(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7223579号
(P7223579)

(45)発行日　令和5年2月16日(2023.2.16)

(24)登録日　令和5年2月8日(2023.2.8)

(51)国際特許分類
Ｇ０６Ｆ　21/57　(2013.01)
Ｇ０６Ｎ　3/04　(2023.01)

ＦＩ
Ｇ０６Ｆ　21/57　３７０
Ｇ０６Ｎ　3/04

請求項の数　10　外国語出願　（全20頁）

(21)出願番号　特願2019-1900(P2019-1900)
(22)出願日　平成31年1月9日(2019.1.9)
(65)公開番号　特開2019-145091(P2019-145091A)
(43)公開日　令和1年8月29日(2019.8.29)
審査請求日　令和4年1月6日(2022.1.6)
(31)優先権主張番号　15/870,275
(32)優先日　平成30年1月12日(2018.1.12)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　500520743
ザ・ボーイング・カンパニー
Ｔｈｅ　Ｂｏｅｉｎｇ　Ｃｏｍｐａｎｙ
アメリカ合衆国、６０６０６－１５９６　イリノイ州、シカゴ、ノース・リバーサイド・プラザ、１００
(74)代理人　110002077
園田・小林弁理士法人
(72)発明者　クレイグ， ジョン エー
アメリカ合衆国 ワシントン ９８１２４ ， シアトル， ピー．オー． ボックス ３７０７， シー／オー ザ ボーイング カンパニー
(72)発明者　ミード， ヤドランカ
アメリカ合衆国 ワシントン ９８１２４
最終頁に続く

(54)【発明の名称】　予測されるサイバー防御

(57)【特許請求の範囲】

【請求項１】

複数のネットワーク資産（２００）の予想されるサイバー防御のコンピュータにより実施される方法であって、

複数のサイバーインシデントレポート（３０２、９０２）を受領すること（１１０２）；

前記複数のサイバーインシデントレポートからキーワードを抽出すること（３００、１１０４）；

前記複数のネットワーク資産の少なくとも前記キーワード及び識別に浅層機械学習技術（４００、１１０６）を適用して、少なくとも第１の脅威シナリオに対して脆弱な前記ネットワーク資産の第１のサブセットの識別及び前記第１の脅威シナリオの識別を得ること；

前記第１の脅威シナリオに対して脆弱な前記ネットワーク資産の第１のサブセットの少なくとも前記識別、前記第１の脅威シナリオの前記識別、前記キーワード、及び前記複数のネットワーク資産の識別に、深層機械学習技術（６００、１１０８）を適用して、少なくとも第２の脅威シナリオに対して脆弱な前記ネットワーク資産の第２のサブセットの識別及び前記第２の脅威シナリオの識別を得ること；

前記複数のネットワーク資産及び前記第２の脅威シナリオをシミュレートして、少なくとも第３の脅威シナリオに対して脆弱な前記複数のネットワーク資産を通る少なくとも一つの経路を識別すること（７００、１１１０）；並びに

前記複数のネットワーク資産を通る前記少なくとも一つの経路の識別及び前記少なくとも第３の脅威シナリオの識別を出力すること（１１１２）

を含む、方法。
【請求項２】
少なくとも前記第３の脅威シナリオに対する改善策を取ることをさらに含む、請求項１に記載の方法。
【請求項３】
前記浅層機械学習技術が最近傍技術を含む、請求項１又は２に記載の方法。
【請求項４】
前記深層機械学習技術が、ニューラルネットワーク技術、相関ルールマイニング技術、又は語埋め込み技術を含む、請求項１から３のいずれか一項に記載の方法。
【請求項５】
前記シミュレートすることが離散事象シミュレーション（ＤＥＳ）エンジン（７０４）により実施される、請求項１から４のいずれか一項に記載の方法。
【請求項６】
前記シミュレートすることにより識別される多くの経路を制限することをさらに含む、請求項１から５のいずれか一項に記載の方法。
【請求項７】
前記複数のサイバーインシデントレポートからキーワードを抽出することが、前記複数のサイバーインシデントレポートから、少なくとも一つの履歴異常のデータベースから、少なくとも一つの脅威シナリオデータベースから、且つ資産データベースからキーワードを抽出することをさらに含む、請求項１から６のいずれか一項に記載の方法。
【請求項８】
複数のネットワーク資産（２００）の予測されるサイバー防御のためのシステム（１２００）であって、
複数のサイバーインシデントレポート（３０２、９０２）を受領すること（１１０２）；
前記複数のサイバーインシデントレポートからキーワードを抽出すること（３００、１１０４）；
前記複数のネットワーク資産の少なくとも前記キーワード及び識別に浅層機械学習技術（４００、１１０６）を適用して、少なくとも第１の脅威シナリオに対して脆弱な前記ネットワーク資産の第１のサブセットの識別及び前記第１の脅威シナリオの識別を得ること；
前記第１の脅威シナリオに対して脆弱な前記ネットワーク資産の第１のサブセットの少なくとも前記識別、前記第１の脅威シナリオの前記識別、前記キーワード、及び前記複数のネットワーク資産の識別に、深層機械学習技術（６００、１１０８）を適用して、少なくとも第２の脅威シナリオに対して脆弱な前記ネットワーク資産の第２のサブセットの識別及び前記第２の脅威シナリオの識別を得ること；
前記複数のネットワーク資産及び前記第２の脅威シナリオをシミュレートして、少なくとも第３の脅威シナリオに対して脆弱な前記複数のネットワーク資産を通る少なくとも一つの経路を識別すること（７００、１１１０）；並びに
前記複数のネットワーク資産を通る前記少なくとも一つの経路の識別及び前記少なくとも第３の脅威シナリオの識別を出力すること（１１１２）
を実施するよう構成された少なくとも一つの電子プロセッサを含む、システム（１２００）。
【請求項９】
前記少なくとも一つの電子プロセッサが、少なくとも前記第３の脅威シナリオに対する改善策を取るようさらに構成されている、請求項８に記載のシステム。
【請求項１０】
前記浅層機械学習技術が最近傍技術を含む、請求項８又は９に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、概して、サイバーセキュリティの脅威を予測し、対処することに関する。

【背景技術】
【０００２】
サイバーセキュリティの脅威並びに侵入検出及び軽減の分野は飛躍的に成長しており、政府、産業界、犯罪者及びカジュアルなサイバー攻撃元の世界のエネルギー、創造性及びリソースに高度で持続的な脅威は存在する。検出、分析及び対応に依拠する従来の防御は、毎日遭遇する脅威の襲来においては不十分である。非犯罪的な世界は、われわれの制度に信任と信頼を取り戻すには、議論、合意及び法学に依存しており、動きが遅い。このペースは、われわれの情報システムの、妨害されず且つ制御できない攻撃元のハイパーソニックな速度と比較して、異様に遅い。
【０００３】
今日、サイバー攻撃の被害者は通常、攻撃が発見されてから１４～３０日以内に、根本原因の分析に続いて、攻撃を報告している。初期のインシデントの通知を提出するスケジュールは、機関や民間産業によって異なり、変更されるが、現在、政府及び民間部門の一部は、初期のインシデントが検出されてから１時間以内にそのようなインシデントを報告する義務がある。初期のインシデントレポートには、検証されていない非常にわずかなレベルの情報が含まれていることがある。これらのレポートは、新しい情報が利用可能になるにつれて迅速に更新される必要があることがある。
【０００４】
２４時間の報告制限を遵守するためには、さまざまな方法及びシステムが整備されていなければならない。これは、特定のシステムに警戒態勢を取らせ、且つ／又は自身のインフラストラクチャ若しくは製品に対する同じ若しくは同じ種類の攻撃を防ぐことを目的として、わずかではあるが即時の情報を利用するために必要である。
【発明の概要】
【０００５】
さまざまな実施形態によれば、複数のネットワーク資産の予測できるサイバー防御のコンピュータにより実施される方法が開示される。本方法は、複数のサイバーインシデントレポートを受領すること；複数のサイバーインシデントレポートからキーワードを抽出すること；少なくとも複数のネットワーク資産のキーワード及び識別に浅層機械学習技術を適用して、少なくとも第１の脅威シナリオに対して脆弱なネットワーク資産の第１のサブセットの識別と第１の脅威シナリオの識別とを取得すること；少なくとも第１の脅威シナリオに対して脆弱なネットワーク資産の第１のサブセットの識別、第１の脅威シナリオの識別、キーワード、及び複数のネットワーク資産の識別に深層機械学習技術を適用して、少なくとも第２の脅威に対して脆弱なネットワーク資産の第２のサブセットの識別と第２の脅威シナリオの識別とを取得すること；複数のネットワーク資産及び第２の脅威シナリオをシミュレートして、少なくとも第３の脅威シナリオに対して脆弱な複数のネットワーク資産を通る少なくとも一つの経路を識別すること；並びに複数のネットワーク資産を通る少なくとも一つの経路の識別及び少なくとも第３の脅威シナリオの識別を出力することを含む。
【０００６】
上述の実施形態の様々なオプションの特徴には、以下が含まれる。本方法は、複数のネットワーク資産を通る少なくとも一つの経路の識別及び少なくとも第３の脅威シナリオの識別を複数のサイバーインシデントレポートに追加すること；抽出を繰り返し、浅層機械学習技術を適用し、深層機械学習技術を適用し、且つ少なくとも第４の脅威シナリオに対して脆弱な複数のネットワーク資産を通る少なくとも第２の経路を識別することを少なくとも一度はシミュレートすること；並びに複数のネットワーク資産を通る少なくとも第２の経路の識別及び少なくとも第４の脅威シナリオの識別を出力することを含み得る。本方法は、少なくとも第３の脅威シナリオに対する改善策を取ることを含み得る。改善策は、少なくとも一つのセキュリティ対策を講じること、少なくとも一つのポートを閉じること、少なくとも一つの資産を止めること、又は少なくとも一つの資産を断絶することの少なくとも一つを含み得る。浅層機械学習技術は、最近傍技術を含み得る。深層機械学習技術

