接続された全体として見なすことが可能になる。

【００３５】

サイバー脅威モジュールはまた、このネットワーク分析を、脅威リスクパラメータのその決定において考慮に入れることができる。

【００３６】

サイバー脅威防御システム１００は、少なくとも３つの別個の機械学習モデルを使用し得る（図９も参照されたい）。各機械学習モデルは、デバイス、ユーザ、ネットワークトラフィックフロー、システムを分析する１つまたは複数のサイバーセキュリティ分析ツールからの出力などの、システムについての正常な生活パターンの特定の側面について訓練され得る。１つまたは複数の機械学習モデルはまた、サイバー脅威のタイプのすべての様式の特徴および側面について訓練され得る。１つまたは複数の機械学習モデルはまた、ｅメール自体の特徴について訓練され得る。

【００３７】

ｅメール活動を監視するｅメールモジュールおよびネットワーク活動を監視するネット

ワークモジュールは共に、これらの活動同士の因果関係を相関させるためにそれらのデータをネットワーク＆ｅメールコーディネータモジュールにフィードして、この入力をサイバー脅威モジュールへ供給し得る。これらの因果関係の応用は、ブロック図、図１０および図１１に実証される。

【００３８】

サイバー脅威モジュールはまた、この特定のｅメールとネットワーク活動とのつながり因果関係分析を、脅威リスクパラメータのその決定において考慮に入れることができる（図１１を参照されたい）。

【００３９】

サイバー脅威防御システム１００は、様々なプローブを使用して、ユーザ活動およびｅメール活動を収集し、次いでその活動を、データストア、ならびに必要に応じてサイバー脅威モジュールおよび機械学習モデルにフィードする。サイバー脅威モジュールは、収集されたデータを使用して、ｅメールシステム内のｅメール活動およびユーザ活動の理解を引き入れ、ならびに、このｅメールシステムおよびそのユーザについて訓練される１つまたは複数の機械学習モデルの訓練を更新する。例えば、ｅメールトラフィックは、ＯｕｔｌｏｏｋもしくはＧｍａｉｌなどのｅメールアプリケーション内にフックを置くこと、および／またはｅメールが送達されるインターネットゲートウェイを監視することによって収集され得る。加えて、プローブは、以下の方法：組織の既存のネットワーク設備に広がるポート、インラインネットワークタップを挿入するまたは再使用すること、ならびに／またはネットワークデータの任意の既存のレポジトリにアクセスすることのうちの１つにより、ネットワークデータおよびメトリックを収集し得る（例えば、図２を参照されたい）。

【００４０】

サイバー脅威防御システム１００は、複数のユーザインターフェースを使用し得る。第１のユーザインターフェースは、ｅメールシステム内に入る／ｅメールシステムから出るｅメール、および分析下の１つまたは複数のｅメールについて知られている任意のサイバーセキュリティ特徴のすべてのインボックススタイルビューを提示するように構築され得る。ｅメールのインボックススタイルビューを有するユーザインターフェースは、分析下の１つまたは複数のｅメールを表示する第１のウィンドウ／カラム、および分析下のそのｅメールまたはｅメールのセットについて知られている関連セキュリティ特徴のすべてを伴う第２のウィンドウ／カラムを有する。複雑な機械学習技術は、ｅメールが表す正常からのいかなる逸脱も説明する変則スコアを決定し、これらは、ユーザおよびサイバー専門家が認識および理解できる慣れ親しんだ方法で、図式で表示される。

【００４１】

サイバー脅威防御システム１００は、次いで、検出された潜在的なサイバー脅威に対抗するための行動を取ることができる。

【００４２】

自律応答モジュールは、行動を取る人間ではない、サイバー脅威モジュールからの脅威リスクパラメータが、行動の指針となり得るしきい値に等しいかまたはそれより大きいとき、サイバー脅威を阻止するために取られるべき１つまたは複数の迅速な自律行動を引き起こすように構成され得る。サイバー脅威を阻止するために取られるべき１つまたは複数の自律行動を引き起こすように、自律応答モジュールと連携して構成されるサイバー脅威モジュールは、何らかの人間の介入を待たずにサイバー脅威に応答することにより、ｅメールシステム内のコンピューティングデバイスを、コンピューティングデバイスにおける未承認のＣＰＵサイクル、メモリスペース、および消費電力を消費することからのサイバー脅威の影響を制限することによって、改善する（図６も参照されたい）。

【００４３】

サイバー脅威防御システム１００は、デバイス上、１つもしくは複数のサーバ上、および／またはその独自のサイバー脅威器具プラットフォーム内でホストされ得る（例えば、図２を参照されたい）。

【００４４】
図２は、ｅメール活動およびネットワーク活動を監視し、このデータをこれらの活動同士の相互に関連した因果関係にフィードし、この入力をサイバー脅威分析に供給する、サイバー脅威防御システムの一実施形態のブロック図を示す。ネットワークは、デスクトップユニット、ラップトップユニット、スマートフォン、ファイアウォール、ネットワークスイッチ、ルータ、サーバ、データベース、インターネットゲートウェイ、サイバー脅威防御システム１００など、様々なコンピューティングデバイスを含むことができる。
【００４５】
ネットワークモジュールは、プローブを使用してネットワーク活動を監視し、また、ユーザ、デバイス、およびそれらの間のインタラクション、またはその後ｅメールシステムに関連付けられるインターネットの正常な挙動について訓練される機械学習モデルを参照することができる。
【００４６】
ユーザインターフェースは、ｉ）ネットワークデータ、アラート、およびイベントを提示／表示するための１つまたは複数のウィンドウ、ならびにｉｉ）ディスプレイ画面上の同じユーザインターフェースを通じて、ｅメールデータ、アラート、イベント、およびそれらのｅメールについてのサイバーセキュリティ詳細を表示するための１つまたは複数のウィンドウの両方を有する。ディスプレイ画面上の同じユーザインターフェース上に示されるこれらの２つの情報のセットは、サイバー専門家が、１つのプラットフォーム内でネットワークデータとｅメールサイバーセキュリティ詳細との間でピボットし、それらを別個の領域ではなく、相互接続された全体として見なすことを可能にする。
【００４７】
ネットワークモジュールおよびその機械学習モデルは、脅威のレベルを示す脅威リスクパラメータ（例えば、スコアまたは確率）を決定するために、サイバー脅威モジュールへの情報の追加入力を提供するために、潜在的に非正常なネットワーク活動を決定するために利用される。
【００４８】
特定のユーザのネットワーク活動は、ネットワークモジュールがネットワーク活動を監視し、ネットワーク＆ｅメールコーディネータモジュールが、ネットワークモジュール観察を受信して、それをこの特定のユーザのｅメール活動の理解に引き入れ、メールシステム内の異なるユーザに対して調整される結果として生じる脅威リスクパラメータを用いて潜在的なｅメール脅威の査定を行うことから、それらユーザのｅメール活動に関連付けられ得る。ネットワークモジュールは、各々のユーザのネットワーク活動を追跡し、それをネットワーク＆ｅメールコーディネータコンポーネントに送信して、ネットワーク活動およびｅメール活動を相互接続し、互いの挙動および潜在的なｅメール脅威の査定を緊密に通知する。
【００４９】
サイバー脅威防御システム１００は、ここでは、組織のネットワーク上のネットワークモジュールによって観察される潜在的な悪意のある活動を、ｅメールモジュールによって観察される特定のｅメールイベントに遡って追跡し、自律迅速応答モジュールを使用して、ネットワーク自体におけるいかなる潜在的に有害な活動もシャットダウンし、また、ネットワーク上の有害な活動をトリガするいかなる同様のｅメール活動もフリーズさせる。
【００５０】
プローブは、ユーザ活動ならびにｅメール活動を収集する。収集された活動は、データストアに供給され、非正常なまたは疑わしい挙動活動、例えば、アラート、イベントなどについて評価され、これらは、ｅメールシステム内のｅメール活動およびユーザ活動の理解を引き入れるためにサイバー脅威モジュールによって評価される。収集されたデータはまた、このｅメールシステム、そのユーザ、ならびにネットワークおよびそのエンティティについての正常な生活パターンについて訓練される１つまたは複数の機械学習モデルに対する訓練を潜在的に更新するために使用され得る。

【００５１】
ｅメールシステムの例となるプローブは、Ｏｆｆｉｃｅ ３６５ Ｅｘｃｈａｎｇｅドメインなどの、組織のｅメールアプリケーションと直接連動し、すべての内向きおよび外向きの通信のブラインドカーボンコピー（ＢＣＣ）を受信するように構成され得る。ｅメールモジュールは、組織のｅメール使用の生活パターンの包括的な認識を提供するためにｅメールを検査する。
【００５２】
図３は、一連の異常挙動が、潜在的なサイバー脅威にどのように相関するか、ならびに「分析下のｅメール活動およびユーザ活動のこの一連の１つまたは複数の非正常な挙動が、得られた正常な無害な挙動から外れる、したがって、悪意のある挙動であるという可能性」を考慮に入れた脅威リスクパラメータを決定するサイバー威モジュールの一実施形態のブロック図を示す。
【００５３】
ユーザインターフェース１５０は、サイバー脅威モジュールが検討する論理、データ、および他の詳細事項を図式で表示することができる。
【００５４】
ユーザインターフェース１５０は、例となるｅメールを表示し、この例となるｅメールは、分析を受けているときに、これに類似した正常なｅメールと統計的に一致しないヘッダー、アドレス、件名、送信者、受信者、ドメインなどの特徴を呈する。
【００５５】
したがって、ユーザインターフェース１５０は、それが挙動的に異常と分類した、例となるｅメールの非正常な活動を表示する。
【００５６】
分析中、ｅメールモジュールは、ｅメールシステムと関連付けられたｅメール活動およびユーザ活動の正常な挙動について訓練される自己学習モデルである１つまたは複数の機械学習モデルを参照することができる。これは、このｅメールシステムに対して設定される様々なｅメールポリシーおよびルールを含むことができる。サイバー脅威モジュールはまた、ｅメール自体の正常な特徴について訓練されるモデルを参照することができる。サイバー脅威モジュールは、これらの様々な訓練された機械学習モデルを、ネットワークモジュールおよびｅメールモジュールからのメトリック、アラート、イベント、メタデータを含むデータに適用することができる。加えて、ＡＩモデルのセットが、各ｅメールユーザについて、その他のネットワークと接続状態にある内部および外部アドレスアイデンティティの正常な「生活パターン」を学習することを担い得る（このデータの視覚ディスプレイについては、例えば図８を参照されたい）。これにより、システムが、そのユーザについて、その過去、そのピアグループ、およびより幅広い組織に関連して、所与のアドレスアイデンティティの正常な「生活パターン」から逸脱する悪意のあるｅメールを無効にすることが可能になる。
【００５７】
次に、ｅメールモジュールは、ｅメールが、Ｏｆｆｉｃｅ ３６５などのｅメールアプリケーションを通過する点において、少なくとも第１のｅメールプローブにｅメールを検査させ、生のｅメールコンテンツならびに送信者および受信者の過去のｅメール挙動から数百のデータ点を抽出する。これらのメトリックは、データストアから取得した対象とする受信者または送信者の生活パターンデータと組み合わされる。メトリックの組み合わされたセットは、ｅメールの単一の変則スコアをもたらすために機械学習アルゴリズムに通され、メトリックの様々な組み合わせが、ｅメールの「タイプ」を規定するのに役立つ通知を生成することを試みる。
【００５８】
「ｅメールおよびそれらのｅメールの任意の関連特性」の変則および／または非正常な挙動によってトリガされる、タイプ通知などのｅメール脅威アラートは、ｅメール媒介攻撃から生じた可能性のあるいかなるネットワークイベントもより良好に識別するために、

サイバー脅威モジュールによって使用される。

【００５９】

特定の脅威アラートおよび変則スコアと併せて、本システムは、ｅメールの送達を妨げる、または潜在的に悪意のあるコンテンツを無効にするように設計されたｅメールに対する行動を促し得る。

【００６０】

次に、データストアは、メトリックと、デフォルトでは少なくとも２７日間である、ある期間にわたって各ｅメールと関連付けられた以前の脅威アラートとを記憶する。このようなデータの集成は、ユーザインターフェース１５０内で完全に検索可能であり、ｅメール管理者およびセキュリティ専門家のために計り知れない洞察をメールフロー内へ提示する。

【００６１】

次に、サイバー脅威モジュールは、非正常なｅメールがいかなる識別可能な悪意のあるｅメールに密接に関連しない場合でさえも、変則評価を発行することができる。この値は、サイバー脅威モジュールが、このｅメールが組織および特定の内部ユーザ（インバウンド受信者またはアウトバウンド送信者のいずれか）の正常な生活パターンと比較してどれほど非正常であると見なすかを示す。サイバー脅威モジュールは、ある時間ウィンドウにおける非正常な挙動についての７５０を超えるメトリックおよび組織的生活パターンに関して検討する。例えば、サイバー脅威モジュールは、最終的な脅威リスクパラメータにおいても考慮される変則スコアをコンピューティングするときに、過去７日間における、非正常な挙動についてのメトリックおよび組織的生活パターンならびに他の補助メトリックを検討する。

【００６２】

図４は、ｅメールおよびそのメタデータのプロパティを分類することを含む、ｅメール自体の複数の特徴およびその関連データの理解を得ることについて訓練される１つまたは複数の機械学習モデルを参照するサイバー脅威防御システムの一実施形態のブロック図を示す。ｅメールモジュールシステムは、すべてのｅメールインバウンドおよびアウトバウンドからメトリックを抽出する。

【００６３】

ユーザインターフェース１５０は、サイバー脅威防御システムが検討する論理、データ、および他の詳細事項を図式で表示することができる。

【００６４】

サイバー脅威モジュールは機械学習モデルと協働して、そのｅメールシステム内のｅメール活動について豊富な生活パターンを展開するために、これらのメトリックを分析する。これにより、サイバー脅威モジュールがｅメールモジュールと連携して、既存のｅメールゲートウェイ防御を回避した／通過した非正常な変則的なｅメールを見分けることを可能にする。

