(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2019-511030
(P2019-511030A)
(43)公表日　平成31年4月18日(2019.4.18)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/55	(2013.01)	G06F 21/55		5K030
H04L 12/70	(2013.01)	H04L 12/70	D	

審査請求 未請求　予備審査請求 未請求　（全 173 頁）

(21)出願番号　特願2018-538714(P2018-538714)
(86)(22)出願日　平成29年1月24日(2017.1.24)
(85)翻訳文提出日　平成30年9月25日(2018.9.25)
(86)国際出願番号　PCT/US2017/014699
(87)国際公開番号　WO2017/127850
(87)国際公開日　平成29年7月27日(2017.7.27)
(31)優先権主張番号　62/294,258
(32)優先日　平成28年2月11日(2016.2.11)
(33)優先権主張国　米国(US)
(31)優先権主張番号　62/286,437
(32)優先日　平成28年1月24日(2016.1.24)
(33)優先権主張国　米国(US)
(31)優先権主張番号　62/307,558
(32)優先日　平成28年3月13日(2016.3.13)
(33)優先権主張国　米国(US)

(71)出願人　517384648
ハサン・シェド・カムラン
アメリカ合衆国　ヴァージニア州、２２０６６、グレート　フォールズ、リバー　ベンド　ロード　６２２
(74)代理人　100125645
弁理士　是枝　洋介
(74)代理人　100145609
弁理士　楠屋　宏行
(72)発明者　ハサン・シェド・カムラン
アメリカ合衆国　ヴァージニア州、２２０６６、グレート　フォールズ、リバー　ベンド　ロード　６２２

Fターム(参考)　5K030 GA15　LE10　MA01　MC08

最終頁に続く

(54)【発明の名称】人工知能によるコンピュータセキュリティ

(57)【要約】
【課題】本発明は、人工知能によるコンピュータセキュリティのシステムに関する。
【解決手段】
人工知能ベースのコンピュータセキュリティシステムは、クラウドベースの重層的情報セキュリティ（ＣＴＩＳ）による重要インフラストラクチャ防護および返報（ＣＩＰＲ）、サイバースペースにおける秘密オペレーションによる秘密機械学習（ＭＡＣＩＮＴ）および返報、論理的推論によるゼロデータベースの演繹型リアルタイム防御（ＬＩＺＡＲＤ）、クリティカルシンキング・メモリおよびパーセプション（ＣＴＭＰ）、辞書的客観性探索（ＬＯＭ）、線形量子情報転送（ＬＡＱＩＴ）、ベース接続協調攻撃統合ノード（ＢＣＨＡＩＮ）を伴った普遍的ＢＣＨＡＩＮ全接続、を備える。
【選択図】図１