は、ニューラルネットワーク技術、相関ルールマイニング技術、又は語埋め込み技術を含み得る。シミュレーションは、離散事象シミュレーション（ＤＥＳ）エンジンによって実施することができる。本方法は、シミュレーションにより識別される多くの経路を制限することを含み得る。制限には、シミュレーションにより識別される多くの経路を取り除くこと、又は深層機械学習技術における数多くのレベルを制限することが含まれ得る。複数のサイバーインシデントレポートからキーワードを抽出することには、複数のサイバーインシデントレポートから、少なくとも一つの履歴異常のデータベースから、少なくとも一つの脅威シナリオデータベースから、且つ資産データベースからキーワードを抽出することがさらに含まれてもよい。

【０００７】

さまざまな実施形態によれば、複数のネットワーク資産の予測できるサイバー防御のためのシステムが開示される。本方法は、複数のサイバーインシデントレポートを受領すること；複数のサイバーインシデントレポートからキーワードを抽出すること；少なくとも複数のネットワーク資産のキーワード及び識別に浅層機械学習技術を適用して、少なくとも第１の脅威シナリオに対して脆弱なネットワーク資産の第１のサブセットの識別と第１の脅威シナリオの識別とを取得すること；少なくとも第１の脅威シナリオに対して脆弱なネットワーク資産の第１のサブセットの識別、第１の脅威シナリオの識別、キーワード、及び複数のネットワーク資産の識別に深層機械学習技術を適用して、少なくとも第２の脅威に対して脆弱なネットワーク資産の第２のサブセットの識別と第２の脅威シナリオの識別とを取得すること；複数のネットワーク資産及び第２の脅威シナリオをシミュレートして、少なくとも第３の脅威シナリオに対して脆弱な複数のネットワーク資産を通る少なくとも一つの経路を識別すること；並びに複数のネットワーク資産を通る少なくとも一つの経路の識別及び少なくとも第３の脅威シナリオの識別を出力することを実施するよう構成された少なくとも一つの電子プロセッサを含む。

【０００８】

上述の実施形態の様々なオプションの特徴には、以下が含まれる。少なくとも一つ電子プロセッサは、複数のネットワーク資産を通る少なくとも一つの経路の識別及び少なくとも第３の脅威シナリオの識別を複数のサイバーインシデントレポートに追加すること；抽出を繰り返し、浅層機械学習技術を適用し、深層機械学習技術を適用し、且つ少なくとも第４の脅威シナリオに対して脆弱な複数のネットワーク資産を通る少なくとも第２の経路を識別することを少なくとも一度はシミュレートすること；並びに複数のネットワーク資産を通る少なくとも第２の経路の識別及び少なくとも第４の脅威シナリオの識別を出力することを実施するようさらに構成されていてもよい。少なくとも一つの電子プロセッサは、少なくとも第３の脅威シナリオに対する改善策を取るようさらに構成されていてもよい。改善策は、少なくとも一つのセキュリティ対策を講じること、少なくとも一つのポートを閉じること、少なくとも一つの資産を止めること、又は少なくとも一つの資産を断絶することの少なくとも一つを含み得る。浅層機械学習技術は、最近傍技術を含み得る。深層機械学習技術は、ニューラルネットワーク技術、相関ルールマイニング技術、又は語埋め込み技術を含み得る。シミュレーションは、離散事象シミュレーション（ＤＥＳ）エンジンによって実施することができる。少なくとも一つの電子プロセッサは、シミュレーションにより識別される多くの経路を制限するようさらに構成されていてもよい。制限には、シミュレーションにより識別される多くの経路を取り除くこと、又は深層機械学習技術における数多くのレベルを制限することが含まれ得る。複数のサイバーインシデントレポートからキーワードを抽出することには、複数のサイバーインシデントレポートから、少なくとも一つの歴史上異例のデータベースから、少なくとも一つの脅威シナリオデータベースから、且つ資産データベースからキーワードを抽出することがさらに含まれてもよい。

【０００９】

実施例は、以下の詳細な説明を参照し、添付の図面と関連性を考慮することによって、より深く理解されるため、実施例の様々な特徴が更に十分に評価されうる。

【図面の簡単な説明】

【００１０】
【図１】様々な実施形態によるシステムの概略図である。
【図２】様々な実施形態によるシステム出力の概略図である。
【図３】様々な実施形態による情報抽出サブシステムのハイブリッド図である。
【図４】様々な実施形態による浅層機械学習サブシステムのハイブリッド図である。
【図５】様々な実施形態による拡張フィードバックループのハイブリッド図である。
【図６】様々な実施形態による深層機械学習サブシステムのハイブリッド図である。
【図７】様々な実施形態による離散事象シミュレーションサブシステムのハイブリッド図である。
【図８】様々な実施形態によるプルーニングループの第１のハイブリッド図である。
【図９】様々な実施例によるプルーニングループの第２のハイブリッド図を示す。
【図１０】様々な実施例によるプルーニングループの第２のハイブリッド図を示す。
【図１１】様々な実施形態による方法のフロー図である。
【図１２】様々な実施形態による例示的なハードウェア実装の概略図である。
【発明を実施するための形態】
【００１１】
添付図面に示す開示される実施例に、以下で詳しく言及していく。可能な場合には、同一の又は類似した部品を参照するために、図面全体を通して同一の参照番号が使用される。以下の説明において、添付図面を参照するが、添付図面は本明細書の一部を形成するものであり、特定の実施例の形で示される。これらの実施例は、当業者がそれらを実施することができるよう十分に詳細に記載されており、他の実施例が利用可能であること、本発明の範囲から逸脱せずに、変更を加えうることが理解されるであろう。したがって、以下の説明は単なる例示にすぎない。
【００１２】
連邦情報セキュリティ管理法に基づく特定の政策下では、いくつかの団体は、検出から２４時間以内にサイバー攻撃を公に報告する必要がある。そのような政策は、初期の通知を迅速に処理するために、原因分析がインシデント処理プロセスの最終段階へ移されることを必要とする。「キャッチ」は、シグネチャの更新、又は部分的若しくは全体的な原因分析（例えば、どこから攻撃が発生したか）を待っている場合、以前と同じくらい企業が脆弱であることである。これらは、初期のインシデントの通知では利用することができないと予測されている。いくつかの実施形態は、一ヶ月早く、そしておそらくは同じタイプの攻撃が自身のインフラストラクチャに対して行われる前に機能する機会を提供する。よって、いくつかの実施形態は、情報が非常にわずかであっても、初期の早期通知要件への準拠を可能にする。
【００１３】
いくつかの実施形態は、入力として、一又は複数の初期インシデントレポートを受け入れ、サイバー脅威から保護するのに有用な様々な情報を出力する。いくつかの実施形態は、初期のインシデントレポートに記載されるものと同じ方法及び攻撃元によって潜在的に攻撃される可能性のある企業内のすべてのシステムを識別する。いくつかの実施形態は、初期のインシデントレポートに記載されているように、攻撃元がシステム侵害の同じレベル及び場所に到達するために取り得るすべての潜在的な経路を識別する。いくつかの実施形態は、潜在的に攻撃されるシステム及び潜在的な攻撃経路を初期のインシデントレポートを受領して７分以内に人間のユーザに知らせる。いくつかの実施形態は、攻撃についての利用可能な初期情報に基づいて、先行技術によれば、攻撃が発見されてから１４～３０日後から、攻撃が発見されてから約６８分（図１）まで、十分に２４時間の報告制限内で、脆弱性の窓を減少させる。いくつかの実施形態は、初期のインシデントレポートの更新である、新規の更新されたレポートが報告される度に、識別の工程を反復する。さらに、いくつかの実施形態は、可能性のあるサイバー攻撃ツリーの枝を、それが使われなくなるにつれてプルーニング、新しいリーフ、中間ノード、又はトップレベルのノードを、それらが更新されたインシデントレポートで識別されるようになるにつれて追加する。これら

及び他の実施形態を本明細書で詳細に記載する。

【００１４】

図１は、様々な実施形態によるシステム１００の概略図である。いくつかの実施形態は、相互接続した資産の標的となる企業のシステムへの潜在的な脅威を、同様の又は異なる産業セクターからの任意のわずかの初期のインシデントレポートに基づいて計算する。いくつかの実施形態は、離散事象シミュレーション（ＤＥＳ）プロセス又はエンジンによって定義され且つそれに基づきターゲットシステムの資産のそれぞれに対する攻撃の可能性に関連する。いくつかの実施形態は、必要に応じてターゲットシステムへの侵入地点を含む潜在的な攻撃経路を計算する。いくつかの実施形態は、さらなる対応のために上記の発見のいずれか、又はその組合せを人間のユーザに提示する。いくつかの実施形態は、自動的にさらなる対応を取る。さらなる対応には、例えば、人間のユーザに攻撃に対する心構えをさせること、ポート又はシステム部分を閉じること、潜在的な標的となる資産に対するさらなるセキュリティ対策及び他の対策を取ることが含まれ得る。