【００６５】

ｅメールモジュールは、この特定の受信者によって受信される際にコンテンツがコンテンツの正常なパターンと一致しないｅメールを検出する。

【００６６】

例となる分析は以下の通りであり得る。

このｅメールの送信者が、以前に受信側の組織内の個人とどの程度まで連絡を取っていたか？

このメールの受信者が、送信者と以前に連絡を取ったこれらの個人とどれくらい密接な関係があるか？

このｅメールのコンテンツが、対象とする受信者が送信または受信する他のｅメールと一致するか？

対象とする受信者によってクリックされるまたは開かれるべきリンクまたは添付ファイルがｅメール内に存在する場合、これがその個人の正常なネットワーク挙動に対して変則

的な活動を構成するか？
ｅメールプロパティが、この特定のユーザの最近のネットワーク活動と一致するか？
【００６７】
こうして、サイバー脅威モジュールはまた、ｅメール自体およびその関連データについて訓練される機械学習モデルを参照して、分析下のｅメールまたはｅメールのセットが潜在的に悪意のある特徴を有するかどうかを決定することができる。サイバー脅威モジュールはまた、このｅメール特徴分析を脅威リスクパラメータのその決定において考慮に入れることができる。
【００６８】
ｅメールモジュールは、Ｏｆｆｉｃｅ　３６５メタデータなどのｅメールアプリケーションのメタデータを遡及的に処理して、それらのユーザの各々、およびそれらユーザのｅメールアドレス、通信相手、ならびに定常操作の詳細な知識を得ることができる。サイバー脅威モジュールの威力は、ｅメールユーザの各々の、それらユーザの過去、それらユーザのピアグループ、およびより幅広い組織に関連して、日々のユーザｅメール挙動のこのような固有の理解を活用することにある（ｅメールアドレスの関連性データの視覚表示については、例えば図８を参照されたい）。悪意のある通信の既定のテンプレートに何がフィットするかではなく、特定の組織および特定の個人について何が「正常」であるかの知識を持つことにより、サイバー脅威モジュールは、無害の通信を模倣しかつ日常の活動として隠された脅威を置く巧妙で精巧なｅメールキャンペーンを識別することができる。
【００６９】
次に、ｅメールモジュールは、観察されるすべてのｅメールの包括的なｅメールログを提供する。これらのログは、複雑な論理クエリを用いてフィルタリングされ得、各ｅメールは、データストアに記憶されたｅメール情報内の膨大な数のメトリックについて問い合わせされ得る。
【００７０】
記憶および分析され得るいくつかの例となるｅメール特徴は、以下である。
【００７１】
ｅメール宛先：メッセージ宛先－アウトバウンドｅメールおよびインバウンドｅメール。
【００７２】
送信時間：送信時間は、メッセージメタデータに従う、ｅメールが元々送信された日時である。
【００７３】
リンク：ｅメール内のすべてのウェブリンクは、その独自のプロパティを有する。ウェブサイトへのリンクは、ｅメールの本文から抽出される。限定されるものではないが、テキスト内の位置、ドメイン、他のｅメールにおけるドメインの出現の頻度、ならびにそれらのｅメールの変則スコアにどれくらい関係するか、そのドメインがｅメールの対象とする受信者の正常な生活パターン、それら受信者の推定ピアグループ、およびそれら受信者の組織にどれくらい良くフィットするかなどの様々な属性が含まれる。
【００７４】
受信者：ｅメールの受信者。ｅメールが複数の受信者宛てだった場合、これら受信者は各々が「受信者」として見られ得る。受信者が送信者にどれくらいよく知られているかなどのｅメール受信者の既知のアイデンティティプロパティ、メールの量の記述子、および、ｅメールが経時的に、どのように変化したか、受信者のｅメールドメインがネットワークの内側でどの程度まで関わり合いがあるか。
【００７５】
件名：ｅメール件名。
【００７６】
添付ファイル：メッセージと関連付けられたすべての添付ファイルは、個別のエントリとしてここではユーザインターフェース内に現れ、各エントリは、表示されかつ詳細に描かれるメトリックに対して問い合わせ可能である。これらは、限定されるものではないが

、添付ファイル名、検出されたファイルタイプ、受信者がそのようなファイルを受信する可能性の記述子、それらのｅメールの様々な変則スコアに反するすべてのｅメール内のファイルなどのファイルの配信の記述子を含む。

【００７７】

ヘッダー：ｅメールヘッダーは、例えば、送信者、受信者、メッセージコンテンツタイプなどの重要な情報を提供する、各メッセージに伴うメタデータのラインである。

【００７８】

図１０は、コンピュータのネットワーク活動を、そのネットワーク活動に関係のあるコンテンツを含むｅメールを受信するそのコンピュータのユーザより前に、ｅメールモジュールに通知するネットワークモジュールの一例を示す。

【００７９】

図１１は、コンピュータのウェブ閲覧活動に関する生活情報の推定パターンを、その生活のパターンと一致していない内容を含むｅメールを受信するそのコンピュータのユーザより前に、ｅメールモジュールに通知するネットワークモジュールの一例を示す。

【００８０】

ユーザインターフェースは、分析下のその他のネットワークに関連してｅメールについての例となる一連の非正常な挙動のグラフ２２０を表示することができる。

【００８１】

ネットワーク＆ｅメールモジュールは、ｅメール領域からのアラートおよびイベントをネットワーク領域からのアラートおよびイベントに結び付けることができる。

【００８２】

サイバー脅威モジュールは、１つまたは複数の機械学習モデルと連携する。１つまたは複数の機械学習モデルは、サイバー脅威分析のために、「非正常なパターンから生じる一連の全く異なるアラートおよび／またはイベントにより何が起こる可能性があるのか」を推論し、次いで、非正常なパターンを形成する一連のアラートおよび／またはイベントのその全く異なる項目と関連付けられた脅威リスクを割り当てるように、数学アルゴリズムを用いて訓練され、およびそれを用いて別途構成される。

【００８３】

これは、サイバー脅威モジュールおよび機械学習モデルによる、分析下のネットワーク／システム／デバイス／ユーザ／ｅメールの非正常な挙動が何であるかの「挙動パターン分析」である。サイバー防御システムは、正常な挙動から逸脱する非正常な挙動を使用し、次いで、一連の非正常な挙動およびこの一連の非正常な挙動同士の因果関係を構築して、サイバー脅威を検出する。非正常な挙動が何であるかの例となる挙動パターン分析は、以下の通りであり得る。非正常なパターンは、分析下のそのネットワーク／システム／デバイス／ユーザ／ｅメールについての正常な生活パターンであることのウィンドウ内に入る活動／イベント／アラートをフィルタアウトすることによって決定され得、次いで、残っている活動／イベント／アラートの挙動のパターンは、フィルタリングの後に、そのパターンが悪意のある当事者―人間、プログラム、ｅメール、または他の脅威―の挙動を示すかどうかを決定するために分析され得る。防御システムは、そのパターンが悪意のある当事者の挙動を示すかどうかの可能性のある仮説を支持するか、またはそれに反証するのに役立てるために、フィルタアウトされた正常な活動のうちのいくつかに戻って、それらを引き出すことができる。その連鎖内に含まれる例となる挙動パターンは、例である７日の時間フレームにわたるグラフに示される。防御システムは、非正常なデータ転送の一連の変則的な挙動を３回、非正常なデータ転送に何らかの因果関係を有するように見える、監視されるシステム内のｅメールにおける非正常な特徴を３回検出する。同様に、情報焦点地域へのアクセスを得ようとするという非正常な挙動を試みた２回の非正常な認証情報、または非正常な挙動を試す非正常な認証情報と関連付けられた悪意のあるＩＰアドレスおよびユーザは、非正常な特徴を有するそれら３つのｅメールのうちの少なくとも１つと因果関係を有する。個々の挙動またはグループとしての連鎖の挙動パターン分析が、悪意のある脅威を示すものであると考えられるとき、防御システムが、非正常なパターンが悪

意のある当事者によって引き起こされたかどうかを識別するというこのアセスメントにどれくらいの確信があるのかのスコアが作成される。次に、さらに割り当てられるのは、この悪意のある当事者がどのレベルの脅威をシステムにもたらすかを示す脅威レベルパラメータ（例えば、スコアまたは確率）である。最後に、サイバー脅威防御システムは、脅威の構成可能なレベルに等しいまたはそれ以上である異なるタイプのサイバー脅威について、この悪意のある当事者によってもたらされたとき、防御システムが、あるとすれば、どのタイプの自動応答行動を取り得るかに関して、防御システムのそのユーザインターフェース内で構成可能である。

【００８４】

サイバー脅威モジュールは、非正常なパターンをその一連の全く異なるアラートおよび／またはイベントのサイバー脅威分析についての全く異なる項目へと形成する個々のアラートおよびイベントをつなぎ得る。サイバー脅威モジュールは、メール脅威について訓練される１つまたは複数の機械学習モデルを参照して、非正常なパターンを形成する一連のアラートおよび／またはイベントで構成されている全く異なる項目を形成する個々のアラートおよび／またはイベントから同様の特徴を識別し得る。

【００８５】

１つまたは複数の機械学習モデルはまた、非正常なパターンを形成する一連／一群のアラートおよび／またはイベントと関連付けられた脅威リスクを分析するために、サイバー脅威のタイプのすべての様式の特徴および側面について訓練され得る。高等な数学を使用する機械学習技術は、ルールなしに、以前に識別されなかった脅威を検出し、自動的にネットワークを防御することができる。

【００８６】

本モデルは、コンピュータおよびコンピュータネットワークにおける挙動変化を検出するために、教師なしベイジアン数学モデルのアプリケーションによる正常な挙動における確率的変化を通じた脅威検出により実施し得る。核となる脅威検出システムは、「ベイジアン確率」と呼ばれる。ベイジアン確率アプローチは、複数の時系列データにおける周期性を決定し、変則挙動検出の目的のために単一または複数の時系列データにわたる変化を識別することができる。メール、およびデータのネットワーク生ソースから、大量のメトリックを得ることができ、各々が所与のメトリックの時系列データをもたらす。

【００８７】

サイバー脅威モジュールであって、そのネットワークモジュールおよびｅメールモジュールコンポーネントを含むサイバー脅威モジュール内の検出器は、ターゲットを用いて異なる変数のセットに対して特定の数学的方法を実施する離散数学モデルであり得る。したがって、各モデルは、例えば、ｉ）そのサイバーセキュリティ分析ツール、ｉｉ）ｅメールの様々な側面を分析すること、ｉｉｉ）システム内の特定のデバイスおよび／またはユーザなどによってもたらされるアラートおよび／またはイベントの生活パターンについて特にターゲットとされる。

【００８８】

根本的には、サイバー脅威防御システムは、デバイスのネットワーク挙動の大量の異なる尺度／異なる尺度のセットの分析に基づいて、何が「正常な」挙動を構成するかを数学的に特徴付ける。サイバー脅威防御システムは、サイバー脅威防御システムによって保護されているシステム内のすべての人物、デバイス、ｅメール活動、およびネットワーク活動について何が正常を表すのかを理解する精巧な「生活パターン」を構築することができる。

【００８９】

論じられるように、各機械学習モデルは、デバイス、ユーザ、ネットワークトラフィックフロー、システムを分析する１つまたは複数のサイバーセキュリティ分析ツールからの出力、各ユーザのｅメール連絡関連性、ｅメール特徴など、システムの正常な生活パターンの特定の側面について訓練され得る。１つまたは複数の機械学習モデルは、システムの正常な生活パターンが何であるかを確立するために少なくとも教師なし学習アルゴリズム

を使用し得る。機械学習モデルは、ｉ）そのシステムのためのアラートおよびイベントの過去の正常な配信、ならびにｉｉ）そのシステムのためのアラートおよび／またはイベントの挙動の正常な生活パターンを確立するために同様のピアシステムからの正常な配信情報が考慮に入れられること、の両方について訓練することができる。機械学習モデルの別のセットは、ｅメールの特徴ならびにそのｅメールユーザの活動および挙動について訓練して、これらについての正常を確立する。

【００９０】

モデルが少なくとも２つの異なるアプローチを活用して変則を検出する：例えば、各システムの挙動をそれ自身の履歴と比較すること、およびそのシステムをそのピアの履歴と比較すること、ならびに／または、例えば、ｅメールをｅメールの特徴ならびにそのｅメールユーザの活動および挙動の両方と比較するとき、この複数ソースの比較は、セキュリティ侵害されるデバイス／ユーザ／コンポーネント／ｅメールが、それらの近しいピアとは異なる挙動を呈することから、モデルが既存の悪い挙動を「正常」として学習することを回避することを可能にするということに留意されたい。

【００９１】

加えて、１つまたは複数の機械学習モデルは、ｉ）同じ複数の次元空間内にマッピングされるそのシステムのためのアラートおよびイベントの過去の正常な配信に対応するそのシステムについての正常な生活パターンと、ｉｉ）分析下の現在の一連の個々のアラートおよびイベント挙動との比較を使用することができる。この比較は、プロットされた個々のアラートおよび／またはイベント内の挙動の１つまたは複数の非正常なパターンの検出をもたらすことができ、それが、単に既定義の記述的オブジェクトおよび／またはシグネチャを用いてサイバー脅威を見つけ出すことと比較して、以前に識別されなかったサイバー脅威の検出を可能にする。したがって、低レベルのアラートおよびイベントを生成するために自らがいつ行動を起こすかをえり好みしようとするますます利口な悪意のあるサイバー脅威が、サイバー分析の他の方法ではまだ識別されていなかったとしても、依然として検出されることになる。これらの利口な悪意のあるサイバー脅威は、マルウェア、スパイウェア、キーロガー、ｅメール内の悪意のあるリンク、ｅメール内の悪意のある添付ファイルなど、ならびに任意の高レベルのアラートまたはイベントを始動させない方法をよく知っている不法な内部情報技術スタッフを含み得る。

【００９２】

本質的に、プロッティングおよび比較は、そのシステムにとって正常であることをフィルタアウトし、次いでそのシステムにとって異常または非正常なことについての分析に焦点を合わせることができるやり方である。その後、一連の非正常なイベントおよび／またはアラートにより何が起こり得るかの各々の仮説について、収集装置モジュールは、元々「正常な挙動」と見なされるメトリックのプールを含むデータストアから追加のメトリックを集めて、分析下のこの一連の非正常な挙動により何が起こり得るかの各々の可能性のある仮説を支持するか、またはそれに反証し得る。

【００９３】

非正常なパターンを形成する一連のアラートおよび／またはイベント内の個々のアラートおよび／またはイベントの各々が、巧妙な異常な挙動を示すことができ、したがって、各アラートおよび／またはイベントは、その個々のアラートおよび／またはイベントと関連付けられた低い脅威リスクを有することができるということに留意されたい。しかしながら、１つまたは複数の機械学習モデルによって一連の非正常なパターンを形成する全く異なる一連／一群のアラートおよび／またはイベント挙動として分析されるとき、その全く異なる一連／一群のアラートおよび／またはイベントは、ここではその連鎖内の個々のアラートおよび／またはイベントのいずれかよりもはるかに高い脅威リスクを有することが決定され得る。