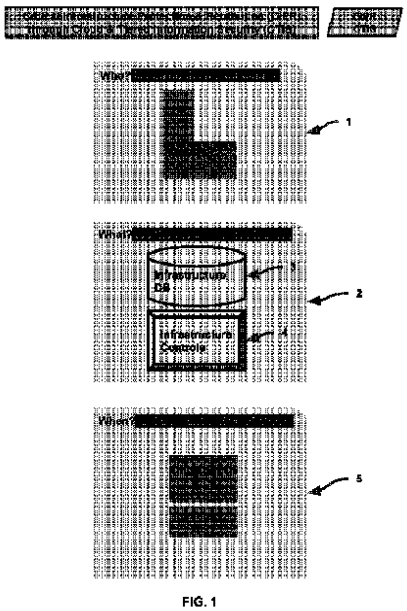


FIG. 1

【特許請求の範囲】
【請求項１】
人工知能によるコンピュータセキュリティシステムであって、システムは、プログラム化された命令を格納するメモリ、メモリに接続され、前記プログラム化された命令を実行するプロセッサ、および少なくとも１つのデータベースを備え、システムは、指定された機能を提供するコンピュータ実装システムを備える、システム。
【請求項２】
前記コンピュータ実装システムとは、クラウドおよび階層化情報セキュリティによる重要インフラストラクチャ防護および報復（ＣＩＰＲ／ＣＴＩＳ）であり、
ａ）ハッカーの行動を報告するエージェント達のネットワークを有する信用プラットフォームと、
ｂ）管理された暗号化セキュリティ、接続性およびコンプライアンスのソリューションおよびサービスを提供する、マネージドネットワークおよびセキュリティサービスプロバイダ（ＭＮＳＰ）をさらに備え、
仮想プライベートネットワーク（ＶＰＮ）は、ＭＮＳＰと信用プラットフォームを接続しており、ＶＰＮは、前記信用プラットフォームとの通信チャネルを提供し、前記ＭＮＳＰは、前記企業ネットワークのすべてのトラフィックを分析できるよう構成され、前記トラフィックは前記ＭＮＳＰにルーティングされる、請求項１に記載のシステム。
【請求項３】
前記ＭＮＳＰは、
ａ）論理的推論によるゼロデータベースの演繹型リアルタイム防御（ＬＩＺＡＲＤ）であって、外来コードから目標と機能を導出し、悪意の存在または正当な動機の欠如に反応して、その外来コードをブロックし、それまでの履歴データを参照せず、脅威それ自体を分析する、論理的推論によるゼロデータベースの演繹型リアルタイム防御と、
ｂ）疑似セキュリティ脅威（ＡＳＴ）であって、セキュリティルールセットの効力をテストするための、仮想のセキュリティシナリオを提供する、疑似セキュリティ脅威と、
ｃ）創作モジュールであって、前形状から新たなハイブリッド形状を知的に創作する処理を実行する、創作モジュールと、
ｄ）共謀検知であって、情報連携を見分け、セキュリティ関連の挙動のパターンを抽出し、多数の共謀セキュリティイベントに対する定期的な素性チェックを提供し、一見無関係なセキュリティイベント同士のパターンや関係を判定しようと試みる、共謀検知と、
ｅ）セキュリティ挙動であって、イベントとそのセキュリティ応答を格納、インデックス付けし、前記応答はブロック／許可の決定事項を含む、セキュリティ挙動と、
ｆ）反復型知的成長／知的進化（I^2GE）であって、ビッグデータとマルウェアシグネチャの認識を活用し、創造性モジュールとともにＡＳＴを活用することでマルウェアの将来起こりうる変化をエミュレートする、反復型知的成長／知的進化と、
ｇ）クリティカルシンキング・メモリ・パーセプション（ＣＴＭＰ）であって、前記ブロック／承認の決定事項を批判し、セキュリティの補完的なレイヤとして機能し、I^2GE、ＬＩＺＡＲＤ、および信用プラットフォームからの相互参照情報収集を活用する、クリティカルシンキング・メモリ・パーセプションを備え、ＣＴＭＰは、ある事柄についての客観的決定事項を構成する能力を推定し、内部の低い確信度に基づいてなされた決定を表明することを差し控える、クリティカルシンキング・メモリ・パーセプションを備える、請求項２に記載のシステム。
【請求項４】
ＬＩＺＡＲＤライトクライアントは、企業ネットワークのデバイスで動作するように構成され、ＭＮＳＰのＬＩＺＡＲＤとの通信を安全に行う、請求項３に記載のシステム。
【請求項５】
非武装地帯（ＤＭＺ）は、通常のコンピュータよりセキュリティ上不利な状態にあるＨＴＴＰサーバを有するサブネットワークを備え、このようなセキュリティ上不利な状態に企業ネットワークの残りの部分をさらすことのないようにしている、請求項３に記載のシ