【００１５】

システム１００への入力１０２は、初期のインシデントレポートを含む。そのようなインシデントレポートは、インシデントが発生する（又は検出される）とすぐに、生成され、システム１００へ提供され得る。インシデントレポートは、産業共有メカニズム又は政府を通じて利用可能であり得る。インシデントレポートは、典型的には、コンピュータ可読テキストフォーマットである。様々な供給源は異なる方法及び分類を有するため、特定のフォーマット又は分類は想定されない。インシデントレポートには、ファイルシステムの侵害（例えば、ファイルの削除や暗号化等）、処理の減速、又はウェブサイトの改ざんのような異常挙動のトップレベルの観察が含まれ得る。インシデントレポートには、ファイルシステム若しくはデータベースの種類、オペレーティングシステムの種類若しくはバージョン、又はインターネットブラウザの種類若しくはバージョンなど、侵入先のコンピュータシステムに関する情報が含まれ得る。インシデントレポートは、コンピュータ可読であり得、非構造化（自然言語で表されたテキスト）情報を含み得る。インシデントレポートは、新情報で（例えば詳細が利用可能になるにつれて）迅速に（例えば毎時間）又はゆっくりと更新され得る。そのような新情報は、以下のいずれかであらゆる順序であってもよい：初期侵入点の種類（例えば、インターネット、内部）、攻撃元がどのようにアクセスしたか（例えば、パスワードクラッカー、パスワードが数か月前に盗まれたか）、実行可能ファイルの識別、メモリアクセスの識別、難読化技術、攻撃元のインターネットアドレス、又は新しいマルウェアのシグネチャ若しくは実行可能ファイル、そして最後に攻撃の詳細な説明。

【００１６】

入力１０２は、米国政府発行レポート、欧州連合発行レポート、米国コンピュータ緊急対応チーム（ＵＳ－ＣＥＲＴ）、米国原子力規制委員会（ＮＲＣ）、非公開リスト、金融セクターからのリスト、又は、例えば航空宇宙セクターからの、情報共有分析センター（ＩＳＡＣ）のいずれか、又は組合せをさらに含み得る。

【００１７】

入力１０２は、履歴異常情報を有するデータベース、脅威シナリオを有するデータベース、又はすべての（ユーザ）システム資産のデータベース、それらの直近（最近傍）の相互接続、並びにそれらのハードウェア及びソフトウェアバージョンのいずれか、又は組合せをさらに含み得る。そのような電子データベースは業界水準であり、それらの操作は業界標準である。

【００１８】

システム１００は情報抽出サブシステム１０４も含み、それは図３を参照して以下に詳述する。

【００１９】

システム１００はまた、二つの機械学習モデルを含む。処理工程中、システム１００は、例えば最近傍法又はいくつかの他の効率的なパターンマッチング法のバージョンの一つ

に基づく浅層機械学習サブシステム１０６と、例えば従来のニューラルネットワークの基づく深層機械学習サブシステム１０８とへのアクセスを有する。浅層機械学習サブシステム１０６は、図４及び５を参照して、以下に詳述する。深層機械学習サブシステム１０８は、図６を参照して、以下に詳述する。

【００２０】

システム１００は、離散事象シミュレーションサブシステム１１０も含む。離散事象シミュレーションサブシステム１１０は、図７を参照して、以下に詳述する。

【００２１】

システム１００は報告サブシステム１１２も含み、それは報告及び情報を出力する。報告及び情報は、以下のいずれか、又はそれらの組み合わせのテキスト表現及び／又は視覚表現を含むことができる：ターゲットシステムが侵入される可能性があるかどうか、例えば初期のインシデントレポートで利用可能な情報による判断、並びにこの事象に関連する可能性、侵入される可能性のある潜在的な資産のリスト、及びこれらの結果に関連する可能性、攻撃が企業のシステム及び資産を通過する可能性のある経路、及びそれらに関連する可能性、及び／又はシステムへの潜在的な侵入点、及びそれらに関連する可能性。さらに、報告及び情報には、過去の事象との類似性、事象の場所、脅威への対応、システムへの影響、脅威ベクトル、又は異常ツリーの視覚化（関連する可能性での決定ツリー及び根本原因分析）のいずれか、又はそれらの組み合わせが含まれることがある。

【００２２】

図１は例示的な現在のタイムライン１１４及び例示的な新タイムライン１１６も含むことに留意されたい。示されているように、例示的な現在のタイムラインは根本原因の分析への到達には典型的には３０日以上かかることを示す。この時のみ、攻撃シグネチャが生成され、業界に配布されて脅威防止プロセスが開始される。いくつかの実施形態によれば初期のインシデント通知は約１時間かかることがあり、情報抽出サブシステム１０４による処理はごくわずかな時間のみかかることがあり、浅層機械学習サブシステムによる処理は約１分間かかることがあり、深層機械学習サブシステム１０８による処理は約１分かかることがあり、離散事象シミュレーションサブシステム１１０による処理は約５分間かかることがあり、脅威防止に関連するレポート又は他の情報の出力は約１分間かかることがあり、この時点で業界は脅威防止プロセスを開始することができることを、例示的な新タイムライン１１６は示している。したがって、いくつかの実施形態は、既存の技術に対して大きな改善を示す。

【００２３】

図２は、様々な実施形態によるシステム出力の概略図である。ターゲットシステム２００は、（場合によっては）例えば飛行機、データベース、空港、ウェブサービス、エンドユーザ装置、無線及び有線接続、電子メールサービス等の相互接続資産を含む。いくつかの実施形態の出力は、以下のいずれか又は組合せを含むことができる。

・ターゲットシステムが同一又は類似する攻撃に屈することがある可能性、Ｐ（システム）２０２；
・資産が同一又は類似する攻撃に屈することがある可能性、Ｐ（資産）２０４；
・異なる資産間の接続経路が同一又は類似する攻撃に屈することがある可能性、Ｐ（経路）２０６；又は
・システムへの侵入点が同一又は類似する攻撃に屈することがある可能性、Ｐ（侵入）２０８。

【００２４】

図３は、様々な実施形態による情報抽出サブシステム３００のハイブリッド図である。情報抽出サブシステムの目的は、初期のインシデントレポートから重要な概念及びキーワードを抽出することである。初期のインシデントレポートは、異常が検出された場合のオペレータのシステムの外部挙動の観察についてのテキストによる説明を含む。それは、異常に挙動していると観察されている資産、及び場合によってはいくつかのさらなる観察情報に関する説明を含み得る。時間が経過するにつれて、初期のインシデントレポートは利

用可能になった時点でより多くの情報で更新される。
【００２５】
いくつかの実施形態は、ＮＩＳＴ ＳＰ ８００－６１ Ｒｅｖ ２のようにすべての初期のインシデントレポートがフォーマットに準拠することを必要としない（例えば、それはＥＵ又はＮＩＳＴガイドラインに従わない国で発生した可能性がある）。したがって、このサブシステムは、他のシステム構成要素により使用される情報を解析及び抽出するために機能する。
【００２６】
図３に示されるように、情報抽出サブシステム３００への入力は、任意のソースから且つ任意のフォーマットの、構造化且つ未構造化の、広範な概念レベルの少なくとも一つの初期のインシデントレポート３０２を含む。そのような初期のインシデントレポートは、異常に挙動するシステムの説明を含み、異常挙動が明記されている（例えば、減速、漏洩等）。図３に示されるような初期のインシデントレポート３０２は、「Ｋｒａｃｋ」と呼ばれるＷＰＡ２に対する脆弱性の説明を含む。保護されるドメイン資産は、ドメインの分類中のＷＡＰ（ワイヤレスアクセスポイント）であり、それは、浅層クラスの機械学習技術に属する連関ルールマッピング機械学習技術をドメインの資産説明データベースに使用することにより得ることができる。
【００２７】
情報抽出サブシステム３００への入力は、保護される資産の説明も含む。情報抽出サブシステム３００は、例えば図１のシステム１００への入力１０２にあるような、全ての（ユーザ）システム資産、それらの直近相互接続、並びにそれらのハードウェア及びソフトウェアバージョンの電子データベースからそのような情報を得ることができる。
【００２８】
情報抽出エンジン３０４は、ドメイン（すなわち保護される資産のセット）用に構成及び特化され、ターゲット会社の資産の分類上でマッピングされた任意の標準化された抽出・加工・書き込み（ＥＴＬ）又は情報抽出ツール（ＩＥＴ）プロセスを利用することができる。これらのツールは、観察された異常挙動（所有権、情報、漏洩、データベース等）及び攻撃されたシステム／資産の種類（例えば、データベース管理システム（ＤＢＭＳ）バージョン）に関するキーワードを抽出する。そのようなツールは、事象の分類、及び場合によっては異常なサブイベントの既知の（サブ）シーケンスの一方若しくは両方、又は根本原因、侵入点、及び完全な脅威の軌跡を出力する。図３に示されるように、情報抽出エンジン３０４は、以下の抽出された用語３０６を初期のインシデントレポート３０２から抽出する：「ｗｐａ２」、「ワイヤレス」、「アクセスポイント」、「アンドロイドアプリ」及び「銀行業務アプリ」。
【００２９】
情報抽出サブシステム３００は、キーワードマッピングエンジン３０８も含み、それは、抽出された用語３０６を、入力として提供された保護される資産の説明へマッピングする。キーワードマッピングエンジン３０８は、出力として、抽出されたキーワードと保護される電子資産との間の電子的に表された関連付け３１０を提供する。
【００３０】
図４は、様々な実施形態による浅層機械学習サブシステム４００のハイブリッド図である。浅層機械学習サブシステム４００は、効率的なアルゴリズムを使用して、初期のインシデントレポートとターゲットシステムの説明、すなわち保護される資産の説明との間に高速の一致を導き出す。浅層機械学習サブシステム４００は、後述する図６の深層機械学習サブシステム６００の動作レベルである意味（意味）類似性とは対照的に、構文（テキスト）類似性のレベルで動作することができる。浅層機械学習サブシステムは、本質的には以下の二つの質問に回答する。一つ目は、「以前にこのようなことがわれわれに対して発生したか？」ということであり、二つ目は、「このようなことがわれわれに対して発生し得るか？」ということである。
【００３１】