【００９４】

加えて、今日のサイバー攻撃は、人間による応答が十分な速さで生じることができないほどの深刻度および速度のものであり得るということに留意されたい。これらの自己学習

の進展のおかげで、今では、マシンが、これらの台頭する脅威を発見し、最も深刻なサイバー脅威に反撃するために適切なリアルタイムの応答を展開することが可能である。

【００９５】

脅威検出システムは、真の変則を見分けるために自己学習して正常性を検出する能力を有し、あらゆるサイズの組織が、個々および群レベルの両方で組織のネットワーク上のユーザおよびマシンの挙動を理解することを可能にする。既定義の記述的オブジェクトおよび／またはシグネチャを使用するのではなく、挙動を監視することは、より多くの攻撃が前もって見分けられ、不正行為の極めて巧妙な標識が検出され得ることを意味する。従来のレガシー防御とは異なり、特定の攻撃タイプまたは新規マルウェアは、それが検出され得る前に、第一に目にされる必要がない。挙動防御アプローチは、今日のますます精巧なサイバー攻撃ベクトルを予測し把握するために、セキュリティ侵害の際およびその地点の後で、マシン、ｅメール、および人間の活動の両方を挙動的に、数学的にモデル化する。したがって、何が正常であるかをコンピュータ的に確立して、次いで異常であることを検出することが可能である。加えて、機械学習は、確率的数学を使用して、挙動に関する仮定を絶えず再訪する。サイバー脅威防御システムの教師なし機械学習法は、予め規定されたラベルを用いてデータを訓練することを必要としない。代わりに、それらは、人間による入力を必要とすることなく、データ内の主なパターンおよび傾向を識別することができる。

【００９６】

ユーザインターフェースおよび出力モジュールはまた、一連の挙動を形成する個々のアラートおよび／またはイベントを、ｉ）時間のウィンドウの横軸、ｉｉ）連鎖内の各アラートおよび／またはイベントに割り当てられた脅威リスクを示す目盛りの垂直軸、ならびに、ｉｉｉ）連鎖の全く異なる項目を形成する個々のアラートおよびイベント間で共有される同様の特徴に対する異なる色（例えば、赤、青、黄色などであり、またグレースケールの場合は、潜在的に異なるハッシュパターンを有するグレー黒および白の異なる濃淡）という第３の次元の、少なくとも３次元を有するユーザインターフェース上へ投影し得る。人間が、データのテキストログを単に閲覧するのではなく、特定の連鎖を空間的およびコンテンツごとに作り上げるのは何であるかを視覚的に見ることができるように、連鎖内のイベントおよび／またはアラートのこれらの類似性は、例えば、同じデバイス、同じユーザ認証情報、同じグループ、同じソースＩＤ、同じ宛先ＩＰアドレス、同じタイプのデータ転送、同じタイプの非正常な活動、同じタイプのアラート、行われている同じ珍しい接続、同じタイプのイベントなどによってもたらされるアラートまたはイベントであり得る。人間の知力が、投影されたパターンおよび対応するデータを視覚的に見ると、人間は、サイバー脅威がもたらされるかどうかを最終的に決定することができるということに留意されたい。ここでも、少なくとも３次元の投影は、人間がこの情報をより容易に合成することに役立つ。ユーザインターフェース上への視覚化は、サイバー脅威防御システムがなぜこれらの凝集されたアラートおよび／またはイベントが潜在的に悪意のあるものであり得るかを支持する、またはそれに反証するデータを人間が見ることを可能にする。また、単純な２値出力「悪意のある」または「無害の」を生成する代わりに、サイバー脅威防御システムの数学アルゴリズムは、潜在的なセキュリティ侵害の異なる程度を示す出力をもたらす。

【００９７】

サイバー脅威防御システム１００は、少なくとも３つの別個の機械学習モデルを使用し得る。各機械学習モデルは、デバイス、ユーザ、ネットワークトラフィックフロー、システムを分析する１つまたは複数のサイバーセキュリティ分析ツールからの出力などの、システムについての正常な生活パターンの特定の側面について訓練され得る。１つまたは複数の機械学習モデルはまた、サイバー脅威のタイプのすべての様式の特徴および側面について訓練され得る。１つまたは複数の機械学習モデルはまた、ｅメール自体の特徴について訓練され得る。

【００９８】

実施形態において、１つまたは複数のモデルは、これらの幅広い概念の特定の側面について訓練され得る。例えば、モデルは、関連性、添付ファイル、コンプライアンス、データ損失＆転送、通則、メタデータ、衛生状態、リンク、近接、なりすまし、タイプ、検証、および他の変則について具体的に訓練され得る。

【００９９】

したがって、例えば、第１のｅメールモデルは、Ｏｆｆｉｃｅ　３６５メタデータを遡及的に処理して、ユーザ、ｅメールアドレス、通信相手、および定常操作の詳細な知識を得る。暗号化されたｅメールを用いた環境においてさえ、サイバー防御システムは、メタデータからキーマーカを得ること、ならびに通信相手のアイデンティティ、通信の頻度、および潜在的なリスクへの価値のある洞察を提供することができる。

【０１００】

加えて、１つまたは複数の機械学習モデルは、教師なし学習アルゴリズムを使用した自己学習であり得る。例えば、１つまたは複数の機械学習モデルのセットは、ユーザの正常な挙動およびそれらユーザのｅメールについて訓練され得、訓練をするためのプローブからのデータを使用し、したがって、正常な挙動の基準線が何であるかを定期的に更新する。この自律的な自己学習防御システムは、悪意のある活動が、ｉ）フィッシングおよびマルウェアｅメールなど、ｅメールからの標準の脅威当事者、ならびにｉｉ）ユーザからのインサイダ脅威のいずれであるにしろ、ｅメールドメイン内の悪意のある活動に対して保護し、それは、悪意のあるｅメールドメイン活動の事前に認識される恣意的なアイディアだけに依存することはなく、代わりに、ユーザおよび組織の標準の挙動と比較してその変則を評価するために各通信を自律的にコンテクスト化する。

【０１０１】

上述のように、１つまたは複数のモデルは、コンプライアンス懸案事項について訓練され得る。しかしながら、コンプライアンス問題について具体的に訓練されるモデルがなくても、訓練されるモデルはまた、コンプライアンス懸案事項を満足させるために使用され得る。

【０１０２】

サイバー脅威モジュールの威力は、ユーザの過去、ユーザのピアグループ、およびより幅広い組織に関連して、日々のユーザｅメール挙動のこのような固有の理解を活用することにある。悪意のある通信の既定のテンプレートに何がフィットするかではなく、特定の組織および特定の個人について何が「正常」であるかの知識を持つことにより、サイバー脅威モジュールは、無害の通信を模倣しかつ日常の活動として隠された脅威を置く巧妙で精巧なｅメールキャンペーンを識別することができる。

【０１０３】

図６は、ｅメールシステム内のｅメールが、フィルタリング可能、検索可能、およびソート可能であるようにするために、サイバー脅威防御システムのユーザインターフェースの例となるウィンドウの一実施形態のブロック図を示す。

【０１０４】

ユーザインターフェース１５０は、ｅメールシステム内のｅメールが、一般的なユーザがよく知っている、ｅメールアプリケーションのユーザインターフェース１５０のようなスタイルであるように外観が構成される、フィルタリング可能、検索可能、およびソート可能なものであることを可能にする。ユーザインターフェース１５０は、ｅメールシステム内のｅメールが、第１のウィンドウ内で分析下の１つまたは複数のｅメールをカスタマイズし、それをターゲットとし、次いでそれらの１つまたは複数のｅメールについて知られている関連セキュリティ特徴を伴う第２のウィンドウの隣に示すために、フィルタリング可能、検索可能、およびソート可能なものであることを可能にする。したがって、これら２つのウィンドウは、それらのそれぞれの情報を同じディスプレイ画面上に表示し、このユーザインターフェース１５０は、サイバー専門家が分析下のｅメールを分析して、それらの１つまたは複数のｅメールが実際にサイバー脅威であるかどうかをより良好に評価することを可能にする。ユーザインターフェース１５０は、非常に複雑な機械学習を調査

およびカスタマイズし、次いでｅメールまたはｅメールのセットの結果として生じる分析を、把握が容易であり外観になじみのある図式的なユーザインターフェース１５０内で見る能力をサイバー専門家に与える。

【０１０５】

ユーザインターフェース１５０は、脅威を調査し、組織のｅメール衛生状態へのより良好な洞察を得るために使用され得る。これは、セキュリティチームが、重要な幹部および他の可能性の高いターゲットを、システム内の他のユーザからの異なる様式でのフィッシングキャンペーンおよびサプライチェーン攻撃を含む攻撃から保護する、ユーザのシステム内の異なるレベルのユーザに合わせたプログラムを実施するのに役立ち得る。

【０１０６】

ユーザインターフェース１５０はまた、なぜ自律応答が呼び出されたかの正確な論理を表示することができる。

【０１０７】

検索フィールドにおいて、サイバー専門家は、自然文および／または構造化されたブール検索を作成して、ユーザ、ｅメールアドレス、ドメイン、観察されるリンク、エイリアスなどについてグローバルｏｍｎｉ検索を実施し得る。

【０１０８】

日付範囲フィールドにおいて、サイバー専門家は、表示されるべき特定の時間フレーム内に入るデータのみを取得し得る。

【０１０９】

フィルタターゲットフィールドは、サイバー専門家が、ｅメールメッセージのどの部分がクエリ論理に対して検査されるかを選択することを可能にする。

【０１１０】

ｅメールシステム内に入る／ｅメールシステムから出るすべてのｅメールおよび分析下の１つまたは複数のｅメールについて知られている任意のサイバーセキュリティ特徴のインボックス－スタイルビューを有するユーザインターフェースの実施形態。ｅメールのインボックス－スタイルビューを有するユーザインターフェースは、分析下の１つまたは複数のｅメールを表示する少なくとも第１のウィンドウ／カラム、および分析下のそれらのそのｅメールまたはｅメールのセットについて知られている関連セキュリティ特徴のすべてを伴う第２のウィンドウを有する。

【０１１１】

同様に別のレベルで、ユーザインターフェースは、ネットワークデータを表示するための１つまたは複数のウィンドウ、ならびに、同じユーザインターフェースを通じてディスプレイ画面上に、ｅメールおよびそれらのｅメールに関するサイバーセキュリティ詳細を表示するための１つまたは複数のウィンドウを有し、それにより、サイバー専門家が、１つのプラットフォーム内でネットワークデータとｅメールサイバーセキュリティ詳細との間でピボットし、それらを同じディスプレイ画面上の別個の領域ではなく、相互接続された全体として見なすことが可能になる。

【０１１２】

図７は、例となる自律行動であって、人間がその行動を開始することなく、自律的迅速応答モジュールが取るように構成され得る例となる自律行動の一実施形態のブロック図を示す。

【０１１３】

自律迅速応答モジュールは、ｉ）知られている悪意のあるｅメールまたはｉｉ）少なくとも悪意のある可能性が非常に高いｅメールがサイバー脅威モジュールによって決定されたときにサイバー脅威を阻止するために自律行動をいつ取るべきかを知るように、ユーザインターフェース１５０を介して、構成可能である。自律迅速応答モジュールは、脅威リスクパラメータが、分析下の１つまたは複数のｅメールがサイバー専門家によって選択可能である行動の指針となり得るしきい値に等しいかまたはそれより大きい、すなわち悪意のある可能性が少なくとも非常に高いことをサイバー脅威モジュールが示すとき、自律迅

速応答モジュールが行うことができる行動のタイプおよび特定の行動を含む、自律迅速応答モジュールが取ることができる自律行動が何であるかをプログラム／設定するように、ユーザインターフェースを通じて構成可能である管理ツールを有する。

【０１１４】

自律迅速応答モジュールが異なるユーザおよびシステムの部分のためにカスタム可能である行動のタイプおよび特定の行動、したがって、サイバー専門家が、自律的な迅速応答モジュールについてそれらの行動を自動的に取ること、およびそれらの行動をいつ自動的に取るべきかを承認／設定するように、構成可能である。

【０１１５】

自律迅速応答モジュールは、ｅメールシステムの特定のユーザへの業務上の混乱を回避するために、悪意のあるｅメールの特定のｅメール要素に対して、そのｅメールに対する全面的隔離またはブロック方式ではなく、自律的に行うためにコンテクスト化されるユーザインターフェース１５０を通じて選択可能な集中的な応答行動を含む、自律的な迅速応答モジュールに可能である行動の応答行動タイプおよび特定の行動のライブラリを有する。自律迅速応答モジュールは、業務上の混乱を反応性の高いコンテクスト化された様式で最小限にするために、それらのｅメール通信に向けた測定される様々な行動を取ることができる。

【０１１６】

自律応答モジュールは、ＡＩモデルと提携して、悪意のあるｅメールを無効にし、ターゲットとされるｅメール媒介攻撃キャンペーンに対する先制保護をリアルタイムで伝達する。

【０１１７】

自律応答モジュールと連携するサイバー脅威モジュールは、例えば、ネットワーク内の感染を検出および阻止し、この感染がそのソースとしてｅメールを有することを認識し、その悪意のあるｅメールを、企業ｅメールアカウントインボックスからそれを削除すること、またはｅメールがその対象とするユーザに達する前にその悪意のある部分を単に取り去ることによって、識別し、無効にする。自律行動は、添付ファイルを平坦化することまたは不審なリンクを取り去ることから、ｅメールが十分なリスクをもたらす場合にはｅメールを完全に食い止めることまで様々である。

【０１１８】

サイバー脅威モジュールは、セキュリティ侵害のソースを識別し、次いで、自律応答モデルにリクエストを送信することによって自律的な不成功応答行動を呼び出すことができる。この自律応答行動は、台頭する攻撃キャンペーンの蔓延を迅速に制止し、人間の応答者に、巻き返しのために必要な重大な時間を与える。

【０１１９】

実施形態において、最初、自律応答モジュールは、人間による確認モードで実行され得、すべての自律的な知的介入は、人間のオペレータによってまず確認されなければならない。自律応答モジュールが組織のｅメール挙動のその理解を精緻化しそれに特別な意味合いを持たせると、自律行動のレベルは、各自律応答行動について人間による監督が要求されなくなるまで増大され得る。大半のセキュリティチームは、このレベルに達すると、ユーザインターフェース１５０において時間をほとんど費やさない。この時、自律応答モジュール応答行動は、いかなる能動的管理の必要性もなしに悪意のあるｅメールを無効にする。自律応答モジュールは、潜在的に悪意のあると観察されるｅメールメッセージに対して１つまたは複数の積極的または反応的な行動を取り得る。行動は、脅威アラートによって、またはサイバーセキュリティシステムによって規定および検出されるような変則の挙動のレベルによって、トリガされ、エンドユーザが介入なしに安全なままであることを可能にする、ｅメール脅威への大いにカスタマイズ可能なターゲットとされる応答行動を提供する。不審なｅメールコンテンツは、さらなる検査またはリリースのための認証のために、完全に保留され得るが、自律的に、選択されたユーザはこのポリシーから免除される。ユーザ挙動および顕著な出来事は、マッピングされ得、詳細な包括的ｅメールログは、

正常な挙動のモデルと比較して幅広い範囲のメトリックによってフィルタされ、ｅメールから潜在的に悪意のあるコンテンツをリリースするか、または取り去り得る。

可能性のある行動例

【０１２０】

送達行動、添付行動、リンク行動、ヘッダーおよび本文行動などに分類される以下の行動例のセクションは、ダッシュボード上に現れ、脅威リスクパラメータがサイバーセキュリティ専門家によって設定される構成可能な設定点に等しいかまたはそれ以上であるときに、自律応答モジュールによって取られ得るか、または取られることが少なくとも提案され得る。