ステム。
【請求項６】
前記Ｉ^{2}ＧＥは、並行する複数の進化系統が発達し選択される反復的進化を備え、イテレートされた世代が、同一の疑似セキュリティ脅威（ＡＳＴ）に適応し、最良のパーソナリティトレイトを有する系統が、結局はこのセキュリティ脅威に対して最もよく耐えることになる、請求項３に記載のシステム。
【請求項７】
前記ＬＩＺＡＲＤは、
ａ）構文モジュールであって、コンピュータのコードを読み書きするためのフレームワークを提供する、構文モジュールと、
ｂ）目標モジュールであって、前記構文モジュールを用いてコードから目標を導出し、前記目標を、自身の複合目標フォーマットに出力する、目標モジュールと、
ｃ）仮想難読化であって、企業ネットワークとデータベースが、仮想環境内に複製され、機密データが模擬（偽の）データと置き換えられ、ターゲットの挙動に応じて環境がリアルタイム動的に変更され、システム全体としてより多くの偽の要素、またはより多くの本物の要素が含まれる、仮想難読化と、
ｄ）信号擬態であって、仮想難読化の分析が終わったときに報復の形状を提供する、信号擬態と、
ｅ）内部整合性チェックであって、外来コードのすべての内部機能の辻褄が合っていることをチェックする、内部整合性チェックと、
ｆ）外来コード改訂であって、前記構文モジュールと目標モジュールを使用し、外来コードを複合目標フォーマットにまとめる、外来コード改訂と、
ｇ）秘密コード検知であって、データおよび送信パケット内に密かに埋め込まれたコードを検知する、秘密コード検知と、
ｈ）要求マップマッチングであって、マップ化された要求および目標の階層構造であり、外来コードがシステムの目的全体にフィットしているかを判断するために参照される、要求マップマッチングを備え、
書き込みでは、前記構文モジュールは、前記目標モジュールから複合様式の目標を受信し、コードを任意のコード構文で書き込み、ヘルパ機能が前記任意のコードを実際の実行可能コードへと翻訳し、読み込みでは、前記構文モジュールは、前記目標モジュールがこのようなコードの機能の目標を導出できるよう、コードの構文解釈を提供し、
前記信号擬態は、マルウェアがハッカーと通信するための構文を読み解くために、前記構文モジュールを使用し、その後、このような通信を乗っ取り、機密データをハッカーに送ることに成功したという、誤った印象をマルウェアに与え、前記ハッカーは、前記マルウェアのエラーコードもＬＩＺＡＲＤによって送られ、このエラーコードが前記マルウェアから来たもののように思わせ、
前記外来コード改訂は、前記導出された目標を使用するコードセットを構築し、これによって、外来コードから読み解かれた所望の目標だけが企業内で実行され、意図しない機能の実行がシステムにアクセスすることのないことが保証される、請求項３に記載のシステム。
【請求項８】
外来コード改訂が外来コードを構文的に再現することで、起こりうる未検知の悪意のエクスプロイトを軽減する様子を示し、組合せメソッドは、宣言された目標を導出された目標と比較し一致させ、前記目標モジュールは、複合目標フォーマットを操作するために使用され、前記導出された目標を用いて、前記要求マップマッチングは、階層的構造を維持管理し、すべての企業の管轄範囲をメンテナンスし、これにより、管轄範囲指向の要求マップの空きに応じて、コードブロックの目的が定義され正当化され、入力された目標が、再帰的デバッグプロセスに取り込まれる、請求項７に記載のシステム。
【請求項９】
前記再帰的デバッグが、コードセグメントをループ処理してバグの有無をテストし、バ

グフィックスを適用し、それでもバグが残っている場合は、前記コードセグメント全体が、オリジナルの外来コードセグメントに置換され、前記オリジナルのコードセグメントは、その後仮想難読化や挙動分析を促進するためにタグ付けされ、前記コードを改訂するために、外来コードを用いて、前記目標モジュールおよび構文モジュールが前記コードのオリジナルの状態を解釈し、改訂バージョンに消えないバグがあるためにオリジナルの外来コードセグメントをインストールする必要がある場合、前記外来コードは前記デバッガから直接参照され、改訂コードでは、セグメントが仮想ランタイム環境によってテストされ、コーディングバグの有無がチェックされ、前記仮想ランタイム環境はコードセグメントを実行し、実行時エラーの有無をチェックし、コーディングバグを用いて、前記仮想ランタイム環境において生じたエラーが、スコープと種別において定義され、目的の整合を用いて、前記宣言された目的からコードを再び導出することで、前記コーディングバグに対する解決策の候補が考え出され、このようなバグを回避するために、前記コーディングバグのスコープが代替フォーマットの形式に書き換えられ、前記解決策の候補が出力され、他になにも解決策がない場合は、前記コードセグメントに対するコード改訂は喪失され、前記外来コードから直接来る前記オリジナルのコードセグメントが最終コードセットにおいて使用される、請求項８に記載のシステム。