浅層機械学習サブシステム４００への入力４０２は、図３の情報抽出サブシステム３００からのキーワード、資産、及び異常出力のリスト、並びに資産データベースを含む。資産データベースは、保護される資産の説明、それらの直近（例えば最近傍）の相互接続、並びにそれらのハードウェア及びソフトウェアバージョン、例えば図１のシステム１００への入力１０２など）を含み得る。入力４０２は、履歴異常データベース、及び脅威シナリオデータベースの一方又は両方からの情報をさらに含み得る。

【００３２】

複数の異なる機械学習パターンマッチング法は、浅層機械学習サブシステム４００に適している。例えば、連関ルールマッピングに加えて、ｋ近傍（ＫＮＮ）法が使用されてもよい。この方法は、最も簡潔な形態では予備トレーニングを必要としない。これは、「怠惰な」機械学習法のカテゴリに属する。「近傍」は、非限定的な例として、ハミング距離又はレーベンシュタイン距離などの様々な測定基準によって判断することができる。ＫＮＮ法は、資産データベース、脅威シナリオデータベース、及び履歴異常データベースに適用することができる（４０４）。特に、ＫＮＮ方法は、情報抽出サブシステム３００から出力された個々のキーワードに対して、そのような各データベース内の最近傍を見つけることによって適用することができる（４０４）。

【００３３】

浅層機械学習サブシステム４００の出力４０６は、以下の一又は複数を含む：

－　情報抽出サブシステム３００により識別される資産に最も近く一致する保護システム内で動作される資産（インシデントレポートにおいて、他の場所で現在攻撃を受けている資産に最も近く一致する保護システムの資産）の識別（例えばリスト）。

－　一又は複数のキーワードが、情報抽出サブシステム３００によって出力されたキーワードに対する保護資産の関連付け３１０と一致する、脅威シナリオ又は過去の異常の識別。

・一連の異常事象、根本原因、侵入点、脅威の軌跡等の、情報抽出サブシステム３００の任意の他の形態の出力についてのパターンマッチング。

－　例えば保守要員がラップトップを航空機のシステム又はワイヤレスアクセスポイントに接続するときに、サブシステム３００及びサブシステム４００によって導き出された概念を含む、異常挙動の最も重要な要因の視覚的表現。

－　将来的な参照及び／又は分析のための更新。

【００３４】

出力４０６は、例えば、人間のユーザのために視覚的表現にフォーマットされることにより、又は図５を参照して以下に示され且つ説明されるようなフィードバックループに提供されることにより、さらに処理され得る（４０８）。

【００３５】

浅層機械学習サブシステム４００によって処理される例として、新たな候補（例えば、図４に図示されるようなＷＡＰ、ワイヤレスアクセスポイント）が、名詞、語句及びシステム資産を表す他の用語の制御された語彙に対して試験されると、出力４０６として、類似性測定基準に応じて、最近傍はＷＡＰ　ＡＦＴ及びＷＡＰ　ＦＷＤ等であることが決定される。

【００３６】

図５は、様々な実施形態による拡張フィードバックループ５００のハイブリッド図である。拡張フィードバックループ５００は、図４の浅層機械学習サブシステム４００の出力４０６の情報を入力４０２として浅層機械学習サブシステム４００に戻すことによって追加の情報を生成する。フィードバックループ５００を使用しないと、図４に示すように履歴異常データベース内の情報と何も一致しなかったのに対し、フィードバックループ５００を使用すると、図５に示すように、一致する履歴異常が出力４０６で識別される。図４に示すように、入力４０２は、ＷＡＰ　ＡＦＴ」及び「ＷＡＰ　ＦＷＤ」の識別を含む。これらは、航空機のそれらの場所によって命名された、この例におけるワイヤレスアクセスポイントの実例である。

【００３７】
図６は、様々な実施形態による深い機械学習サブシステム６００のハイブリッド図である。深層機械学習サブシステム６００は、構文の類似性のレベルについてのみ機能する浅層パターンマッチングシステムが発見できない可能性がある一致を識別するために使用される。深層機械学習技術によって検出された一致は、機内エンターテインメントシステムの異なる種類のアプリケーション、又はクレジットカードを使用して銀行業務アプリケーションと特徴を共有するという事実など、様々な概念レベルの関連付けである。浅層機械学習技術が、距離測定基準に基づいてテキストマイニング及び類似性検索を利用することができるのに対して、深層法は、代わりに、事実、実体及び他の情報間の関係に焦点を当てる。よって、深層機械学習サブシステム６００は、図３の情報抽出サブシステム３００から抽出されたキーワードの制限されたリストからより高いレベルの概念を導き出し、それらを使用して、より高い（より広い）レベルですべての履歴データベース、脅威シナリオデータベース及び資産データベースとパターンマッチングする。深層機械学習サブシステム６００は以下の質問に回答する。この脅威は潜在的にわれわれの資産に当てはまるか、そしてわれわれの環境ではそれはどのように見えるか？ということである。

【００３８】
深層機械学習サブシステム６００は、初期のインシデントレポートの仕様書が包括的でなく、この特徴を欠いたシステムが、用語、又は識別された攻撃指標の広さ若しくは深さのいずれかにおいて包括的ではなく、且つそれらのシステムが構文的に一致する可能性がないため、いくつかの実施形態で使用される。初期のレポートで言及される特定の特徴は、初期のインシデントレポートで言及されるものに関連するより高い又はより低いレベルの概念の両方が含まれない場合、それら自体のシステム内で、可能性のある攻撃のいくつかの重要な指標を見落とすことがある。深層機械学習サブシステム６００は、均一に適用又は適合されたオントロジーを必要としない。むしろ、オントロジーに依存しない。これは、適合させることができる形式主義は容認されないが、実施形態は攻撃を予想する機会を見逃してはならないためである。

【００３９】
深層機械学習サブシステムは、入力６０２として、情報抽出サブシステム３００からのすべての出力及び浅層機械学習サブシステム４００からのすべての出力を容認する。深層機械学習サブシステム６００は、入力６０２として、履歴異常情報を有するデータベース、脅威シナリオを有するデータベース、又はすべての（ユーザ）システム資産のデータベース、それらの直近（最近傍）の相互接続、並びにそれらのハードウェア及びソフトウェアバージョンのいずれか、又はそれらの組合せからの情報も容認する。

【００４０】
深層機械学習サブシステム６００は、非制限的な例として、実体関係モデリング（すなわち実体間の学習関係）、又はリンク及び連関分析を含む様々な深層学習技術を実行し得る。連関ルールマッピング（アプリオリアルゴリズム）、単語埋め込み、及びニューラルネットワーク（例えば畳み込みニューラルネットワーク）が特に適している。よって、深層機械学習技術は、資産データベース、脅威シナリオデータベース、及び履歴異常データベースに適用することができる（６０４）。

【００４１】
これらのツールは、初期のインシデントレポートから抽出キーワードからより高いレベルの概念を作り出す。例えば、初期のインシデントレポートが「ルータ」を列挙する場合、この用語は、すべてのボーダールータ、内部ルータ、ボーダーゲートウェイプロトコル（ＢＧＰ）及びその他のプロトコルデバイス、スイッチ、そして最終的にはネットワークデバイスの調査をもたらし得る。潜在的には、ありとあらゆるこれらのコンピューティング、ネットワーキング、ストレージ等の資産は、後のフォレンジックで影響を受けることがある。

【００４２】
深層機械学習サブシステム６００の出力６０６は、本質的には浅層機械学習サブシステ

ム４００のものと同じ種類の出力であるが、より広くより深い到達度を有する。言い換えれば、深層機械学習サブシステム６００は、キーワードそのものではなく、キーワードが何を意味しているのかを識別する。

【００４３】

例えば、深層機械学習サブシステム６００は、用語「ＩＦＥシステム（「機内エンターテインメントシステム」）に適用されると、それに関連する機内ショッピングを含むすべての関連アプリケーションを出力６０６として導き出す。用語「機内ショッピング」は、出力６０６の別の部分である「クレジットカード」に大きく関連する。また、図６に示すように、「ＩＦＥシステム」と「ＷＡＰ　ＦＷＤ」との間の関連性が資産データベースから導き出されることにも留意されたい。潜在的なターゲットである、ＩＦＥ　ＦＷＤ及びＷＡＰ　ＡＦＴのどちらも、初期のインシデントレポートでは言及されなかったことにも留意されない。これらは、最終的な（先行技術の）脆弱性又はインシデント分析レポートで言及される可能性があるが、それは本開示の方法におけるこの工程から数週間後のことだろう。

【００４４】

いくつかの実施形態は、深層機械学習サブシステム６００で古典的な自然言語処理情報抽出法を使用し得る。ここでは「情報抽出」とは、プレーンテキストからの機械処理ができる構造化情報を抽出するための方法の集合（実体抽出、関係抽出、事象抽出等と命名される）を指す。企業又は他の資産のセットが、関連する、ラベル付けされた、資産のリスト及びそれらの関係を有する場合、古典的な方法での作業が好ましい。しかしながら、必要とされる情報を抽出するためのすべての必要とされる情報の、広範で、正確な、適切に維持された機械可読リポジトリは、実際に入手するのは困難である。適切にレベル付けされたデータセットの潜在的な欠損に加えて、ラベル付けの人的エラー及び情報のギャップが存在することがある。したがって、いくつかの実施形態は、監視なしの設定でニューラルネットワーク法を使用し得る。深層ニューラルネットワークにおけるいくつかの方法は、監視なしの方法において、神経言語プログラミングタスクのための深層学習を行い、利用可能なテキスト及びあらゆる種類のデータコーパスからそれらのデータ及びテキスト内に含有される事実及び関係についての知識を蓄積することによって学習する。したがって、いくつかの実施形態は、任意のテキストから直接関係句とともに事実を抽出するために、事前定義されたオントロジー又は関係クラスを必要としない既存の手法を使用する。