【０１２１】

メッセージを保留する：自律応答モジュールは、疑わしいコンテンツまたは添付ファイルが理由で送達前にメッセージを保留している。保留ｅメールは、再処理され、調査後にオペレータによってリリースされ得る。ｅメールは、送達が妨げられるか、または送達がすでに実施されている場合には、受信者のインボックスから削除される。元のメールは、データストアによってバッファキャッシュに維持され、回復され得るか、または、ユーザインターフェース１５０内の「リリース」ボタンを使用して代替のメールボックスに送信され得る。

【０１２２】

リンクをロックする：自律応答モジュールは、リンクのＵＲＬを、そのリンクのクリックがまず代替の宛先によりユーザをそらすように、置き換える。代替の宛先は、任意選択的に、処理の前にユーザからの確認を要求し得る。元のリンク宛先および元のソースは、ユーザがそのソースへのアクセスを許可される前に追加のチェックの対象となる。

【０１２３】

添付ファイルを変換する：自律応答モジュールは、典型的には初期画像変換によりＰＤＦに変換することによってファイルを平坦化し、このｅメールの１つまたは複数の添付ファイルを安全な形式に変換する。これは、添付ファイルのコンテンツを対象とする受信者に伝達するが、リスクは大幅に低減されている。画像、ｐｄｆ、およびＭｉｃｒｏｓｏｆｔ　Ｏｆｆｉｃｅ形式など、本質的に視覚的である添付ファイルの場合、添付ファイルは、画像形式へと処理され、続いて、ＰＤＦ（Ｍｉｃｒｏｓｏｆｔ　Ｏｆｆｉｃｅ形式およびＰＤＦの場合）へ、または元のファイル形式の画像（画像の場合）へレンダリングされる。いくつかのｅメールシステムにおいて、ｅメール添付ファイルは、最初に削除され、添付ファイルが処理下にあることをユーザに知らせる通知と置き換えられ得る。処理が完了すると、変換された添付ファイルは、ｅメールに挿入して戻される。

【０１２４】

リンクを二重ロックする：自律応答モジュールは、ＵＲＬをリダイレクトされるｅメールリンクと置き換える。このリンクがクリックされると、ユーザは、そのリンクの元の宛先にアクセスすることが許可されていないという、そのユーザに対する通知を提示される。ユーザは、元のソースへのリンクへ進むことができないが、リンクへ進もうとするユーザの意図は、自律応答モジュールを介してデータストアによって記録される。

【０１２５】

添付ファイルを取り去る：自律応答モジュールは、このｅメールの１つまたは複数の添付ファイルを取り去る。大半のファイル形式は、変換された添付ファイルとして送達される。可視の文書（例えば、実行可能なもの、圧縮タイプ）へ変換しないファイル形式は、リスクを低減するために取り去られる。「添付ファイルを取り去る」行動は、システムに、添付ファイルをｅメールから削除させ、それを、元の添付ファイルが削除されたことをユーザに知らせるファイルと置き換えさせる。

【０１２６】

ジャンク行動：自律応答モジュールは、ジャンクとして分類されるｅメールまたは他の悪意のあるｅメールが受信者のジャンクフォルダ、または「隔離」などの他の指定された宛先へそらされることを確実にする。

【０１２７】
リダイレクト：自律応答モジュールは、ｅメールが、対象とする受信者には送達されないが、代わりに特定のｅメールアドレスに送達されることを確実にする。
【０１２８】
コピー：自律応答モジュールは、ｅメールが元の受信者に送達されるが、コピーが別の特定のｅメールアドレスに送信されることを確実にする。
【０１２９】
保留または変更しない：特定のユーザ基準で設定され得る。自律応答モジュールは、他のモデルによって実施されるか、または一般的な脅威レベルによってトリガされる行動にかかわらず、ｅメールが決して保留されず、システムによって決して何らかの形で変更されないことを確実にする。
【０１３０】
添付ファイルに対する行動を取らない：特定のユーザ基準で設定され得る。この行動は、特定の脅威アラートに応答するにしろ、全体的に検出される変則レベルに応答するにしろ自律応答モジュールによって別の方法で取られ得るいかなる添付ファイル行動も上書きする。
【０１３１】
ヘッダーおよび本文行動：自律応答モジュールは、メールのヘッダーおよび／または本文内の既存の文、画像、または他のコンテンツに追加するまたは置き換えるために、特定のカスタム文をｅメール本文または件名に挿入する。
【０１３２】
なりすまし解除：自律応答モジュールは、標準のｅメールヘッダーアドレスフィールド（例えば、ｒｆｃ８２２タイプ）を識別し、個人名およびヘッダーｅメールアドレスを、ｅメールの真の送信者についてもっと明らかにし得る代替の名前またはｅメールアドレスと置き換える。この機構は、なりすましの企ての心理的影響を著しく低減する。
【０１３３】
図８は、ｅメールアドレス同士の関係がどのように視覚的に提示され得るか、ｅメールモジュールの一実施形態のブロック図を示す。
【０１３４】
受信者、送信者、各ユーザの連絡リストは、どれくらい近い関係が存在するか、したがって、この受信者がこの送信者からｅメールを受信する、およびその逆がどのくらい起こる可能性があるか、またはそれがどれくらい非正常であるかの因子を見るために図式化され得る。
【０１３５】
ネットワークモジュールおよびその機械学習モデルならびにｅメールモジュールおよびその機械学習モデルは、脅威リスクパラメータを決定するためにサイバー脅威モジュールへの情報の追加入力を提供する潜在的に非正常なネットワーク活動を決定するために利用される。特定のユーザのネットワーク活動は、ネットワークモジュールがネットワーク活動を監視し、サイバー脅威モジュールが、ネットワークモジュール観察を受信して、それをこの特定のユーザのｅメール活動の理解に引き入れ、メールシステム内の異なるユーザに対して調整される結果として生じる脅威リスクパラメータを用いて潜在的なｅメール脅威の査定を行うことから、それらユーザのｅメール活動に関連付けられ得る。
【０１３６】
送信者インタラクション：ユーザインターフェースの第１の区画は、送信者ｅメールアドレスについてｅメールモジュールによって観察されるｅメールインタラクションの例を図形で表す。送信者ノードは、中央ノードであり、選択された特定のメッセージの受信者は、より大きい接続ノードによって示される。
【０１３７】
受信者インタラクション：ユーザインターフェースの第２の区画は、受信者ｅメールアドレスについてｅメールモジュールによって観察されるｅメールインタラクションのすべ

ての例を図形で表す。受信者ノードは、中央ノードであり、選択された特定のメッセージの送信者は、より大きい接続ノードによって示される。

【０１３８】

ｅメールモジュールは、それが監視しているｅメールアプリケーションのドメインに関連してドメインが内部であるか外部であるかを追跡する。したがって、外部受信者／送信者にとっては、それらの組織またはドメインからの他者もまた外部のように見える。

防御システム

【０１３９】

図９は、例となるネットワークを保護するサイバー脅威防御システムの一例を示す。例となるネットワーク図９は、脅威検出システムを使用するコンピュータシステム５０のネットワークの一例を示す。図９によって描写されるシステムは、本発明の説明を簡単にするために提供される簡略化された一例を示す。システム５０は、建物内に第１のコンピュータシステム１０を備え、第１のコンピュータシステム１０は、検出のための脅威検出システムを使用し、それにより、その範囲内でコンピューティングデバイスへの脅威を防ぐことを試みる。第１のコンピュータシステム１０は、３つのコンピュータ１、２、３、ローカルサーバ４、ならびに、印刷、スキャン、およびファクシミリ機能をコンピュータ１、２、３の各々に提供する多機能デバイス５を備える。第１のコンピュータシステム１０内のデバイスのすべては、ローカルエリアネットワーク６を介して通信可能に結合される。その結果、コンピュータ１、２、３のすべては、ＬＡＮ６を介してローカルサーバ４にアクセスし、ＬＡＮ６を介してＭＦＤ５の機能を使用することができる。

【０１４０】

第１のコンピュータシステム１０のＬＡＮ６は、インターネット２０に接続され、この際インターネット２０は、コンピュータ１、２、３にサーバ３０および第２のコンピュータシステム４０を含む多数の他のコンピューティングデバイスへのアクセスを提供する。第２のコンピュータシステム４０はまた、第２のＬＡＮ４３によって接続される２つのコンピュータ４１、４２を含む。

【０１４１】

本発明のこの例示的な実施形態において、第１のコンピュータシステム１０上のコンピュータ１は、脅威検出システムを有し、したがって、第１のコンピュータシステムへの脅威を検出するための脅威検出法を実行する。したがって、コンピュータ１は、本明細書に説明されるプロセスのステップを実行するように構成されたプロセッサ、このプロセスの実行に関する情報を記憶するように要求されるメモリ、ならびに要求される情報を収集するためのネットワークインターフェースを備える。この方法は、これより図９を参照して詳細に説明されるものとする。

【０１４２】

コンピュータ１は、システム１０内の各ユーザおよびマシンの「正常な挙動」の動的な常に変化するモデルを構築し維持する。本アプローチは、ベイジアン数学に基づき、システム１０内のすべてのインタラクション、イベント、および通信―どのコンピュータがどのコンピュータと話すのか、作成されたファイル、アクセスされているネットワーク―を監視する。

【０１４３】

例えば、コンピュータ２は、企業のサンフランシスコオフィスを拠点とし、マーケティング従業員によって運用され、このマーケティング従業員は、マーケティングネットワークに定期的にアクセスし、通常、第２のコンピュータシステム４０内のこの企業のＵ．Ｋ．オフィス内のマシンと、午前９時半から正午まで通信し、およそ午前８時半から午後６時までアクティブである。この同じ従業員は、事実上一度も従業員タイムシートにアクセスすることはなく、企業のアトランタネットワークに接続することはめったになく、東南アジアには取引がない。脅威検出システムは、この従業員に関する利用可能なすべての情報を取り出し、その人物の「生活パターン」を確立し、この「生活パターン」はさらなる情報が集められると動的に更新される。「正常な」モデルは、変動する基準として使用さ

れ、システムが、この正常な生活パターンから外れるように思われるシステム上の挙動を見分け、この挙動を変則としてフラグを立て、さらなる調査を依頼することを可能にする。

【０１４４】

脅威検出システムは、今日の攻撃者がますます用心深くなっており、攻撃者は、ユーザのマシンを遅くすることなどによってエンドユーザに疑いを生じさせることを回避することを確実にするために、正常なソフトウェアプロトコルを使用してシステム内に「隠れている」場合があるという事実に対処するように構築される。したがって、いかなる攻撃プロセスも、マウスまたはキーボードが使用される場合には停止する、または「引き下がる」。しかしながら、依然としてより精巧な攻撃は、逆を試み、正常なプロセスに見せ掛けてメモリ内に隠れ、比較的単純な警備プロセスを打破しようと企ててマシンがアクティブであるときにのみＣＰＵサイクルを盗む。これらの精巧な攻撃者は、ユーザの入力と直接関連付けられない活動を探す。ＡＰＴ（Ａｄｖａｎｃｅｄ　Ｐｅｒｓｉｓｔｅｎｔ　Ｔｈｒｅａｔ：高度な持続的脅威）攻撃は、典型的には、数週間、数か月、数年という非常に長いミッションウィンドウを有し、そのようなプロセッササイクルは、マシン性能に影響を与えないように、それほど頻繁には盗まれない場合がある。しかし、どれほど攻撃が隠されかつ精巧であるとしても、セキュリティ侵害の前後で典型的なマシン挙動における測定可能な差分は、たとえ極端にわずかであるとしても存在するものである。この挙動の差分は、コンピュータ１にインストールされる脅威検出システムによって使用されるベイジアン数学分析の形態で、観察され作用され得る。

【０１４５】

サイバー防御自己学習プラットフォームは、機械学習技術を使用する。高等な数学を使用する機械学習技術は、ルールなしに、以前に識別されなかった脅威を検出し、自動的にネットワークを防御することができる。今日の攻撃は、人間による応答が十分な速さで生じることができないほどの深刻度および速度のものであり得るということに留意されたい。これらの自己学習の進展のおかげで、今では、マシンが、台頭する脅威を発見し、最も深刻なサイバー脅威に反撃するために適切なリアルタイムの応答を展開することが可能である。

【０１４６】

サイバー脅威防御システムは、サイバー脅威防御システムによって保護されているシステム内のすべての人物、デバイス、およびネットワーク活動について何が正常性を表すのかを理解する精巧な「生活パターン」を構築する。

【０１４７】

脅威検出システムは、真の変則を見分けるために自己学習し正常性を検出する能力を有し、あらゆるサイズの組織が、個別および群レベルの両方で組織のネットワーク上のユーザおよびマシンの挙動を理解することを可能にする。既定義の記述的オブジェクトおよび／またはシグネチャを使用するのではなく、挙動を監視することは、より多くの攻撃が前もって見分けられ、不正行為の極めて巧妙な標識が検出され得ることを意味する。従来のレガシー防御とは異なり、特定の攻撃タイプまたは新規マルウェアは、それが検出され得る前に、第一に目にされる必要がない。挙動防御アプローチは、今日のますます精巧なサイバー攻撃ベクトルを予測し把握するために、セキュリティ侵害の際およびその地点の後で、マシン、および人間の活動の両方を挙動的に、数学的にモデル化する。したがって、何が正常であるかをコンピュータ的に確立して、次いで異常であることを検出することが可能である。

【０１４８】

この知的システムは、価値判断をすること、およびより高い価値、より思慮に富んだタスクを実行することができる。機械学習は、複雑なアルゴリズムが考案されること、および生成される結果を解釈するための全般的なフレームワークを必要とする。しかしながら、これらのアプローチは、正しく適用されるとき、マシンが、論理的な確率ベースの決定を行い、思慮に富んだタスクを請け負うことを促進することができる。

【０１４９】

高度な機械学習は、自動化されたサイバー脅威および人間が引き起こすサイバー脅威に対する戦いの最前線にあり、ルールおよびシグネチャベースのアプローチの限界を克服する。
・機械学習は、ネットワーク内で何が正常であるかを学習する―それは、以前の攻撃の知識に依存しない。
・機械学習は、すべてのデバイスおよび人物がわずかに異なるという近代ビジネスの複雑性および多様性の規模で発達する。
・機械学習は、攻撃者のイノベーションを攻撃者に向ける―いかなる非正常な活動も可視である。
・機械学習は、確率論的数学を使用して、挙動に関する仮定を絶えず再訪する。
・機械学習は、常に最新であり、人間による入力を頼りにしない。サイバーセキュリティ技術において機械学習を利用することは難しいが、正しく実施されれば、非常に強力である。機械学習は、以前は識別されなかった脅威が、それらの発現がいかなるルールセットまたはシグネチャもトリガすることに失敗するときでさえ、検出され得ることを意味する。代わりに、機械学習は、システムが、大量のデータセットを分析し、それが目にするものについての「生活パターン」を学習することを可能にする。