【請求項１０】

要求マップマッチングの操作ために、ＬＩＺＡＲＤクラウドおよびＬＩＺＡＲＤライトは、企業の管轄範囲部門の階層構造マップを参照し、入力された目標が主張されたものか、前記目標モジュール経由で導出されたものかにかかわらず、要求マップマッチングはコード／関数が前記企業システムの内部で実行するための根拠を確認し、前記階層構造マップのマスターコピーが、ＭＮＳＰのＬＩＺＡＲＤクラウドに格納され、前記マスターコピーを参照することで、要求マップマッチング内の要求インデックスが計算され、そして、予め最適化された前記要求インデックスが、すべてのアクセス可能なエンドポイントのクライアントに配布され、前記要求マップマッチングは最も適切なシステム全体としての要求に関する要求リクエストを受信し、対応する出力は、前記適切な要求を表している複合目標フォーマットである、請求項８に記載のシステム。

【請求項１１】

企業のＬＡＮインフラストラクチャ全体がＭＮＳＰ内で仮想的に再構築され、前記システムが挙動分析を実行すると、前記ハッカーは現実のＬＡＮインフラおよび仮想クローンバージョンのＬＡＮインフラの双方にある要素に対してさらされ、このような分析の結果がリスクを示す場合、前記ハッカーの仮想クローンインフラへの露出は、実際のデータおよび／またはデバイスが攻略されるリスクを軽減するために増加される、請求項３に記載のシステム。

【請求項１２】

マルウェアルートシグネチャの新版／変種を生成するために、前記マルウェアルートシグネチャがＡＳＴに与えられ、マルウェアの多型変種がI^2ＧＥから出力され、マルウェア検知に転送される、請求項３に記載のシステム。

【請求項１３】

前記マルウェア検知は、ユーザスペース、カーネルスペース、およびファームウェア／ハードウェアスペースが設けられたコンピュータの構成の３つのレベルすべてに配置され、前記スペースのすべては、ＬＩＺＡＲＤライトエージェントによって監視される、請求項１２に記載のシステム。