【００４５】

図７は、様々な実施形態による離散事象シミュレーションサブシステム７００のハイブリッド図である。離散事象シミュレーションサブシステム７００は、根本原因、脅威経路、及び保護されるシステムに対する潜在的なダメージを決定するために使用され得る。より詳細には、離散事象シミュレーションサブシステム７００は、保護資産のモデルを使用して、資産、事象、並びにキーワード及びより高いレベルの概念により識別されるその他のアーチファクトを含むシミュレートされたシステムを作り出す。離散事象シミュレーションサブシステム７００は、初期のインシデントレポートからの事象それ自体についての情報及び深層機械学習サブシステム６００の結果として追加されたものをきっかけにして動作する可能性のあるシステムを通して根本原因及び潜在的な経路を明らかにする。

【００４６】

離散事象シミュレーションサブシステム７００への入力７０２は、情報抽出サブシステム３００の出力（例えば関連付け３１０）、浅層機械学習サブシステム４００の出力４０６、及び深層機械学習サブシステム６００の出力６０６のいずれか、又はそれらの組み合わせを含む。

【００４７】

離散事象シミュレーションサブシステム７００は、離散事象シミュレーションエンジン７０４を含み、該エンジンは、入力７０２で離散事象シミュレーションを実行して、インプットからのキーワードのいずれか一つ又は組み合わせを含むわれわれの動作システムを通る全ての経路を、出力７０６として識別及び提供する。

【００４８】
よって、離散事象シミュレーションサブシステム７００は、考慮中の脅威又は類似する脅威が取る可能性のある保護下の資産を通る潜在的な攻撃経路、そのような攻撃の侵入点、及び動作システムへの影響を出力７０６として提供する。より具体的には、離散事象シミュレーションサブシステム７００は、以下の識別を出力７０６として提供する：侵入に対して脆弱な経路、侵入に対して脆弱な資産、侵入点、侵入に対して脆弱な全体的なシステム、及びこれらのいずれかの可能性。
【００４９】
図７を参照して上記に示され説明される技術は、識別される経路の過剰な拡散を潜在的に引き起こすことがある。実際、開示される技術の利点は、人間が解決困難なすべての経路及び経路の組み合わせを検討することができる点である。識別された経路の数を、重要な経路を維持するだけでなく、その技術が確実に収束するレベルに保つために考えられる２つの技術がある。第１のプルーニング技術は、深層機械学習サブシステム６００による概念生成の深さを制御することである。この技術は、多くのレベルの概念が深層機械学習サブシステム６００によってキーワードからどのように生成されるかを制限する。これは設定可能なシステムパラメータである。第１の技術は、システムの前方、「拡張」方向に適用されることに留意されたい。第２のプルーニング技術は、システムを通して、枝又は経路全体を切り取ることである。この技術は、図８及び９を参照して、以下に記載される。
【００５０】
図８は、様々な実施形態によるプルーニングループ８００の第１のハイブリッド図である。この技術は、後方「プルーニング」方向で使用され、ここでシステム１００は、その「リスニング」状態へ戻り、さらなる更新を待つ。より詳細な情報によって、システム１００は連続する工程に集中し、管理可能且つ人前に出せる状態になるであろう。一般に、プルーニングループ８００は、深層機械学習サブシステム６００による処理が終了した後、概念図８０６に図示されるように、任意の他の概念とは接続性を見出さないキーワードリスト８０２及び警戒リスト８０４中の全エントリを削除する。プルーニングループ８００の後、システムは、資産の現在の知識とともにＬＩＳＴＥＮ状態に定まり、ＷＡＰ　ＦＷＤ、ＩＦＥシステム及び機内ショッピングを警戒する。
【００５１】
図９は、様々な実施例によるプルーニングループの第２のハイブリッド図を示す。システム１００は、初期のインシデントレポート９０２から警戒する資産９０４へ移行した。ユーザへのディスプレイは、いくつかの実施形態による右側の箱と似ている。初期のインシデントレポート９０２中の構文のいずれも、警戒する資産９０４中の構文のいずれかと完全に一致しない。
【００５２】
図１１は、様々な実施形態による方法１１００のフロー図である。方法１０００は、例えば図１２を参照して示され且つ説明されるハードウェアを使用して、図１のシステム１００により実行され得る。
【００５３】
ブロック１１０２では、システム１００は、少なくとも一つの初期のインシデントレポートを受領する。レポートは、図１を参照して上に示され且つ説明されるようなものであり得る。初期のインシデントレポートは、電子固定記憶装置から且つ／又はインターネットのようなネットワーク上で受領され得る。
【００５４】
ブロック１１０４では、システム１００はキーワードを抽出する。キーワードは、図３を参照して上に示され且つ説明されるようなものであり得る。
【００５５】
ブロック１１０６では、システム１００は浅層機械学習技術を適用する。浅層機械学習技術は、図４を参照して上に示され且つ説明されるように適用され得る。
【００５６】

ブロック１１０８では、システム１００は深層機械学習技術を適用する。深層機械学習技術は、図６を参照して上に示され且つ説明されるように適用され得る。

【００５７】

ブロック１１１０では、システム１００は、資産が保護されることをシミュレートする。シミュレーションは、図７を参照して上に示され且つ説明されるように達成され得る。

【００５８】

ブロック１１１２では、システム１００は出力を提供する。出力は、人間のユーザ、又は別のコンピュータシステム、例えば改善策を自動的に実行するよう構成されているシステムへのものであり得る。改善策は、その出力に応じて自動的に人間のユーザによって開始されても、システム１００によって開始されても、少なくとも一つのセキュリティ対策を取ること、少なくとも一つのポートを閉じること、少なくとも一つの資産を止めること、又は少なくとも一つの資産を断絶することを含みみ得る。

【００５９】

図１２は、様々な実施形態による例示的なハードウェア実装の概略図である。プロセッサシステム１２００は、様々なコア構成（多数のコアを含む）及びクロック周波数の一又は複数のプロセッサ１２０２を含み得る。一又は複数のプロセッサ１２０２は、指示を実行する、論理を適用する等のために動作可能であり得る。これらの機能は、多数のプロセッサにより又は並行して且つ／若しくは通信可能に結合して動作する単一チップ上の多数のコアにより提供され得ることが認識されるであろう。少なくとも一つの実施形態では、一又は複数のプロセッサ１２０２は、一又は複数の図形処理ユニットであり得るか、又はそれを含み得る。

【００６０】

プロセッサシステム１２００は、画像、ファイル、及びプロセッサ１２０２によって実行されるプログラム命令などのデータを記憶するための、様々な物理的寸法、アクセス可能性、記憶容量等の一又は複数の記憶装置及び／又はコンピュータ可読媒体１２０４（例えばフラッシュドライブ、ハードドライブ、ディスク、ランダムアクセスメモリなど）であり得るか、又はそれらを含み得るメモリシステムも含み得る。一実施形態では、コンピュータ可読媒体１２０４は、プロセッサ１２０２によって実行されるときに、プロセッサシステム１２００に動作を実施させるよう構成されている指示を記憶し得る。例えば、そのような指示の実行は、プロセッサシステム１２００が本明細書に記載される方法の一又は複数の部分及び／又は実施形態を実施することを生じさせ得る。

【００６１】

プロセッサシステム１２００は、一又は複数のネットワークインターフェース１２０６もまた含んでいてよい。ネットワークインターフェース１２０６は、任意のハードウェアアプリケーション、及び／又は他のソフトウェアを含み得る。したがって、ネットワークインターフェース１２０６は、イーサネット、ワイヤレスイーサネット等のプロトコルを使用する有線又は無線媒体上での通信のためのイーサネットアダプタ、ワイヤレストランシーバ、周辺機器構成要素相互接続（ＰＣＩ）インターフェース、及び／又はシリアルネットワーク構成要素を含み得る。

【００６２】

プロセッサシステム１２００は、ディスプレイスクリーン、プロジェクタ、キーボード、マウス、タッチパッド、センサ、他の種類のインプット及び／又は出力周辺機器等との通信のための一又は複数の周辺機器インターフェース１２０８をさらに含み得る。いくつかの実装では、プロセッサシステム１２００のための構成要素は、単一のエンクロージャ中に囲われる必要はなく、あるいは互いに接近して配置される必要さえないが、他の実装では、構成要素及び／又は他のものは、単一のエンクロージャ中に提供され得る。

【００６３】

コンピュータ可読媒体１２０４は、又は複数の記憶デバイス１２０１０にデータを記憶するよう物理的又は論理的に配置又は構成され得る。記憶デバイス１２１０は、一又は複数の任意の適切なフォーマットのファイルシステム又はデータベースを含み得る。記憶デ

バイス１２１０は、一又は複数のソフトウェアプログラム１２１２も含んでよく、これは開示される方法の一又は複数を実施するための解釈可能又は実行可能な指示を含有してもよい。ソフトウェアプログラム１２１２の一又は複数、又はその一部は、プロセッサ１２０２により要求されるとき、プロセッサ１２０２による実行のために記憶デバイス１２１０からメモリデバイス１２０４へロードされ得る。