【０１５０】

機械学習は、以下のようないくつかの人間の能力をマシンへ近似することができる。
・思考：機械学習は、過去の情報および洞察を使用してその判断を形成する。
・リアルタイム：システムは、情報を即時に処理する。
・自己改善：モデルの機械学習理解は、新しい情報に基づいて、絶えず挑戦および適合されている。

【０１５１】

したがって、新規の教師なし機械学習は、コンピュータが、事前の警告または監督なしに、台頭する脅威を認識することを可能にする。

教師なし機械学習

【０１５２】

教師なし学習は、予め規定されたラベルなしに問題を解明する。一連の異なる動物をソートする場合、システムは、情報を分析し、動物の異なる類を解明する。これにより、システムは、予想外のことに対処し、不確実性を受け入れることが可能になる。システムは、何を探しているのかを常に知っているわけではないが、データを独立して分類し、説得力のあるパターンを検出することができる。

【０１５３】

サイバー脅威防御システムの教師なし機械学習法は、予め規定されたラベルを用いてデータを訓練することを必要としない。代わりに、それらは、人間による入力を必要とすることなく、データ内の主なパターンおよび傾向を識別することができる。教師なし学習の利点は、コンピュータが、そのコンピュータのプログラマがすでに知っていることを超えて、以前には知られていない関係を発見することを可能にするということである。

【０１５４】

サイバー脅威防御システムは、教師なし機械学習アルゴリズムの固有の実装形態を使用して、ネットワークデータを大規模に分析し、予想外のことに知的に対処し、不確実性を受け入れる。何を探すべきかを知ることができるように過去の脅威の知識に頼る代わりに、データを独立して分類し、正常な挙動であると見なされ得ることを規定する説得力のあるパターンを検出することができる。「正常性」のこの観念を構成するそれらから逸脱する任意の新規挙動は、脅威またはセキュリティ侵害を示し得る。サイバー脅威防御システムの、サイバーセキュリティに対する教師なし機械学習の影響は、変革的である。
・別の方法では未検出されずにいる脅威が、見分けられ、強調され、コンテクストに従って優先付けされ、これらのアルゴリズムを使用して孤立され得る。
・機械学習の適用は、全ネットワーク可視性およびはるかに大幅に向上した検出レベルを提供する可能性を有し、ネットワークが内部防御機構を有することを確実にする。

・機械学習は、最も深刻なサイバー脅威に対して自動応答をいつ起こすべきか学習する能力を有し、進行中の攻撃を、それらが組織にとっての危機になる前に粉砕する。

【０１５５】

この新規の数学は、データ内の重要な関係を識別するだけでなく、そのような推論と関連付けられた不確実性を数値化する。この不確実性を知り、理解することによって、ベイジアン確率分析に基づいて、多くの結果を一貫したフレームワーク内にまとめることが可能になる。機械学習の裏の数学は、非常に複雑でありきちんと理解することは難しい。ロバストな信頼できるアルゴリズムが、現実世界環境へのそれらの適用の成功を可能にするスケーラビリティを伴って、開発される。

概要

【０１５６】

実施形態において、サイバー脅威防御システムの機械学習アルゴリズムおよびアプローチの詳細は以下の通りである。

【０１５７】

サイバーセキュリティへのサイバー脅威防御システムの確率的アプローチは、ベイジアンフレームワークに基づく。これにより、潜在的に変則のネットワーク挙動の大量の弱い標識を統合して、どれくらいの可能性でネットワークデバイスがセキュリティ侵害されるかの単一の明白な尺度を生み出すことが可能になる。この確率的数学アプローチは、ネットワークのノイズの中、たとえ何を探しているのか分からないときでも、重要な情報を理解する能力を提供する。

脅威のランク付け

【０１５８】

重要なことに、サイバー脅威防御システムのアプローチは、データ内に存在する不可避の曖昧さを説明し、異なるデータが含み得るわずかに異なる証拠レベル同士を区別する。単純な２値出力「悪意のある」または「無害の」を生成する代わりに、サイバー脅威防御システムの数学アルゴリズムは、潜在的なセキュリティ侵害の異なる程度を示す出力をもたらす。この出力は、システムのユーザが、異なるアラートを厳密な様式でランク付けして、最も早急に行動を必要とするものを優先させ、同時にルールベースのアプローチと関連付けられた多数の擬陽性の問題を削除することを可能にする。

【０１５９】

根本的には、サイバー脅威防御システムは、デバイスネットワーク挙動の大量の異なる尺度／異なる尺度のセットの分析に基づいて、何が「正常な」挙動を構成するかを数学的に特徴付ける。例は以下を含む。

・サーバアクセス
・データアクセス
・イベントのタイミング
・認証情報使用
・ＤＮＳリクエスト
・他の同様のパラメータ

【０１６０】

ネットワーク挙動の各尺度は、次いで、変則の挙動を検出するためにリアルタイムで監視される。

クラスタリング

【０１６１】

何がデバイスにとって正常と見なされるべきかを正しくモデル化するために、その挙動は、ネットワーク上の他の同様のデバイスのコンテクストにおいて分析されなければならない。これを達成するために、サイバー脅威防御システムは、教師なし学習の強みを活用して、程よいサイズのネットワーク上でさえも手動では行うことが不可能であるタスクである、デバイスの自然発生するグルーピングをアルゴリズム的に識別する。

【０１６２】

ネットワーク内の関係の展望をできる限り全体論的に達成するために、サイバー脅威防御システムは、マトリクスベースのクラスタリング、密度ベースのクラスタリング、および階層的クラスタリング技法を含むいくつかの異なるクラスタリング法を同時に採用する。結果として生じるクラスタは、次いで、模範的な挙動のモデリングを個々のデバイスに通知するために使用される。

クラスタリング：一見して、

・ネットワーク上の他の同様のデバイスのコンテクスト内で挙動を分析する。

・アルゴリズムは、手動では行うことが不可能である、自然発生するデバイスのグルーピングを識別する。

・モデルを通知するためにいくつかの異なるクラスタリング法を同時に実行する。

ネットワークトポロジ

【０１６３】

また、いかなるサイバー脅威検出システムも、ネットワークがその個々の部分の合計よりもはるかに多く、その意味のほとんどがその異なるエンティティ間の関係に含まれているということ、および複雑な脅威は、多くの場合、このネットワーク構造内のわずかな変化を誘発することができるということを認識しなければならない。そのような脅威を把握するため、サイバー脅威防御システムは、ネットワークトポロジの複数の相をモデル化することができるように、いくつかの異なる数学法を採用する。

【０１６４】

１つのアプローチは、ネットワーク内の重要な接続構造を明らかにする反復マトリクス法に基づく。これらと並行して、サイバー脅威防御システムは、ネットワークの「エネルギーランドスケープ」のモデル化により、中に隠されている変則の基礎構造を明らかにすることを可能にする、統計物理学の分野からのモデルの革新的な適用を開発した。

ネットワーク構造

【０１６５】

ネットワークデバイス、ならびにネットワーク自体の挙動のモデル化におけるさらに重要な課題は、大量の潜在的な予測変数の存在を伴う問題の高次元構造である。エンタープライズＬＡＮ、ＷＡＮ、およびクラウド内のパケットトラフィックおよびホスト活動を観察することは、入力および出力の両方が多くの相互に関係した特徴（プロトコル、ソースおよび宛先マシン、ログ変化、ならびにルールトリガなど）を含み得ることから困難である。疎かつ一貫した構造の予測関数を学習することは、過剰適合の害を回避するには重要である。

【０１６６】

このコンテクストにおいて、サイバー脅威防御システムは、Ｌ１－正則化技法（例えば、ラソー法）を適用することに基づいてネットワーク挙動および接続性のモデル内の疎構造を学習するために最先端の大規模計算アプローチを採用している。これにより、効率的に解決可能な凸最適化問題が割り当てられ、簡素なモデルをもたらし得る異なるネットワークコンポーネントおよびイベント間の真の関連性の発見が可能になる。

再帰的ベイジアン推定

【０１６７】

ネットワーク挙動の異なる尺度のこれら複数の分析を組み合わせて、各デバイスの状態の単一の包括的描写を生成するために、サイバー脅威防御システムは、ベイズフィルタの実装により再帰的ベイジアン推定（ＲＢＥ）の強みを生かす。

【０１６８】

ＲＢＥを使用して、サイバー脅威防御システムの数学モデルは、新規情報がシステムに利用可能になると、コンピュータ的に効率的な様式で絶えず適合することができる。それらは、新規の証拠と照らし合わせて脅威レベルを継続して再計算して、従来のシグネチャベースの方法が失敗するところの、変化する攻撃挙動を識別する。

【０１６９】

サイバーセキュリティへのサイバー脅威防御システムの革新的なアプローチは、変化す

るデバイス挙動およびコンピュータネットワーク構造を追跡するためのベイジアン法の使用を開拓した。サイバー脅威防御システムの数学モデリングの中核は、その数学モデルが新規のネットワークデータにリアルタイムで適用されることを可能にする精巧なソフトウェアプラットフォームによって可能にされる、模範的な挙動の決定である。その結果が、サイバー脅威またはセキュリティ侵害を示し得るコンピュータネットワーク挙動履歴内のマシンイベントにおけるわずかな変動を識別することができるシステムである。

【０１７０】

サイバー脅威防御システムは、数学分析および機械学習を使用して潜在的な脅威を検出し、システムが台頭するリスクの先を行くことを可能にする。サイバー脅威防御システムアプローチは、検出がもはや以前の攻撃のアーカイブに依存しないことを意味する。代わりに、攻撃は、ネットワーク内で何が正常性を表すかの背景理解に対して見分けられ得る。プリ定義は必要とされず、それが、最も可能性のある洞察および今日の脅威に対する防御を可能にする。検出能力に加えて、サイバー脅威防御システムは、最も脅迫的なサイバー侵害への即時の応答として、デジタル抗体を自動的に作成することができる。サイバー脅威防御システムアプローチは、サイバー脅威に対して検出および防護の両方を行う。純粋な教師なし機械学習は、機能していないサイバーセキュリティへのシグネチャベースのアプローチに対する依存を取り除く。サイバー脅威防御システムの技術は、自らのネットワークの規模を理解し、活動のレベルを観察し、潜在的に弱いエリアを検出しようとするセキュリティチームにとって必須のツールになることができる。これらは、手動で捜し出されることをもはや必要としないが、自動化されたシステムによってフラグが立てられ、それらの意義に関してランク付けされる。

【０１７１】

機械学習技術は、今日のハッカーおよびインサイダ脅威からのシステムの防御における、およびサイバー攻撃の知られていない方法への応答を定式化することにおける、基礎的な味方である。それは、サイバーセキュリティにおける画期的な段階的変化である。防御は内部で開始しなければならない。

例となる方法

【０１７２】

脅威検出システムはこれより、コンピュータおよびコンピュータネットワークにおける挙動変化を検出するための教師なしベイジアン数学モデルの適用により正常な挙動における確率的変化を通じたサイバー脅威の自動検出のための脅威検出システムによって実行されるプロセスのフローを参照してさらに詳細に説明されるものとする。

【０１７３】

核となる脅威検出システムは、「ベイジアン確率的」と呼ばれる。ベイジアン確率は、複数の時系列データにおける周期性を自動的に決定し、変則挙動検出の目的のために単一または複数の時系列データにわたる変化を識別するベイジアンシステムである。

【０１７４】

人間、マシン、または他の活動は、ステップＳ１において最初にデータをいくつかのソースから取り込み、ステップＳ２においてその生のデータから二次メトリックを得ることによってモデル化される。

【０１７５】

生のデータソースは以下を含むが、これらに限定されない。

・ＩＰまたは他のネットワークＴＡＰもしくはＳＰＡＮポートから取得される生のネットワークＩＰトラフィック
・マシン生成されたログファイル
・建物アクセス（「スワイプカード」）システム
・産業用制御システム（ＩＣＳ）分散型ネットワークを流れるＩＰまたは非ＩＰデータ
・個々のマシン、周辺機器、またはコンポーネント電力使用量
・電気通信信号強度、および／または
・オンホストのソースから得られるマシンレベル性能データ（ＣＰＵ使用量／メモリ使用

量／ディスク使用量／ディスクフリースペース／ネットワーク使用量／など）
【０１７６】
これらの生のデータソースから、所与のメトリックについて各々が時系列データを生み出す大量のメトリックが得られ得る。データは、個々のタイムスライス（例えば、観察される数は、１秒あたり、１０秒あたり、または６０秒あたりに数えられ得る）内へ放り込まれ、この個々のタイムスライスは、選択される内部サイズの任意の倍数についてより長い範囲値を提供することが必要とされる後のステージにおいて組み合わせられ得る。例えば、選択される根本的なタイムスライスが６０秒の長さである場合、各メトリック時系列は、６０秒ごとにそのメトリックについての単一の値を記憶し、次いで、６０秒の固定倍数（１２０秒、１８０秒、６００秒など）の任意の新規の時系列データが、正確性の損失なしに計算され得る。メトリックは、直接選択され、低次モデルによってベイジアン確率に供給され、この低次モデルは、データの何らかの固有の基本部分を反映し、かつ特定のドメイン知識を用いて生のデータから得られ得る。獲得されるメトリックは、システムが探している脅威に依存する。安全なシステムを提供するために、幅広い範囲の潜在的な脅威に関する大量のメトリックが獲得されるべきであるということは一般的である。知られている不審なドメインに接触するネットワーク内のコンポーネントからの通信。
【０１７７】
使用される実際のメトリックは、ここで説明されるベイジアン確率的システムには大部分は不適切であるが、いくつかの例が以下に提供される。
【０１７８】
ネットワークトラフィックから得られるメトリックは、以下のようなデータを含み得る。
・時間間隔あたりに、ネットワーク化されたデバイスに入る、またはそこを去るデータのバイト数。
・ファイルアクセス。
・通信プロセスの共通性／珍しさ
・無効なＳＳＬ証明。
・失敗した認証の試み。
・ｅメールアクセスパターン。
【０１７９】
ＴＣＰ、ＵＤＰ、または他のトランスポート層ＩＰプロトコルがＩＰネットワークにわたって使用される場合、および、代替のインターネット層プロトコルが使用される（例えば、ＩＣＭＰ、ＩＧＭＰ）場合には、使用中のプロトコルの構造の知識および基本パケットヘッダー分析が、以下のようなさらなるメトリックを生成するために利用され得る。
・ネットワーク化されたデバイスから生じ、かつ公的にアドレス指定可能なＩＰ範囲に達することを目的とする、時間間隔あたりのマルチキャストの数。
・ネットワーク化されたデバイスから生じる内部リンク－ローカルＩＰブロードキャストリクエストの数。
・パケットペイロードデータのサイズ。
・デバイスによって作られる個々のＴＣＰの数、または、デバイスによって、すべての宛先にわたる組み合わされた総計として、または任意の定義可能なネットワーク範囲へ（例えば、単一のターゲットマシン、または特定のネットワーク範囲）のいずれかで転送されるデータ。
【０１８０】
ＩＰトラフィックの場合、アプリケーション層プロトコルが決定および分析され得る場合には、例えば以下のような、時系列メトリックのさらなるタイプが規定され得る。
・ネットワーク化されたデバイスが、ここでも、任意の定義可能なネットワーク範囲に対して、または総計のいずれかで、時間間隔あたりに生成するＤＮＳリクエストの数。
・マシンが時間間隔あたりに生成する、ＳＭＴＰ、ＰＯＰ、またはＩＭＡＰログインまたはログイン失敗の数。
・生成されるＬＤＡＰログインまたはログイン失敗の数。