【請求項１４】

前記コンピュータ実装システムは、サイバースペースにおける秘密オペレーションによる秘密機械学習（ＭＡＣＩＮＴ）および報復であって、

ａ）知的情報および構成管理（I^2ＣＭ）であって、知的情報の管理、閲覧、および制御を提供する、知的情報および構成管理と、

ｂ）管理コンソール（ＭＣ）であって、入出力チャネルをユーザに提供する、管理コンソールをさらに備え、

前記Ｉ^{2}ＣＭは、
ｉ）アグリゲーションであって、汎用のレベル判定基準を使用して、不必要で冗長な情報を遮断し、多数のプラットフォームからの情報ストリームをマージ、タグ付けする、アグリゲーションと、
ｉｉ）設定および導入サービスであって、新たな企業の資産（コンピュータ、ノートパソコン、携帯電話）を、正しいセキュリティ設定と通信設定で導入するためのインタフェースである、設定および導入サービスと、
ｉｉｉ）管轄範囲による分割であって、タグ付けされた情報の集積が、管理コンソールのユーザに該当する管轄範囲にしたがって、排他的に分割される、管轄範囲による分割と、
ｉｖ）脅威による分割であって、個々の脅威に応じて情報を整理する、脅威による分割と、
ｖ）自動化制御であって、ＭＮＳＰクラウド、信用プラットフォーム、または付加的なサードパーティサービスにアクセスする、自動化制御を備える、請求項１に記載のシステム。
【請求項１５】
ＭＮＳＰクラウドにおいて、挙動分析は、模擬データ環境にいる間のマルウェアの状態と実行された活動を観察し、前記マルウェアが偽データをハッカーのもとへ送信しようとしているとき、送信される信号は、偽のハッカーが受信するようにルーティングされ、ハッカーインタフェースは、前記マルウェアのコード構造を受け取り、前記マルウェアの内部構造についてリバースエンジニアリングを行い、ハッカーインタフェースを出力し、偽のハッカーおよび偽のマルウェアを仮想環境の中でエミュレートし、仮想化された偽のハッカーは、前記マルウェアの次の挙動パターンを観察するために、前記本物のマルウェアに応答信号を送信し、前記ハッカーには、本物のマルウェアの挙動／状態と関係のない偽の応答コードが与えられる、請求項１４に記載のシステム。
【請求項１６】
エクスプロイトスキャンは、犯罪資産の能力と性質を特定し、それによって得られるスキャン結果が、エクスプロイトによって管理され、エクスプロイトは、信用プラットフォームによって、標的となる犯罪システムに潜入する報復エクスプロイトデータベースを経由して送信されたプログラムであり、報復エクスプロイトデータベースは、設置されたバックドアおよび既知の脆弱性としてハードウェアベンダによって提供された、犯罪活動をエクスプロイトする手段を含んでおり、統合科学捜査的証拠データベースが、多数の企業にわたる多数のソースから収集された科学捜査的証拠を含んでいる、請求項１４に記載のシステム。
【請求項１７】
犯罪システムからの二重スパイが、企業ネットワークのファイルを捕捉し、ファイアウォールがログを生成し、ログはログ集約に転送され、ログ集約は、長期／深層スキャンとリアルタイム／表面スキャンに向けて、データをカテゴリ別に分離する、請求項１４に記載のシステム。
【請求項１８】
前記深層スキャンは、共謀検知サブアルゴリズムおよび外来エンティティ管理サブアルゴリズムを活用して、ビッグデータに貢献および連動し、セキュリティチェックポイントからの標準ログが集約され、ログ集約の低制限フィルタにより選択され、イベントインデックス＋トラッキングはイベントの詳細情報を格納し、異常検知は、前記深層スキャンモジュールによって提供された中間データ基づいてイベントインデックスおよびセキュリティ挙動を用いることにより、可能性のあるリスクイベントを決定し、外来エンティティ管理および共謀検知はイベントの分析に関わっている、請求項１７に記載のシステム。
【請求項１９】
前記信用プラットフォームは、任意コンピュータを検索して、その任意コンピュータまたはその関連／近隣サーバ（任意コンピュータが接続するサーバ）が、前記信用プラット

フォームに対する、過去に設置した二重または三重のスパイであるかをチェックし、エージェント検索チェックは、信用できる二重スパイインデックス＋トラッキングクラウドおよび、信用できる三重スパイインデックス＋トラッキングクラウドで実行され、前記任意コンピュータに信用されている二重スパイが、その信用されたチャネルを通じてエクスプロイトをプッシュし、エクスプロイトは、機密ファイルを発見しようとし、機密ファイルを検疫し、機密ファイルの正確な状態を信用プラットフォームに送り返し、その後、その機密ファイルを前記犯罪コンピュータから安全に消去しようとする、請求項１７に記載のシステム。

【請求項２０】

ＩＳＰＡＰＩのリクエストが、信用プラットフォーム経由で行われ、ネットワーク監督で、前記任意システムに関するネットワークログと、犯罪コンピュータにファイルが転送された可能性が見つかり、メタデータを使用して、ファイルがどのコンピュータに送られたかを、かなりの確信度をもって決定し、前記ネットワーク監督は、犯罪コンピュータのネットワークの詳細情報を発見し、このような情報を、別ルートで前記信用プラットフォームに送り、前記信用プラットフォームを使用して、ソフトウェアベンダおよびハードウェアベンダが提供するセキュリティＡＰＩを実行し、司法調査を支援することができる、設置されたバックドアをエクスプロイトする方法を示している、請求項１９に記載のシステム。