【００６４】

プロセッサシステム１２００は、開示されている実行形態を実施するために必要なあらゆる随伴ファームウェア又はソフトウェアを含む、任意の種類のハードウェア構成要素を含み得るため、上述の構成要素はハードウェア構成の一例にすぎないことを、当業者は認識するであろう。プロセッサシステム１２００は、部分的又は全体的に、特定用途向け集積回路（ＡＳＩＣ）やフィールドプログラマブルゲートアレイ（ＦＰＧＡ）といった、電子回路構成要素又はプロセッサによっても実装され得る。

【００６５】

さらに、本開示は、以下の条項による実施形態を含む。

【００６６】

条項１：複数のネットワーク資産の予測されるサイバー防御のコンピュータにより実施される方法であって、複数のサイバーインシデントレポートを受領すること；複数のサイバーインシデントレポートからキーワードを抽出すること；少なくとも複数のネットワーク資産のキーワード及び識別に浅層機械学習技術を適用して、少なくとも第１の脅威シナリオに対して脆弱なネットワーク資産の第１のサブセットの識別と第１の脅威シナリオの識別とを取得すること；少なくとも第１の脅威シナリオに対して脆弱なネットワーク資産の第１のサブセットの識別、第１の脅威シナリオの識別、キーワード、及び複数のネットワーク資産の識別に深層機械学習技術を適用して、少なくとも第２の脅威に対して脆弱なネットワーク資産の第２のサブセットの識別と第２の脅威シナリオの識別とを取得すること；複数のネットワーク資産及び第２の脅威シナリオをシミュレートして、少なくとも第３の脅威シナリオに対して脆弱な複数のネットワーク資産を通る少なくとも一つの経路を識別すること；並びに複数のネットワーク資産を通る少なくとも一つの経路の識別及び少なくとも第３の脅威シナリオの識別を出力することを含む、方法。

【００６７】

条項２：複数のネットワーク資産を通る少なくとも一つの経路の識別及び少なくとも第３の脅威シナリオの識別を複数のサイバーインシデントレポートに追加すること；抽出を繰り返し、浅層機械学習技術を適用し、深層機械学習技術を適用し、且つ少なくとも第４の脅威シナリオに対して脆弱な複数のネットワーク資産を通る少なくとも第２の経路を識別することを少なくとも一度はシミュレートすること；並びに複数のネットワーク資産を通る少なくとも第２の経路の識別及び少なくとも第４の脅威シナリオの識別を出力することをさらに含む、条項１に記載の方法。

【００６８】

条項３：少なくとも第３の脅威シナリオに対する改善策を取ることをさらに含む、条項１に記載の方法。

【００６９】

条項４：改善策が、少なくとも一つのセキュリティ対策を講じること、少なくとも一つのポートを閉じること、少なくとも一つの資産を止めること、又は少なくとも一つの資産を断絶することの少なくとも一つを含む、条項３に記載の方法。

【００７０】

条項５：浅層機械学習技術が最近傍技術を含む、条項１に記載の方法。

【００７１】

条項６：深層機械学習技術が、ニューラルネットワーク技術、相関ルールマイニング技術、又は語埋め込み技術を含む、条項１に記載の方法。

【００７２】

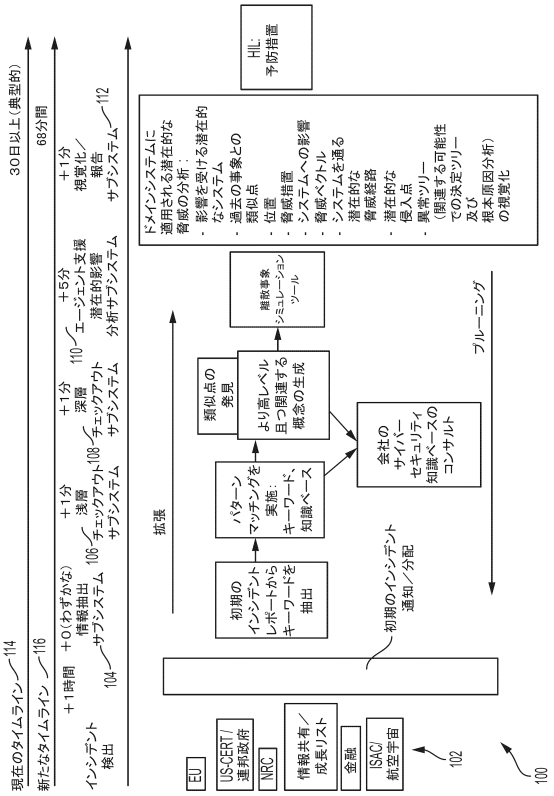
条項７：シミュレーションが離散事象シミュレーション（ＤＥＳ）エンジンにより実施

される、条項１に記載の方法。
【００７３】
条項８：シミュレーションにより識別される多くの経路を制限することをさらに含む、条項１に記載の方法。
【００７４】
条項９：制限が、シミュレーションにより識別される多くの経路を取り除くこと、又は深層機械学習技術における数多くのレベルを制限することを含む、条項８に記載の方法。
【００７５】
条項１０：複数のサイバーインシデントレポートからキーワードを抽出することが、複数のサイバーインシデントレポートから、少なくとも一つの履歴異常のデータベースから、少なくとも一つの脅威シナリオデータベースから、且つ資産データベースからキーワードを抽出することをさらに含む、条項１に記載の方法。
【００７６】
条項１１：複数のネットワーク資産の予測されるサイバー防御のためのシステムであって、複数のサイバーインシデントレポートを受領すること；複数のサイバーインシデントレポートからキーワードを抽出すること；少なくとも複数のネットワーク資産のキーワード及び識別に浅層機械学習技術を適用して、少なくとも第１の脅威シナリオに対して脆弱なネットワーク資産の第１のサブセットの識別と第１の脅威シナリオの識別とを取得すること；少なくとも第１の脅威シナリオに対して脆弱なネットワーク資産の第１のサブセットの識別、第１の脅威シナリオの識別、キーワード、及び複数のネットワーク資産の識別に深層機械学習技術を適用して、少なくとも第２の脅威に対して脆弱なネットワーク資産の第２のサブセットの識別と第２の脅威シナリオの識別とを取得すること；複数のネットワーク資産及び第２の脅威シナリオをシミュレートして、少なくとも第３の脅威シナリオに対して脆弱な複数のネットワーク資産を通る少なくとも一つの経路を識別すること；並びに複数のネットワーク資産を通る少なくとも一つの経路の識別及び少なくとも第３の脅威シナリオの識別を出力することを実施するよう構成された少なくとも一つの電子プロセッサを含む、システム。
【００７７】
条項１２：少なくとも一つ電子プロセッサが、複数のネットワーク資産を通る少なくとも一つの経路の識別及び少なくとも第３の脅威シナリオの識別を複数のサイバーインシデントレポートに追加すること；抽出を繰り返し、浅層機械学習技術を適用し、深層機械学習技術を適用し、且つ少なくとも第４の脅威シナリオに対して脆弱な複数のネットワーク資産を通る少なくとも第２の経路を識別することを少なくとも一度はシミュレートすること；並びに複数のネットワーク資産を通る少なくとも第２の経路の識別及び少なくとも第４の脅威シナリオの識別を出力することを実施するようさらに構成されている、条項１１に記載のシステム。
【００７８】
条項１３：少なくとも一つの電子プロセッサが、少なくとも第３の脅威シナリオに対する改善策を取るようさらに構成されている、条項１１に記載のシステム。
【００７９】
条項１４：改善策が、少なくとも一つのセキュリティ対策を講じること、少なくとも一つのポートを閉じること、少なくとも一つの資産を止めること、又は少なくとも一つの資産を断絶することの少なくとも一つを含む、条項１３に記載のシステム。
【００８０】
条項１５：浅層機械学習技術が最近傍技術を含む、条項１１に記載のシステム。
【００８１】
条項１６：深層機械学習技術が、ニューラルネットワーク技術、相関ルールマイニング技術、又は語埋め込み技術を含む、条項１１に記載のシステム。
【００８２】
条項１７：シミュレーションが離散事象シミュレーション（ＤＥＳ）エンジンにより実