・ＳＭＢ、ＳＭＢ２、ＦＴＰなどのファイル共有プロトコルを介して転送されるデータ。
・Ｍｉｃｒｏｓｏｆｔ Ｗｉｎｄｏｗｓ Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙへのログイン、ＬｉｎｕｘもしくはＵｎｉｘ様システムへのＳＳＨもしくはローカルログイン、またはＫｅｒｂｅｒｏｓなどの他の認証システム。

【０１８１】

これらのメトリックを獲得するために必要とされる生のデータは、ネットワーク内部開閉装置への受動型ファイバまたは銅接続を介して、仮想開閉実装形態から、クラウドベースのシステムから、または通信デバイス自身から収集され得る。理想では、システムは、組織のフルカバレージを提供するために全通信パケットのコピーを受信する。

【０１８２】

他のソースの場合、いくつかのドメイン特有の時系列データが得られ、これらデータは各々が、そのデータの根本的なソースの全く異なるおよび識別可能な相を反映するように選択され、それは経時的なそのシステムの使用または挙動をある意味では反映する。

【０１８３】

これら時系列データの多くは、極めて疎であり、０に等しいデータ点の大部分を有する。例は、従業員が建物もしくは建物の部分にアクセスするためにスワイプカードを使用すること、または、ユーザがＭｉｃｒｏｓｏｆｔ Ｗｉｎｄｏｗｓ Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙサーバによって認証された自分のワークステーションにログインすることであり、これは、典型的には１日あたり少ない回数が実施される。例えば、常時ｏｎのウェブサーバ内外へ移動するデータのサイズ、ウェブサーバＣＰＵ利用、または複写機の電力使用量など、他の時系列データは、一層稠密される。

【０１８４】

データのタイプにかかわらず、そのような時系列データが、明確な人間の挙動、または自動化コンピュータもしくは他のシステムの結果として元来生成されるにしろ、周期性を呈すること、およびほぼ定期的な間隔で繰り返されるデータ内の様々なパターンの傾向を有することは極めて一般的である。さらには、そのようなデータが、時系列内で明白である、多くの全く異なるが独立した定期的な時間期間を有することは一般的である。

【０１８５】

Ｓ３において、検出器は、二次メトリックの分析を実行する。検出器は、ターゲットネットワークを有する異なる変数セットに対して特定の数学法を実施する離散数学モデルである。例えば、ＨＭＭは、ノード間のパケットのサイズおよび送信時間を特に見る場合がある。検出器は、大まかに配置されたモデルのピラミッドである階層内に提供される。各検出器モデルは、フィルタとして効率的に作用し、その出力をピラミッドのより高い場所にある別のモデルへ渡す。ピラミッドのトップにあるのは、最終的な脅威決定モデルであるベイジアン確率である。低次の検出器は各々が、根本的なネットワークおよびもしくはコンピュータの異なるグローバル属性または「特徴」を監視する。これらの属性は、パケット速度および形態、エンドポイントファイルシステム値、ならびにＴＣＰ／ＩＰプロトコルタイミングおよびイベントなどのすべての内部の計算的な特徴についての経時的な値からなる。各検出器は、ＨＭＭなどの内部数学モデルを所有する検出器に基づいて異なる環境因子を記録し、それについて決定を行うように特殊化される。

【０１８６】

脅威検出システムは、可能性のあるいかなる脅威も探すように構成され得る一方、実践では、本システムは、脅威検出システムが使用されているネットワークに応じて、１つまたは複数の特定の脅威を見続ける場合がある。例えば、脅威検出システムは、所望のコンプライアンスおよびヒューマンリソースポリシーなどのネットワークの知られている特徴が、確率決定出力から生じる確率異常のセットまたは変動するしきい値と協力するときにトリガすることができる明示的に規定されたヒューリスティックまたは検出器内に包含されるやり方を提供する。ヒューリスティックは、データ測定／トークン化する検出器およびローカルの文脈情報の出力から実行時に得られる原子オブジェクトを有する正規表現を呈する複雑な一連の重み付けされた論理表現を使用して構築される。これらの一連の論理

表現は、次いで、オンラインライブラリ内および／または上に記憶され、尺度／トークン化する検出器からの出力に対してリアルタイムにパースされる。例となるポリシーは、「ＨＲ懲戒状況の対象となる任意の従業員（文脈情報）が以前の挙動と比較したときに変則である様式で（ベイジアン確率出力）機密情報（ヒューリスティック定義）にアクセスしている場合にアラートをする」という形態をとり得る。言い換えると、検出器のピラミッドの異なるアレイが、特定のタイプの脅威を検出するために提供される。

【０１８７】

二次メトリック上で検出器によって実施される分析は、次いで、正常な挙動のモデルと一緒に使用するのに好適な形態でデータを出力する。分かるように、データは、正常な挙動のモデルと比較すること、および正常な挙動のモデルを更新することに好適な形態にある。

【０１８８】

Ｓ４において、脅威検出システムは、観察された挙動の生活パターン分析にマッピングされる自動化された適応周期性検出を使用して、脅威が存在する可能性を示す脅威リスクパラメータを計算する。これは、脅威が経時的に、模範的な集合的なまたは個々の挙動からの逸脱をそれ自体が示した属性の収集されたセットから存在することを推定する。自動化された適応周期性検出は、ベイジアン確率が、観察されたネットワークおよび／またはマシン内で最も適切であるように計算された時間の期間を使用する。さらには、生活パターン分析は、どのように人間および／またはマシンが経時的に行動するか、すなわち、それらが典型的にはいつ作業を開始および終了するかを識別する。これらのモデルは継続して自動的に適合するため、本質的に、既知のシステムよりも打破することが難しい。脅威リスクパラメータは、特定の構成において脅威が存在する確率である。代替的に、脅威リスクパラメータは、脅威が存在することを表す値であり、これは、脅威の可能性を示す１つまたは複数のしきい値と比較される。

【０１８９】

実践では、脅威を計算するステップは、ユーザに関連して収集される現在のデータを、分析されているユーザおよびシステムの正常な挙動のモデルと比較することを伴う。収集される現在のデータは、時間における期間に関し、これは、新規データのある特定の流入、または数秒から数日までの特定の時間期間に関連し得る。いくつかの構成において、システムは、システムの予期される挙動を予測するように構成される。予測される挙動は、次いで、脅威が存在するかどうかを決定するために実際の挙動と比較される。

【０１９０】

システムは、機械学習／人工知能を使用して、企業のネットワークの内側で何が正常であるか、および、何かが正常ではないときを理解する。システムは次いで、自動応答を呼び出して、人間のチームが巻き返すことができるまでサイバー攻撃を粉砕する。これは、接続を中断すること、悪意のあるｅメールの送信を妨げること、ファイルアクセスを妨げること、組織の外側の通信を妨げることなどを含み得る。このアプローチは、例えばラップトップの正常な挙動に影響を与えることなく攻撃を中断するためにできる限り外科的かつ管理されたやり方で始まるが、攻撃がエスカレートすると、最終的には、組織に対するより幅広い危害を防ぐためにデバイスを隔離することが必要になる。

【０１９１】

システムの精度を向上させるために、チェックは、ユーザの現在の挙動を、関連ユーザ、すなわち、単一のオフィス内のユーザと比較するために実行される。例えば、予想外に低レベルのユーザからの活動が存在する場合、これは、ユーザからの非正常な活動には起因しないかもしれないが、オフィス全体に影響を与える因子に起因し得る。異常な挙動が実際に脅威を示すかどうかを評価するために、様々な他の因子が考慮され得る。

【０１９２】

最後に、ステップＳ５において、脅威に関してさらなる行動が取られる必要があるかどうかについて、脅威リスクパラメータに基づいて決定がなされる。この決定は、脅威が存在する確率が提示された後に人間のオペレータによってなされ得るか、または、アルゴリ

ズムが、例えば、決定された確率をしきい値と比較することによって、決定を行い得る。

【０１９３】

１つの構成において、ベイジアン確率の固有のグローバル入力を前提とすると、脅威可視化の形態が提供され、それは、ユーザが、すべての内部トラフィックにわたって脅威ランドスケープを見ることができ、そのようなことを、それらの内部ネットワークがどのように構造化または稠密されるかを知る必要なしに、および「ユニバーサルな」表示がネットワークの大きさに関係なく単一の区画内に提示されるような方法で、行うことができるものである。精密な調査下のネットワークのトポロジは、インタラクティブな３Ｄユーザインターフェースを介して、デバイス通信関係に基づいてグラフとして自動的に投影される。投影は、事前のシーディングまたはスケルトン定義なしに任意のノードスケールに直線的にスケールすることができる。

【０１９４】

したがって、上述された脅威検出システムは、確率状態変数にわたる分布を維持するために再帰的ベイジアン推定の妥当性形態を実装する。この分布は、低レベルのホスト、ネットワーク、およびトラフィック観察または「特徴」の複雑なセットから構築される。これらの特徴は、反復的に記録され、プラットフォーム上でリアルタイムに処理される。エンタープライズネットワーク、生体細胞もしくはソーシャルコミュニティ、または確実にインターネット全体などの、一般には動的システム内のエンティティ間の関連性情報の妥当な表示は、経時的にトポロジ配線換えをしているおよび意味的に発展している確率的ネットワークである。入力および出力の両方が、数万、時には数百万の、相互に関係のある特徴（データトランスポート、ホスト－ウェブ－クライアントダイアログ、ログ変化、およびルールトリガなど）を含むことができる分散されたデジタルエンタープライズ内のパケットトラフィックおよびホスト活動の観察など、多くの高次構造化されたＩ／Ｏ問題において、疎かつ一貫した構造の予測関数を学習することは、正規分布の欠如という課題を抱える。これを克服するために、脅威検出システムは、作業日、シフトパターン、および他のルーチンなどの反復性の時間サイクルが動的に割り当てられる、ステップワイズ法というよりもむしろ回転する連続体を決定するデータ構造からなる。このようにして、説明変数、観察、および特徴セット間の因果関係を推論および試験するための非頻度論的アーキテクチャを提供する。これが、効率的に解決可能な凸最適化問題を可能にし、倹約モデルをもたらす。そのような構成において、脅威検出処理は、新規データの入力によってトリガされ得る。代替的に、脅威検出処理は、予測データがないことによりトリガされ得る。いくつかの構成において、処理は、特定の行動の指針となり得るイベントの存在によりトリガされ得る。

【０１９５】

本方法およびシステムは、コンピュータ可読媒体上に実行可能な形態で記憶されるソフトウェアの任意の部分を有する１つまたは複数の処理コンポーネントによって実施されるように構成される。コンピュータ可読媒体は、非一時的であり得、無線または他の搬送波を含まない。コンピュータ可読媒体は、例えば、半導体または固体メモリ、磁気テープ、リムーバブルコンピュータフロッピーディスク、ランダムアクセスメモリ（ＲＡＭ）、リードオンリメモリ（ＲＯＭ）、剛性磁気ディスク、および、ＣＤ－ＲＯＭ、ＣＤ－Ｒ／Ｗ、またはＤＶＤなどの光学ディスクなどの物理的なコンピュータ可読媒体であり得る。

【０１９６】

上述された様々な方法は、コンピュータプログラム製品によって実施され得る。コンピュータプログラム製品は、上述された様々な方法のうちの１つまたは複数の機能を実施するようにコンピュータに命令するように構成されたコンピュータコードを含み得る。そのような方法を実施するためのコンピュータプログラムおよび／またはコードは、コンピュータ可読媒体、またはコンピュータプログラム製品上の、コンピュータなどの装置に提供される。コンピュータプログラム製品の場合、一時的なコンピュータ可読媒体は、無線または他の搬送波を含み得る。

【０１９７】

コンピュータなどの装置は、本明細書内で論じられる様々な方法に従って１つまたは複数のプロセスを実施するためのそのようなコードに従って構成され得る。

ウェブサイト

【０１９８】

ウェブサイトは、サイバー脅威防御システムを構成し、分析し、それと通信するためのブラウザベースのツールまたは直接連携アプリツールとして構成される。

ネットワーク

【０１９９】

いくつかの電子システムおよびデバイスは、ネットワーク環境内で互いと通信することができる。ネットワーク環境は、通信ネットワークを有する。ネットワークは、光ネットワーク、セルラネットワーク、インターネット、ローカルエリアネットワーク（「ＬＡＮ」）、ワイドエリアネットワーク（「ＷＡＮ」）、衛星ネットワーク、第三者「クラウド」環境、ファイバネットワーク、ケーブルネットワーク、およびそれらの組み合わせから選択される１つまたは複数のネットワークを含み得る。いくつかの実施形態において、通信ネットワークは、インターネットである。通信ネットワークを介して互いと接続された多くのサーバコンピューティングシステムおよび多くのクライアントコンピューティングシステムが存在し得る。

【０２００】

通信ネットワークは、少なくとも第１のサーバコンピューティングシステムおよび第２のサーバコンピューティングシステムから選択される１つまたは複数のサーバコンピューティングシステムを、互いと、ならびに少なくとも１つまたは複数のクライアントコンピューティングシステムとも接続することができる。サーバコンピューティングシステムは各々、任意選択的に、データベースなどの系統的なデータ構造を含み得る。１つまたは複数のサーバコンピューティングシステムの各々は、１つまたは複数の仮想サーバコンピューティングシステムを有し得、複数の仮想サーバコンピューティングシステムが、設計により実装され得る。１つまたは複数のサーバコンピューティングシステムの各々は、データ完全性を保護するために１つまたは複数のファイアウォールおよび同様の防御を有し得る。

【０２０１】

少なくとも１つまたは複数のクライアントコンピューティングシステム、例えば、モバイルコンピューティングデバイス（例えば、アンドロイドベースのオペレーティングシステムを有するスマートフォン）はサーバと通信することができる。クライアントコンピューティングシステムは、例えば、第１の電気式個人用輸送車両および／または第２の電気式個人用輸送車両と通信を交換することができる場合のあるソフトウェアアプリケーションまたはハードウェアベースのシステムを含み得る。１つまたは複数のクライアントコンピューティングシステムの各々は、データ完全性を保護するために１つまたは複数のファイアウォールおよび同様の防御を有し得る。