【請求項２１】

前記信用プラットフォームが、前記犯罪コンピュータに対してソフトウェアまたはファームウェアの更新を行うことにより、新たなバックドアを設置し、隠密であることを守るために、プラセボアップデートが近隣の類似機器にプッシュされ、ターゲットの身元詳細情報が、前記信用プラットフォームに送信され、前記信用プラットフォームは、ソフトウェア／ファームウェア保守者２８７と通信し、プラセボアップデートおよびバックドアアップデートを該当するコンピュータにプッシュし、前記バックドアアップデートは、犯罪コンピュータに既に設置したソフトウェアアップデートシステムを用いることにより、犯罪コンピュータのシステムに新たなバックドアを導入し、プラセボアップデートはバックドアを取り除き、保守者は、バックドアを標的に転送し、加えて標的に平均以上の露出をしているコンピュータにも転送し、バックドアアップデートを通じてエクスプロイトを設置すると、機密ファイルは、そのメタデータ使用履歴を後で分析できるように検疫されコピーされ、捕捉となる科学捜査データが集められ、前記信用プラットフォームにある、エクスプロイトの接点に送られる、請求項１４に記載のシステム。

【請求項２２】

ありとあらゆる変更／アップデートについて犯罪システムをモニターするために、長期優先フラグが信用プラットフォームにプッシュされ、前記企業システムは標的をワラントモジュールに提出し、このワラントモジュールは、系列システムのすべての入力をスキャンして、定義された標的の任意の関連性を検索し、一致するものがあれば、その情報は企業システムに渡され、企業システムは、そのワラントを定義しており、標的へ潜入しようとし、前記入力は、所望の分析モジュールに転送され、分析モジュールが、相互に有益なセキュリティ情報を同期する、請求項１４に記載のシステム。

【請求項２３】

前記コンピュータ実装システムとは、論理的推論によるゼロデータベースの演繹型リアルタイム防御（ＬＩＺＡＲＤ）であり、

ａ）静的コア（ＳＣ）であって、主に不変のプログラムモジュールを備えている、静的コアと、

ｂ）イテレーションモジュールであって、ダイナミックシェル上のモジュールを変更、作成、および処分し、セキュリティ上のパフォーマンスの参考のために、ＡＳＴを使用し、イテレーションコアを使用して自動コード記述の方法論を処理する、イテレーションモジュールと、

ｃ）差分変更アルゴリズムであって、前記ＡＳＴが見つけた欠陥にしたがって基底バー

ジョンを変更し、差分ロジックが適用された後、新バージョンが提示され、その直後にイテレーションコアが再帰的に呼び出され、ＡＲＴによってテストされたものと同じプロセスを経る、差分変更アルゴリズムと、

ｄ）論理減算アルゴリズムであって、疑似セキュリティ脅威（ＡＳＴ）からダイナミックシェルのバージョンの既知のセキュリティ応答を受信し、ＬＤＡはまた、どのコードセット構成が既知の正しい応答を達成するかを、セキュリティシナリオに合わせて推論する、論理減算アルゴリズムと、

ｅ）ダイナミックシェル（ＤＳ）であって、イテレーションモジュール（ＩＭ）によって自動的にプログラムされたダイナミックプログラムモジュールを主に含む、ダイナミックシェルと、

ｆ）コード検疫であって、外来コードを制限付の仮想環境に隔離する、コード検疫と、

ｇ）秘密コード検知であって、データおよび送信パケット内に密かに埋め込まれたコードを検知する、秘密コード検知と、

ｈ）外来コード改訂であって、外来コードの目標を導出した後、コードの一部あるいは全部を改訂し、改訂版だけの実行を許可する、外来コード改訂をさらに備え、

すべての企業デバイスはＬＩＺＡＲＤにルーティングされ、企業デバイスを稼働させるすべてのソフトウェアとファームウェアは、あらゆる種類のダウンロード／アップロードを、永続プロキシのようにＬＩＺＡＲＤ経由で実行するようにハードコードされており、ＬＩＺＡＲＤは、移動中のデータ、休止中のデータ、および使用中のデータを含む３種類のデータと相互作用し、ＬＩＺＡＲＤは、ファイル、電子メール、ウェブ、モバイル、クラウド、リムーバブルメディアを含むデータメディアと相互作用する、請求項１に記載のシステム。

【請求項２４】

ａ）ＡＳＴオーバーフロー中継であって、前記システムが低確信度の判断しかできないときは、将来のバージョンの改善のために、データがＡＳＴに中継される、ＡＳＴオーバーフロー中継と、