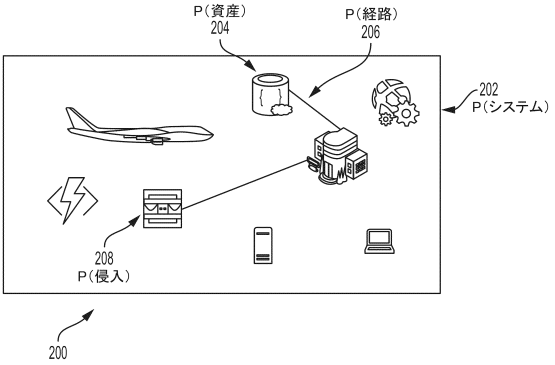
施される、条項１１に記載のシステム。
【００８３】
条項１８：少なくとも一つの電子プロセッサが、シミュレーションにより識別される多くの経路を制限するようさらに構成されている、条項１１に記載のシステム。
【００８４】
条項１９：少なくとも一つの電子プロセッサによる制限が、シミュレーションにより識別される多くの経路を取り除くこと、又は深層機械学習技術における数多くのレベルを制限することを含む、条項１８に記載のシステム。
【００８５】
条項２０：複数のサイバーインシデントレポートからキーワードを抽出することが、複数のサイバーインシデントレポートから、少なくとも一つの履歴異常のデータベースから、少なくとも一つの脅威シナリオデータベースから、且つ資産データベースからキーワードを抽出することをさらに含む、条項１１に記載のシステム。
【００８６】
上述のある実施例は、コンピュータアプリケーション又はプログラムを使用して部分的に実行されうる。コンピュータプログラムは、機能している場合も休止しているも、様々な形態で存在しうる。例えば、コンピュータプログラムは、ソースコード、オブジェクトコード、実行可能コード又は他の形式のプログラム命令、ファームウェアプログラム、又はハードウェア記述言語（ＨＤＬ）ファイルからなりうる、一又は複数のソフトウェアプログラム、ソフトウェアモジュール、又はその両方で存在しうる。上述のいずれかは、圧縮された形態又は非圧縮形態コンピュータ可読記憶デバイス及び媒体を含みうる、コンピュータ可読媒体上で具現化されうる。例示的なコンピュータ可読記憶デバイス及び媒体は、従来のコンピュータシステムのＲＡＭ（ランダムアクセスメモリ）、ＲＯＭ（読出し専用メモリ）、ＥＰＲＯＭ（消去可能なプログラマブルＲＯＭ）、ＥＥＰＲＯＭ（電気的に消去可能なプログラマブルＲＯＭ）、及び磁気ディスク又は磁気テープ或いは光ディスク又は光テープを含む。
【００８７】
当業者であれば、上述の実施例に対して、その理念及び範囲を逸脱することなく、様々な修正を行うことが可能であろう。本明細書で使用されている用語及び記述は、説明のみを目的としたもので、限定を意図していない。詳細には、方法は例によって説明されているが、この方法のステップは、例示とは異なる順序で、又は同時に、実施されうる。当業者には、これらの変形例及びその他の変形例は、以下の特許請求の範囲及びその均等物において規定される理念及び範囲に含まれることが可能であることが、認識されよう。

【図面】

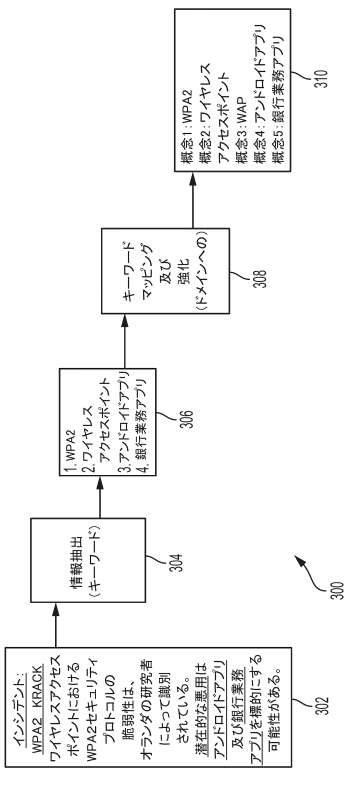
【図１】


現在のタイムライン 114
新たなタイムライン 116
＋1時間
＋0（わずかな）
インシデント検出
情報抽出 106
サブシステム 104
＋1分
浅層
チェックアウト 108
サブシステム
＋1分
深層
チェックアウト
サブシステム
110
＋5分
エージェント支援
潜在的影響
分析サブシステム
＋1分
視覚化／報告
サブシステム 112
30日以上（典型的）
68分間
ドメインシステムに適用される潜在的な脅威の分析：
・影響を受ける潜在的なシステム
・過去の事象との類似点
・位置
・脅威指標
・システムへの影響
・脅威ベクトル
・システムを通る潜在的な脅威経路
・潜在的な侵入点
・異常ツリー（関連する可能性での決定ツリー及び根本原因分析）の視覚化
HIL：予防措置
離散事象シミュレーションツール
より高レベル且つ関連する概念の生成
類似点の発見
パターンマッチングを実施：キーワード、知識ベース
会社のサイバーセキュリティ知識ベースのコンサルト
初期のインシデントレポートからキーワードを抽出
拡張
初期のインシデント通知／分配
ブルーニング
EU
US-CERT／連邦政府
NRC
情報共有／成長リスト
金融
ISAC／航空宇宙
102
100

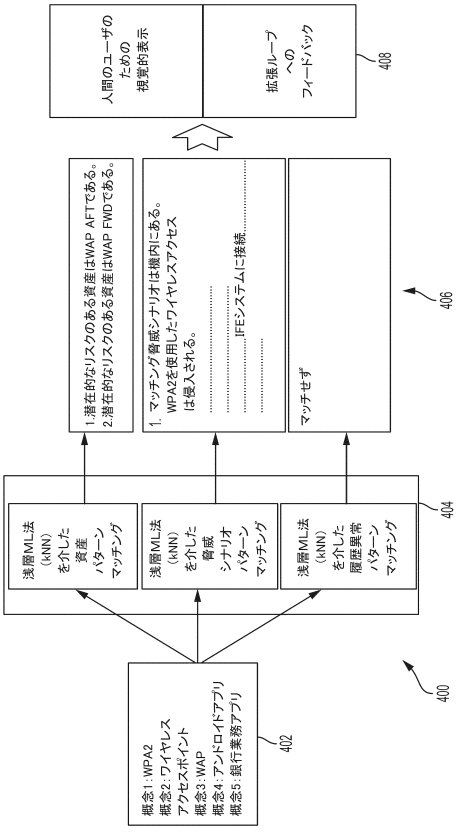
【図２】


P（資産）
204
P（経路）
206
202
P（システム）
208
P（侵入）
200

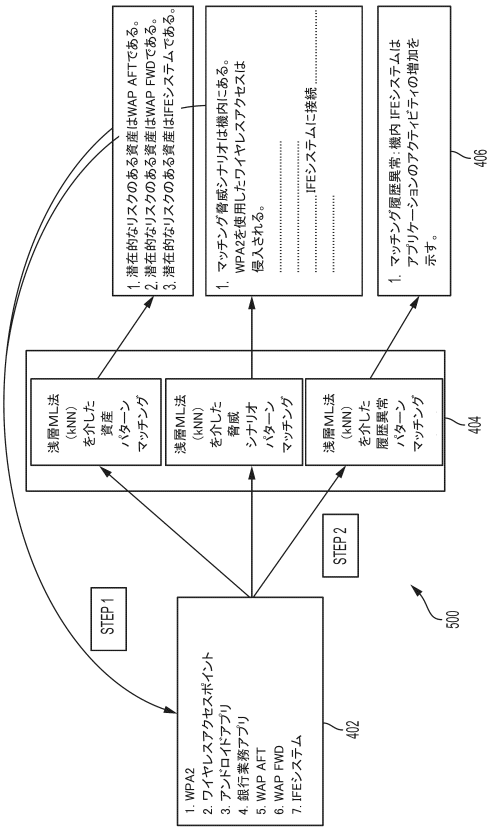
【図３】


インシデント：
WPA2 KRACK
ワイヤレスアクセスポイントにおけるWPA2セキュリティプロトコルの脆弱性は、オランダの研究者によって識別されている。潜在的な悪用はアンドロイドアプリ及び銀行業務アプリを標的にする可能性がある。
302
情報抽出（キーワード）
304
1. WPA2
2. ワイヤレスアクセスポイント
3. アンドロイドアプリ
4. 銀行業務アプリ
306
キーワードマッピング及び強化（ドメインへの）
308
概念1：WPA2
概念2：ワイヤレスアクセスポイント
概念3：WAP
概念4：アンドロイドアプリ
概念5：銀行業務アプリ
310
300

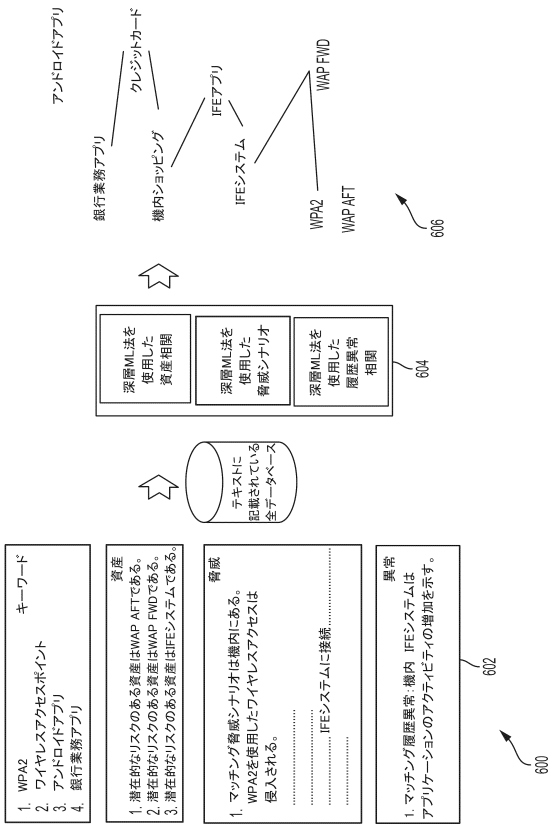
【図４】


人間のユーザのための視覚的表示
拡張ループへのフィードバック
408
1.潜在的なリスクのある資産はWAP AFTである。
2.潜在的なリスクのある資産はWAP FWDである。
1. マッチング脅威シナリオは機内にある。
WPA2を使用したワイヤレスアクセスは侵入される。
IFEシステムに接続
マッチせず
406
浅層ML法（kNN）を介した資産パターンマッチング
浅層ML法（kNN）を介した脅威シナリオパターンマッチング
浅層ML法（kNN）を介した履歴異常パターンマッチング
404
概念1：WPA2
概念2：ワイヤレスアクセスポイント
概念3：WAP
概念4：アンドロイドアプリ
概念5：銀行業務アプリ
402
400