【０２０２】

クラウドプロバイダプラットフォームは、サーバコンピューティングシステムのうちの１つまたは複数を含み得る。クラウドプロバイダは、クラウド（例えば、インターネットなどのネットワーク）内でアプリケーションソフトウェアをインストールし動作させることができ、クラウドユーザは、クライアントコンピューティングシステムのうちの１つまたは複数からアプリケーションソフトウェアにアクセスすることができる。一般に、クラウド内にクラウドベースのサイトを有するクラウドユーザは、アプリケーションソフトウェアが実行する場所であるクラウドインフラストラクチャまたはプラットフォームを単独で管理することができない。したがって、サーバコンピューティングシステムおよびその系統的なデータ構造は、共有リソースであり得、各クラウドユーザが共有リソースの特定の量の専用使用が与えられる。各クラウドユーザのクラウドベースのサイトは、クラウド内の仮想量の専用空間および帯域幅を与えられ得る。クラウドアプリケーションは、実行時に複数の仮想マシン上にタスクを模倣して変化する作業要求を満たすことによって達成

され得るスケーラビリティにおいて他のアプリケーションとは異なり得る。負荷分散装置は、仮想マシンのセットに作業を分散させる。このプロセスは、単一のアクセスポイントのみを見るクラウドユーザに対して透過的である。

【０２０３】

クラウドベースのリモートアクセスは、ハイパーテキスト転送プロトコル（「ＨＴＴＰ」）などのプロトコルを利用して、クライアントコンピューティングシステム内のウェブブラウザアプリケーションなど、クライアントコンピューティングシステム上のアプリケーションによる要求および応答サイクルに従事するようにコードされ得る。クラウドベースのリモートアクセスは、スマートフォン、デスクトップコンピュータ、タブレット、または任意の他のクライアントコンピューティングシステムによって、いつでもおよび／またはどこでもアクセスされ得る。クラウドベースのリモートアクセスは、１）すべてのウェブブラウザベースのアプリケーションからの要求および応答サイクル、３）専用オンラインサーバからの要求および応答サイクル、４）クライアントデバイス内のネイティブアプリケーションと、別のクライアントコンピューティングシステムへのクラウドベースのリモートアクセスとの直接的な間の要求および応答サイクル、ならびに５）それらの組み合わせに従事するようにコードされる。

【０２０４】

実施形態において、サーバコンピューティングシステムは、サーバエンジン、ウェブページ管理コンポーネント、コンテンツ管理コンポーネント、およびデータベース管理コンポーネントを含み得る。サーバエンジンは、基本の処理およびオペレーティングシステムレベルタスクを実施することができる。ウェブページ管理コンポーネントは、デジタルコンテンツおよびデジタル広告を受信および提供することと関連付けられた、ウェブページまたは画面の作成および表示またはルーティングを扱うことができる。ユーザ（例えば、クラウドユーザ）は、それらと関連付けられたユニフォームリソースロケータ（「ＵＲＬ」）によって、サーバコンピューティングシステムのうちの１つまたは複数にアクセスすることができる。コンテンツ管理コンポーネントは、本明細書に説明される実施形態内の機能の大部分を扱うことができる。データベース管理コンポーネントは、データベース、データベースへのクエリ、およびデータの記憶に関する記憶および取得タスクを含み得る。

【０２０５】

いくつかの実施形態において、サーバコンピューティングシステムは、ウィンドウ、ウェブページ等に情報を表示するように構成され得る。例えば、サーバコンピューティングシステム上で実行されるときに実行可能な任意のプログラムモジュール、アプリケーション、サービス、プロセス、および他の同様のソフトウェアを含むアプリケーションは、サーバコンピューティングシステムに、ディスプレイ画面スペースの一部分内にウィンドウおよびユーザインターフェース画面を表示するようにさせることができる。ウェブページに関して、例えば、クライアントコンピューティングシステム上のブラウザを介したユーザは、ウェブページと相互作用し、次いで、ユーザインターフェース画面に提示されるクエリ／フィールドおよび／またはサービスへの入力を供給することができる。ウェブページは、ウェブサーバ、例えば、サーバコンピューティングシステムによって、ハイパーテキストマークアップ言語（「ＨＴＭＬ」）またはワイヤレスアクセスプロトコル（「ＷＡＰ」）対応のクライアントコンピューティングシステム（例えば、クライアントコンピューティングシステム８０２Ｂ）またはそれらの任意の等価物上でサーブされ得る。クライアントコンピューティングシステムは、サーバコンピューティングシステムと相互作用するためにブラウザおよび／または特定のアプリケーションをホストすることができる。各アプリケーションは、ソフトウェアコンポーネントが所望の情報の詳細を取り出すために提示フィールドなどを実行するようにコードされる機能を実施するように記述されるコードを有する。例えばサーバコンピューティングシステム内のアルゴリズム、ルーチン、およびエンジンは、提示フィールドから情報を取り出し、その情報をデータベースなどの適切な記憶媒体（例えば、データベース）に入れることができる。比較ウィザードは、データベースを参照し、そのようなデータを使用するように記述され得る。アプリケーション

は、例えば、サーバコンピューティングシステム上でホストされ、例えば、クライアントコンピューティングシステムの特定のアプリケーションまたはブラウザにサーブされ得る。次いで、アプリケーションは、詳細事項のエントリを可能にするウィンドウまたはページをサーブする。

コンピューティングシステム

【０２０６】

コンピューティングシステムは、全体的または部分的に、いくつかの実施形態に従って、サーバまたはクライアントコンピューティングデバイスのうちの１つまたは複数の部分であり得る。コンピューティングシステムのコンポーネントは、限定されるものではないが、１つまたは複数の処理コアを有する処理ユニット、システムメモリ、およびシステムメモリを含む様々なシステムコンポーネントを処理ユニットに結合するシステムバスを含み得る。システムバスは、メモリバスまたはメモリコントローラ、周辺機器用バス、および様々なバスアーキテクチャのいずれかを使用するローカルバスから選択されるいくつかのタイプのバス構造のいずれかであり得る。

【０２０７】

コンピューティングシステムは、典型的には、様々なコンピューティングマシン可読媒体を含む。コンピューティングマシン可読媒体は、コンピューティングシステムによってアクセスされ得、かつ揮発性および不揮発性両方の媒体、ならびにリムーバブルおよび非リムーバブル媒体を含む任意の利用可能な媒体であり得る。限定ではなく例として、コンピューティングマシン可読媒体使用は、コンピュータ可読命令、データ構造、他の実行可能なソフトウェアまたは他のデータなどの情報の記憶を含む。コンピューター記憶媒体は、所望の情報を記憶するために使用され得、かつコンピューティングデバイス９００によってアクセスされ得る、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリもしくは他のメモリ技術、ＣＤ－ＲＯＭ、デジタルバーサタイルディスク（ＤＶＤ）もしくは他の光ディスクストレージ、磁気カセット、磁気テープ、磁気ディスクストレージもしくは他の磁気ディスクストレージデバイス、または任意の他の有形媒体を含むが、これらに限定されない。ワイヤレスチャネルなどの一時的な媒体は、マシン可読媒体には含まれない。通信媒体は、典型的には、コンピュータ可読命令、データ構造、他の実行可能なソフトウェア、または他の輸送機構を具現化し、任意の情報伝達媒体を含む。

【０２０８】

システムメモリは、リードオンリメモリ（ＲＯＭ）およびランダムアクセスメモリ（ＲＡＭ）などの揮発性および／または不揮発性メモリの形態にあるコンピュータ記憶媒体を含む。起動中などコンピューティングシステム内の要素間の情報を転送するのに役立つ基本ルーチンを含む基本入出力システム（ＢＩＯＳ）は、典型的には、ＲＯＭに記憶される。ＲＡＭは、典型的には、直ちにアクセス可能である、および／または、処理ユニットによって現在動作されているデータおよび／またはソフトウェアを含む。限定ではなく例として、ＲＡＭは、オペレーティングシステム、アプリケーションプログラム、他の実行可能なソフトウェア、およびプログラムデータの一部分を含み得る。

【０２０９】

ドライブおよび上述したそれらの関連コンピュータ記憶媒体は、コンピュータ可読命令、データ構造、他の実行可能なソフトウェア、コンピューティングシステムの他のデータのストレージを提供する。

【０２１０】

ユーザは、キーボード、タッチスクリーン、またはソフトウェアもしくはハードウェア入力ボタン、マイク、ポインティングデバイス、および／または、マウス、トラックボール、もしくはタッチパッドなどのスクローリング入力コンポーネントなどの入力デバイスを介してコンピューティングシステムにコマンドおよび情報を入力し得る。マイクは、音声認識ソフトウェアと連携することができる。これらおよび他の入力デバイスは、多くの場合、システムバスに結合されるユーザ入力インターフェースを通じて処理ユニットに接続されるが、パラレルバス、ゲームポート、またはユニバーサルシステムバス（ＵＳＢ）

などの他のインターフェースおよびバス構造によって接続されてもよい。ディスプレイモニタまたは他のタイプのディスプレイ画面デバイスもまた、ディスプレイインターフェースなどのインターフェースを介してシステムバスに接続される。モニタに加えて、コンピューティングデバイスはまた、出力周辺機器インターフェースを通じて接続され得る、スピーカ、バイブレータ、照明、および他の出力デバイスなどの他の周辺機器出力デバイスを含み得る。

【０２１１】

コンピューティングシステムは、リモートコンピューティングシステムなどの１つまたは複数のリモートコンピュータ／クライアントデバイスへの論理接続を使用してネットワーク化環境において動作することができる。論理接続は、パーソナルエリアネットワーク（「ＰＡＮ」）（例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標））、ローカルエリアネットワーク（「ＬＡＮ」）（例えば、Ｗｉ－Ｆｉ）、およびワイドエリアネットワーク（「ＷＡＮ」）（例えば、セルラネットワーク）を含み得るが、他のネットワークもまた含み得る。そのようなネットワーキング環境は、オフィス、エンタープライズ全体のコンピュータネットワーク、イントラネット、およびインターネットにありふれている。クラウドプラットフォームとやりとりをするブラウザアプリケーションまたはダイレクトアプリは、コンピューティングデバイス内にあり得、メモリに記憶され得る。

【０２１２】

本設計は、単一のコンピューティングシステム上で、および／または、本設計の異なる部分が分散コンピューティングシステムの異なる部分で実行される分散システム上で実行され得るということに留意されたい。

【０２１３】

本明細書に説明されるアプリケーションは、ソフトウェアアプリケーション、モバイルアプリ、およびオペレーティングシステムアプリケーションの部分であるプログラムを含むが、これらに限定されない。本説明のいくつかの部分は、コンピュータメモリ内のデータビットに対する動作のアルゴリズムおよび象徴的表現に関して提示される。これらのアルゴリズム的な説明および表現は、データ処理分野の当業者によって、自らの作業の内容を他の当業者に最も効果的に伝えるために使用される手段である。アルゴリズムは、ここでは、および一般的には、所望の結果につながるステップの自己一致シーケンスであると考えられる。ステップは、物理量の物理的操作を必要とするものである。通常、しかしながら必須ではなく、これらの量は、記憶される、転送される、組み合わされる、および別の方法で操作されることが可能である電気または磁気信号の形態をとる。時々、主に慣用の理由のため、これらの信号を、ビット、値、要素、記号、文字、用語、数字等と呼ぶのが便利であることが証明されている。これらのアルゴリズムは、Ｐｙｔｈｏｎ、Ｃ、Ｃ＋、または他の同様の言語など、いくつかの異なるソフトウェアプログラミング言語で書かれ得る。また、アルゴリズムは、ソフトウェア内のコード行、ソフトウェア内の構成済み論理ゲート、またはその両方の組み合わせと共に実施され得る。実施形態において、論理は、ブール論理のルールに従う電気回路、命令のパターンを含むソフトウェア、またはその両方の任意の組み合わせからなる。

【０２１４】

しかしながら、これらの用語および同様の用語のすべては、適切な物理量と関連付けられることになり、これらの量に適用される便利なラベルにすぎないということについて留意すべきである。上の記載から明白であるように別途明確に示されない限り、説明全体を通して、「処理」または「コンピューティング」または「計算」または「決定」または「表示」などの用語を利用した記載は、コンピュータシステムのレジスタおよびメモリ内の物理（電子）量として表されるデータを、コンピュータシステムメモリもしくはレジスタ、または他のそのような情報ストレージ、送信または表示デバイス内の物理量として同様に表される他のデータへと操作および変換するコンピュータシステム、または同様の電子コンピューティングデバイスの行動およびプロセスを指すということを理解されたい。

【０２１５】

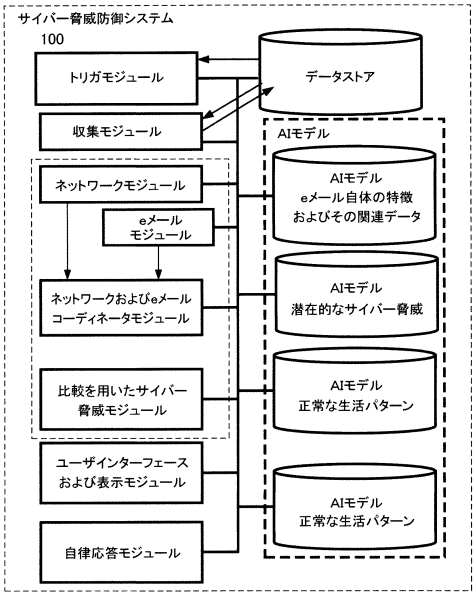
電子ハードウェアコンポーネントによって実施される多くの機能は、ソフトウェアエミュレーションによって複製され得る。したがって、それらの同じ機能を達成するために書き込まれるソフトウェアプログラムは、入力－出力回路内のハードウェアコンポーネントの機能性をエミュレートすることができる。

【０２１６】

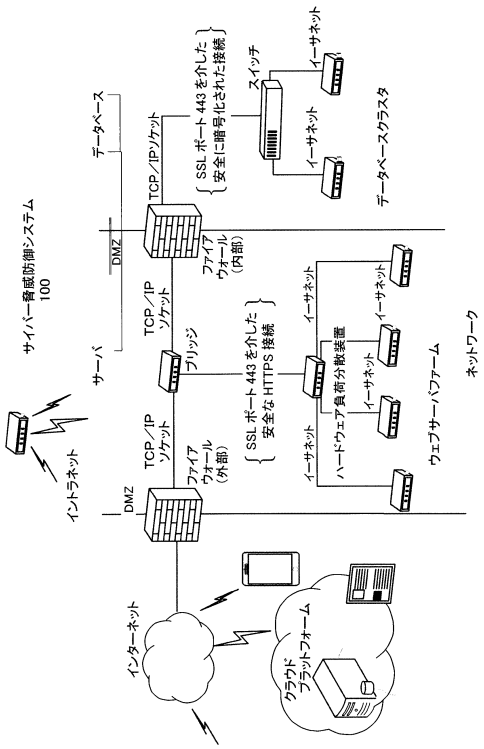
先述の設計およびその実施形態は、かなり詳細に提供されているが、本明細書に提供される設計および実施形態が制限されることは出願者の意図ではない。追加の適合および／または集成が可能であり、また、幅広い態様において、これらの適合および／または集成も包含される。したがって、以下の特許請求の範囲によって生じた範囲から逸脱することなく、先述の設計および実施形態が準備され得、この範囲は、適切に解釈されるときには特許請求の範囲によってのみ制限される。