ｂ）内部整合性チェックであって、外来コードのブロックのすべての内部機能の辻褄が合っているかどうかをチェックする、内部整合性チェックと、

ｃ）ミラーテストであって、前記改訂版の入出力の関係が、元のコードのものと同じであることを確かめ、これによって、元のコードに存在する隠されたエクスプロイトはどれも使われなくなり、二度と実行されることがない、ミラーテストと、

ｄ）要求マップマッチングであって、マップ化された要求および目標の階層構造を備え、外来コードが前記システムの目的全体にフィットしているかを判断するために参照される、要求マップマッチングと、

ｅ）実データ同期部であって、混合環境に与えられるデータを、どの優先順位で与えるのかを選択し、これによって、疑われるマルウェアに機密情報をアクセスできなくする、実データ同期部と、

ｆ）データマネージャであって、仮想環境の外部から来るエンティティとデータとの間にある中間者インタフェースである、データマネージャと、

ｇ）仮想難読化であって、仮想化された偽の環境に、徐々にかつ部分的に沈めることで、コードを乱雑にし、制限する、仮想難読化と、

ｈ）秘密輸送モジュールであって、マルウェアに何も知らせず慎重にマルウェアを模擬データ環境に転送する、秘密輸送モジュールと、

ｉ）データリコール追跡であって、疑わしいエンティティからアップロードされたりそこへダウンロードされたりするすべての情報を追跡する、データリコール追跡をさらに備える、請求項２３に記載のシステム。

【請求項２５】

目標比較モジュールであって、４つの異なるタイプの目的を比較し、システムの全体的な目的に対して良い結果をもたらすことにおいて、そのエンティティの存在および挙動が合理的でＬＩＺＡＲＤによって理解されることを保証する、目標比較モジュールをさらに

備える、請求項２４に記載のシステム。
【請求項２６】
前記イテレーションモジュールは、前記ＳＣを使用して、データ返送中継（ＤＲＲ）からの定義された目標にしたがって、ＤＳのコードベースを構文的に変更し、前記改変バージョンのＬＩＺＡＲＤは、前記ＡＳＴによって、多数のさまざまなセキュリティシナリオのもとで、並行してストレステストを受ける、請求項２５に記載のシステム。
【請求項２７】
前記ＳＣの内部では、論理的導出が、初期のより簡易な機能から、必要な機能を論理的に導出し、これにより、機能の依存性のツリー全体が、宣言された複合目標から構築され、
コード翻訳が、構文モジュール機能によって直接読み解かれる任意の汎用コードを、任意に選ばれた既知のコンピュータ言語に変換され、既知のコンピュータ言語から任意のコードへの逆翻訳も行われ、
ロジック削減が、コードに記述されたロジックを、より簡易な形状にまとめて相互に接続された機能のマップを生成し、
複合目標フォーマットが、目標の全体を表している相互に連携する下位目標を格納するための格納フォーマットを表しており、
目標の関連性が、挙動の機能および型のどれがどの種類の目標を指しているかを調べるための、ハードコーティングされた参考資料のことであり、
反復的拡張が、目標の関連性を参照し、詳細と複雑性を追加して、単純なゴールを複合目標に進化させ、
反復型解釈は、相互に接続された機能をループ処理し、かつ、目標の関連性を参照することにより、解釈された目標を生成し、
協力しあうことで未知の外来コードから論理的な目標を導出し、また宣言された機能コードのゴールから実行可能コードを生成する、構文モジュールおよび目標モジュールによって、外側コアが形成され、
外来コードは、ＬＩＺＡＲＤには未知であるコードで、その機能および意図された目標は未知であり、外来コードは内側コアへの入力であり、導出された目標が出力であり、前記導出された目標は、前記目標モジュールにより推定されたものとしての、任意のコードの意図であり、前記導出された目標は、複合目標フォーマットで返される、請求項２６に記載のシステム。
【請求項２８】
前記ＩＭは、セキュリティ上のパフォーマンスの参考のためにＡＳＴを使用し、イテレーションコアを使用して自動コード記述の方法論を処理し、前記ＤＲＲでは、ＬＩＺＡＲＤがやむなく低い確信度で意志決定をしなければならない場合に、悪意の攻撃および常習犯のデータが前記ＡＳＴに中継され、前記イテレーションコアの内部では、差分変更アルゴリズム（ＤＭＡ）が、前記内側コアから、構文／目的プログラミング能力とシステムの目的のガイダンスを受け取り、このようなコードセットを使うことで、前記ＡＲＴが見つけた欠陥にしたがって基底バージョンを変更し、セキュリティテスト結果での欠陥が、前記仮想実行環境を実行している間に前記基底バージョンをパスしたセキュリティ脅威を示すために、可視的に提示される、請求項２７に記載のシステム。
【請求項２９】
前記ＤＭＡの内部では、現在の状態は、ダイナミックシェルのコードセットを、象徴的に相関している図形、サイズ、および位置とともに表しており、これらの図形の種々の構成は、セキュリティ情報収集およびセキュリティ応答の種々の構成を示しており、前記ＡＳＴは、誤りであったり、正しい応答であったりする、現在の状態のありうる応答を提供し、
攻撃ベクトルは、サイバーセキュリティの脅威の象徴的な実証として機能し、方向、サイズ、および色はすべて、攻撃ベクトル、マルウェアのサイズ、マルウェアの種類のような、仮定のセキュリティプロパティに関連しており、前記攻撃ベクトルは、コードセット