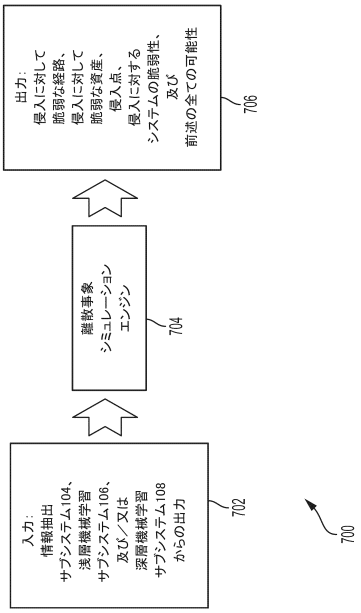
【図５】


1. WPA2
2. ワイヤレスアクセスポイント
3. アンドロイドアプリ
4. 銀行業務アプリ
5. WAP AFT
6. WAP FWD
7. IFEシステム
402
STEP 1
STEP 2
浅層ML法（kNN）を介した資産パターンマッチング
浅層ML法（kNN）を介した脅威シナリオパターンマッチング
浅層ML法（kNN）を介した履歴異常パターンマッチング
404
1. 潜在的なリスクのある資産はWAP AFTである。
2. 潜在的なリスクのある資産はWAP FWDである。
3. 潜在的なリスクのある資産はIFEシステムである。
1. マッチング脅威シナリオは機内にある。
WPA2を使用したワイヤレスアクセスは侵入される。
.....
.....IFEシステムに接続.....
.....
.....
1. マッチング履歴異常：機内 IFEシステムはアプリケーションのアクティビティの増加を示す。
406
500

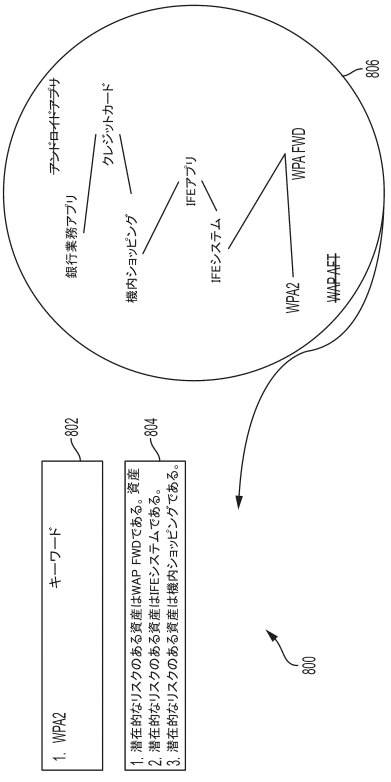
【図６】


アンドロイドアプリ
クレジットカード
銀行業務アプリ
機内ショッピング
IFEアプリ
IFEシステム
WAP FWD
WPA2
WAP AFT
606
深層ML法を使用した資産相関
深層ML法を使用した脅威シナリオ
深層ML法を使用した履歴異常相関
604
テキストに記載されている全データベース
1. WPA2
2. ワイヤレスアクセスポイント
3. アンドロイドアプリ
4. 銀行業務アプリ
キーワード
資産
1. 潜在的なリスクのある資産はWAP AFTである。
2. 潜在的なリスクのある資産はWAP FWDである。
3. 潜在的なリスクのある資産はIFEシステムである。
脅威
1. マッチング脅威シナリオは機内にある。
WPA2を使用したワイヤレスアクセスは侵入される。
.....
.....
.....IFEシステムに接続.....
.....
.....
異常
1. マッチング履歴異常：機内 IFEシステムはアプリケーションのアクティビティの増加を示す。
602
600

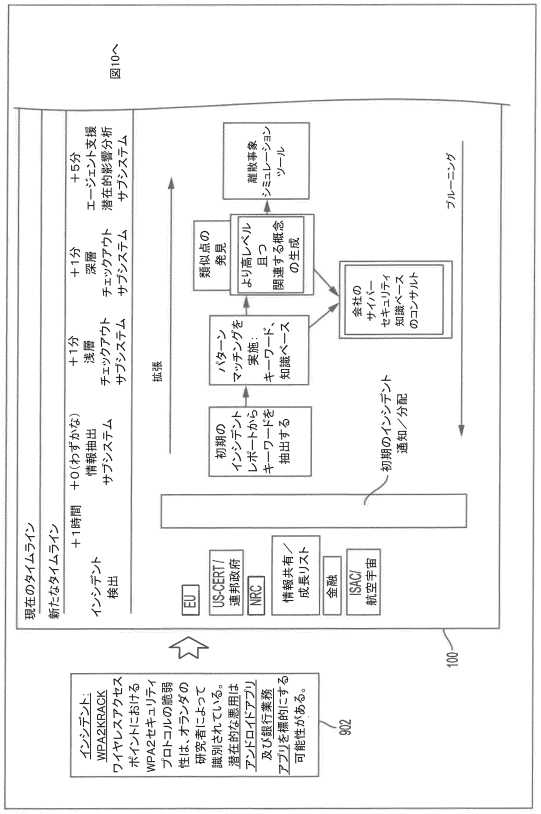
【図７】


入力：
情報抽出
サブシステム104、
浅層機械学習
サブシステム106、
及び／又は
深層機械学習
サブシステム108
からの出力
702
離散事象
シミュレーション
エンジン
704
出力：
侵入に対して
脆弱な経路、
侵入に対して
脆弱な資産、
侵入点、
侵入に対する
システムの脆弱性、
及び
前述の全ての可能性
706
700

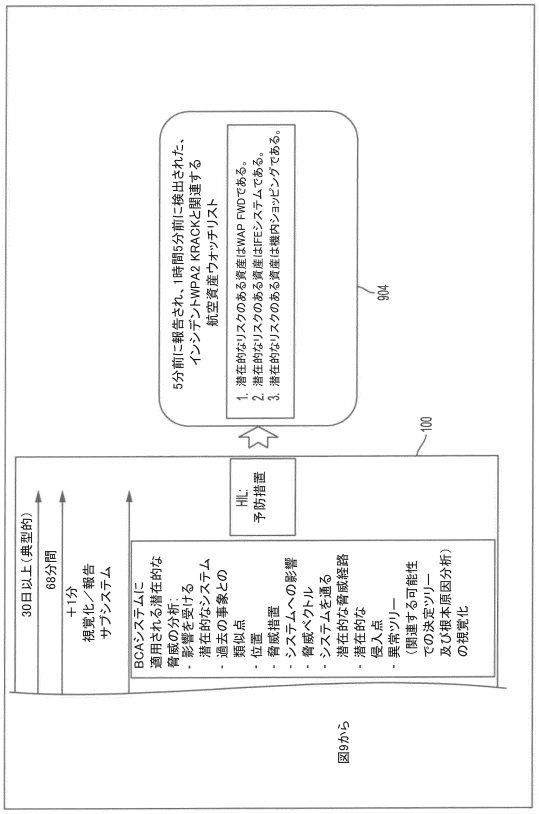
【図８】


アンドロイドアプリ
クレジットカード
銀行業務アプリ
機内ショッピング
IFEアプリ
IFEシステム
WPA FWD
WPA2
WAP AFT
806
1. WPA2
キーワード
802
1. 潜在的なリスクのある資産はWAP FWDである。資産
2. 潜在的なリスクのある資産はIFEシステムである。
3. 潜在的なリスクのある資産は機内ショッピングである。
804
800

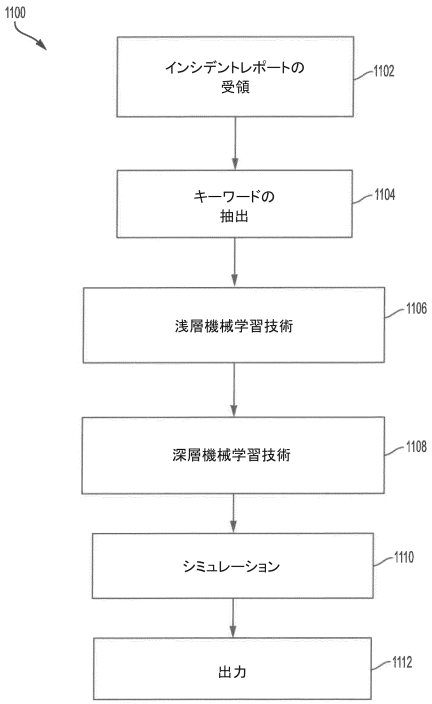
【図９】



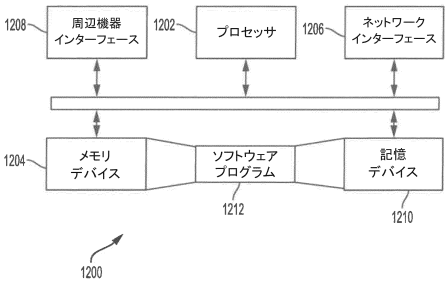
【図１０】



【図１１】



【図１２】



フロントページの続き

，シアトル，ピー．オー．ボックス３７０７，シー／オー ザ ボーイング カンパニー
(72)発明者 ヴァサツカ，ジェームズ イー．
アメリカ合衆国 ワシントン ９８１２４，シアトル，ピー．オー．ボックス ３７０７，シー／オー ザ ボーイング カンパニー

審査官 平井 誠

(56)参考文献 米国特許出願公開第２０１７／０２２８６５８（ＵＳ，Ａ１）
特開２０１４－１０２５５５（ＪＰ，Ａ）
国際公開第２０１４／２０８４２７（WO，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／５７
Ｇ０６Ｎ ３／０４