【図面】

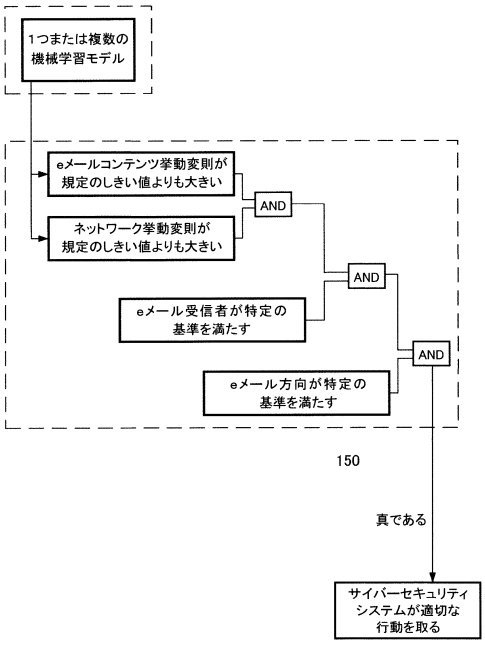
【図１】


サイバー脅威防御システム
100
トリガモジュール
収集モジュール
ネットワークモジュール
eメール
モジュール
ネットワークおよびeメール
コーディネータモジュール
比較を用いたサイバー
脅威モジュール
ユーザインターフェース
および表示モジュール
自律応答モジュール
データストア
AIモデル
AIモデル
eメール自体の特徴
およびその関連データ
AIモデル
潜在的なサイバー脅威
AIモデル
正常な生活パターン
AIモデル
正常な生活パターン

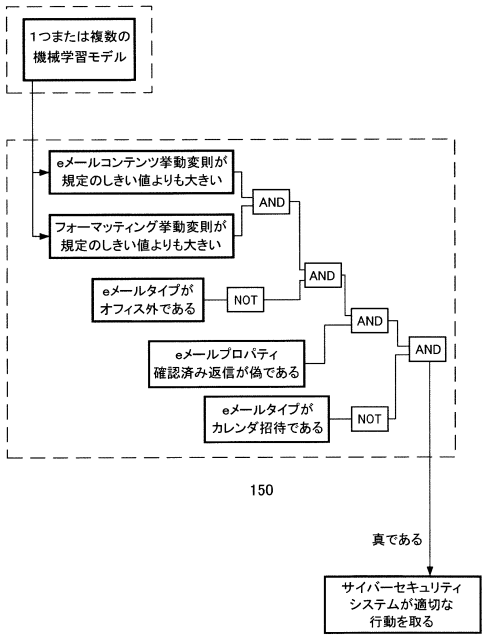
【図２】


サイバー脅威防御システム
100
サーバ
データベース
TCP／IPソケット
SSL ポート 443 を介した
安全に暗号化された接続
スイッチ
イーサネット
イーサネット
データベースクラスタ
DMZ
ファイア
ウォール
（内部）
TCP／IP
ソケット
ブリッジ
SSL ポート 443 を介した
安全な HTTPS 接続
イーサネット
イーサネット
イーサネット
ハードウェア真贋分散装置
ウェブサーバファーム
ネットワーク
イントラネット
TCP／IP
ソケット
ファイア
ウォール
（外部）
DMZ
インターネット
クラウド
プラットフォーム

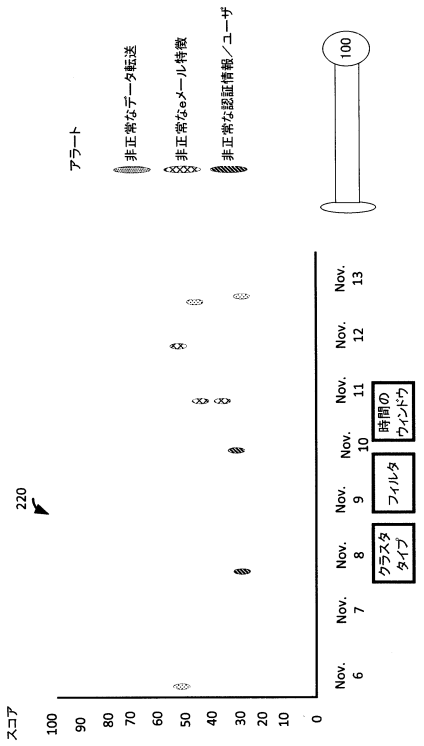
【図３】


1つまたは複数の
機械学習モデル
eメールコンテンツ挙動変則が
規定のしきい値よりも大きい
ネットワーク挙動変則が
規定のしきい値よりも大きい
AND
AND
eメール受信者が特定の
基準を満たす
AND
eメール方向が特定の
基準を満たす
150
真である
サイバーセキュリティ
システムが適切な
行動を取る

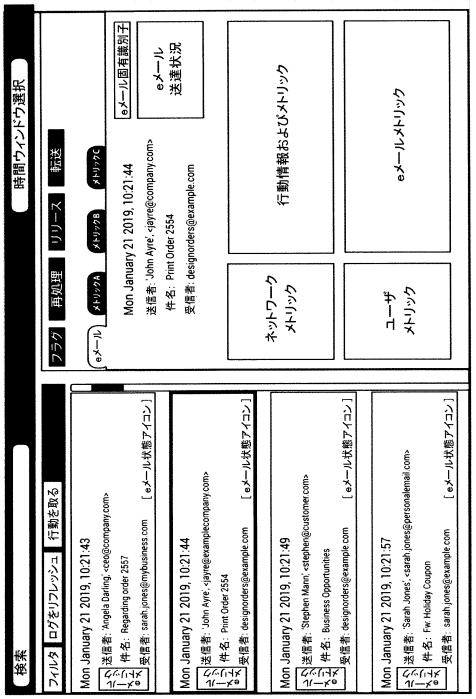
【図４】


1つまたは複数の
機械学習モデル
eメールコンテンツ挙動変則が
規定のしきい値よりも大きい
フォーマッティング挙動変則が
規定のしきい値よりも大きい
AND
eメールタイプが
オフィス外である
NOT
AND
eメールプロパティ
確認済み返信が偽である
AND
AND
eメールタイプが
カレンダ招待である
NOT
150
真である
サイバーセキュリティ
システムが適切な
行動を取る

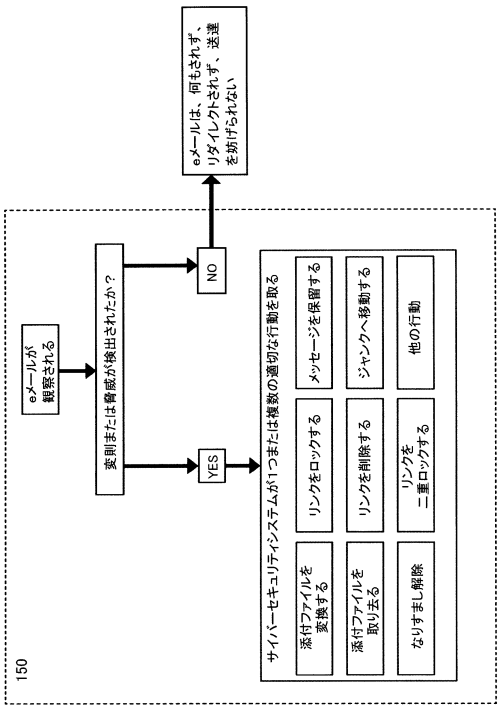
【図５】


アラート
非正常なデータ転送
非正常なeメール特徴
非正常な認証情報／ユーザ
スコア
220
100
90
80
70
60
50
40
30
20
10
0
Nov. 6
Nov. 7
Nov. 8
Nov. 9
Nov. 10
Nov. 11
Nov. 12
Nov. 13
クラスタタイプ
フィルタ
時間のウィンドウ

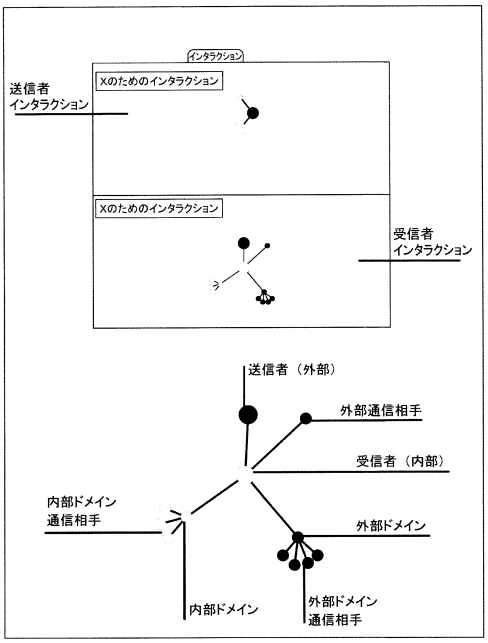
【図６】


検索
時間ウィンドウ選択
フィルタ
ログをリフレッシュ
行動を取る
フラグ
再処理
リリース
転送
eメール
メトリックA
メトリックB
メトリックC
eメール固有識別子
eメール送達状況
ネットワークメトリック
ユーザメトリック
行動情報およびメトリック
eメールメトリック

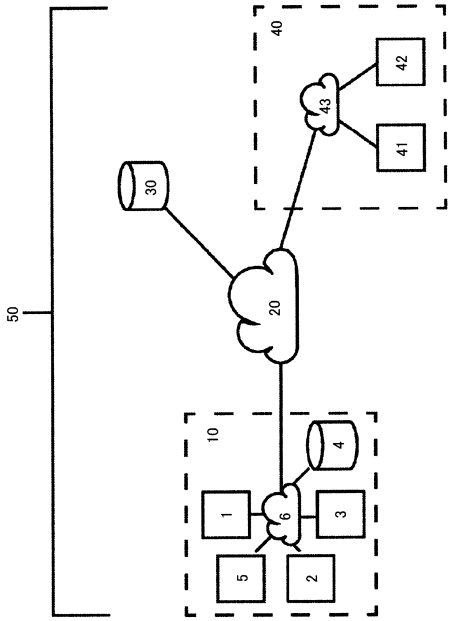
【図７】


150
eメールが観察される
変則または脅威が検出されたか？
YES
NO
eメールは、何もされず、リダイレクトされず、送達を妨げられない
サイバーセキュリティシステムが1つまたは複数の適切な行動を取る
添付ファイルを変換する
リンクをロックする
メッセージを保留する
他の行動
添付ファイルを取り去る
リンクを削除する
ジャンクへ移動する
なりすまし解除
リンクを二重ロックする

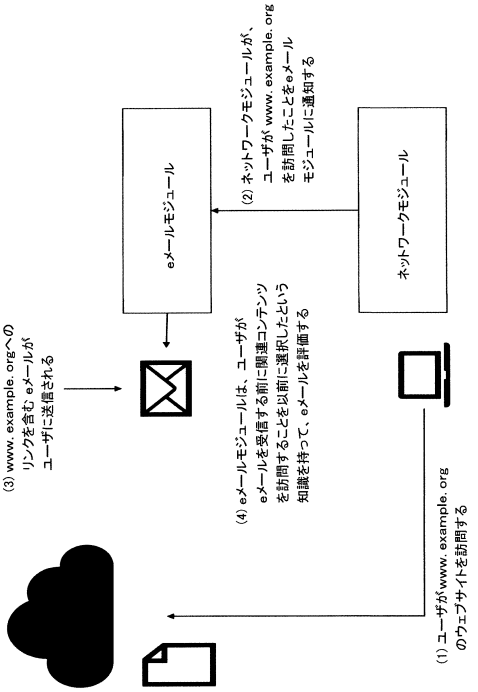
【図８】


インタラクション
送信者インタラクション
Xのためのインタラクション
Xのためのインタラクション
受信者インタラクション
送信者（外部）
外部通信相手
受信者（内部）
内部ドメイン通信相手
外部ドメイン
内部ドメイン
外部ドメイン通信相手

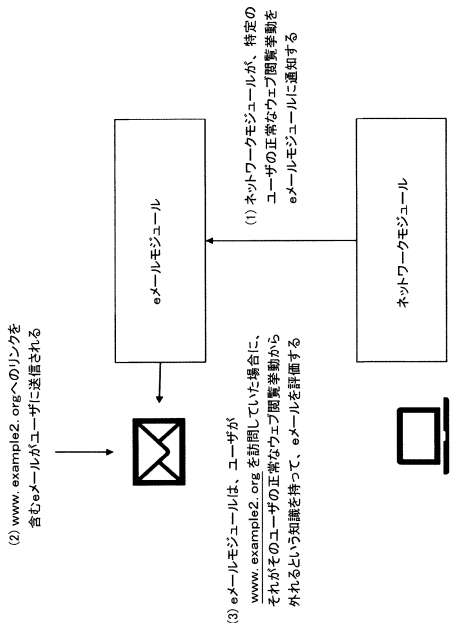
【図９】


50
30
20
40
43
42
41
10
4
1
6
3
5
2

【図１０】


eメールモジュール
ネットワークモジュール
(2) ネットワークモジュールが、
ユーザが www. example. org
を訪問したことをeメール
モジュールに通知する
(3) www. example. orgへの
リンクを含む eメールが
ユーザに送信される
(4) eメールモジュールは、ユーザが
eメールを受信する前に関連コンテンツ
を訪問することを以前に選択したという
知識を持って、eメールを評価する
(1) ユーザが www. example. org
のウェブサイトを訪問する

【図１１】


eメールモジュール
ネットワークモジュール
(1) ネットワークモジュールが、特定の
ユーザの正常なウェブ閲覧挙動を
eメールモジュールに通知する
(2) www. example2. orgへのリンクを
含むeメールがユーザに送信される
(3) eメールモジュールは、ユーザが
www. example2. org を訪問していた場合に、
それがそのユーザの正常なウェブ閲覧挙動から
外れるという知識を持って、eメールを評価する

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
(72)発明者 マシュー ファーガソン
イギリス， ＰＥ２９ １ＳＤ， ハンティンドン， エセックス ロード ５５
(72)発明者 マシュー シャーウィン
イギリス， ＣＢ５ ８ＤＳ， ケンブリッジ， オークランド ロード， オークランド コート フラット５９
合議体
審判長 須田 勝巳
審判官 大塚 俊範
審判官 吉田 美彦
(56)参考文献 米国特許第８５６６９３８（ＵＳ，Ｂ１）
(58)調査した分野 (Int.Cl.，ＤＢ名)
G06F 21/55
H04L 51/00
G06N 20/00