のセキュリティ応答を表すために、そのコードセットに象徴的にぶつかり、
正しい状態は、ダイナミックシェルのコードブロックから所望のセキュリティ応答を生ずる、前記ＤＭＡのプロセスの最終結果を表しており、前記現在の状態と正しい状態の結果の差異は、種々の攻撃ベクトルの応答の差異に帰し、
前記ＡＳＴは、正しいセキュリティ応答に加えてセキュリティ上の既知の欠陥を提供し、ロジック推論アルゴリズムは、前記ＤＳの過去のバージョンを使用して、正しいセキュリティ応答プログラムと呼ばれる、優秀で十分な設備が整っているダイナミックシェルのバージョンを生成する、請求項２８に記載のシステム。
【請求項３０】
仮想難読化の内部では、疑問の余地のあるコードが密かに、データの半分が模擬データと知的に混合されている環境に割り当てられ、実システム内で稼働しているどの対象も、仮想的隔離により、部分模擬データ環境または完全模擬データ環境に容易かつ秘密裏に転送され、模擬データジェネレータは、偽造かつ無用なデータを作成するためのテンプレートとして、前記実データ同期部を使用し、到来する外来コードの認知におけるリスクの確信度の認知は、ＬＩＺＡＲＤが選ぶ難読化のレベルに影響し、コードが悪意のあるということにおける確信度が高い場合は、多量の模擬データを含む環境が割り当てられ、コードが悪意のあるということにおける確信度が低い場合は、実システムあるいは１００％模擬データの環境のどちらかが割り当てられる、請求項２６に記載のシステム。
【請求項３１】
データリコール追跡は、疑わしいエンティティからアップロードされたりそこへダウンロードされたりするすべての情報を追跡し、模擬データが正当な企業エンティティに送信された場合、すべての模擬データを呼び戻すコールバックが実行され、実データが、代わりに送信され、コールバックトリガーは、正当な企業エンティティが、データが偽ではないと確認されるまで、特定の情報に対する操作を差し控えるように実装されている、請求項３０に記載のシステム。
【請求項３２】
挙動分析は、修正処置の候補を決定するために、疑わしいエンティティのダウンロードおよびアップロードの挙動を追跡し、実システムは、仮想環境の完全な外部に存在する、前記オリジナルの実データを含み、模擬データを置き換える実データは、実データがフィルタリングされずに前記データリコール追跡に提供される場所であり、これにより、実データパッチを作成して、前記模擬データを以前の疑わしいエンティティ上の実データと置き換えることができ、仮想的に隔離された環境に沈められているデータマネージャは、前記データリコール追跡から実データパッチを受け取り、無害コードが挙動分析によって悪意を持っていると明らかにされると、修正処置が実行されることで、前記以前の疑わしいエンティティの前記模擬データを、それが表す前記実データに置き換え、シークレットトークンは、ＬＩＺＡＲＤによって生成され割り当てられるセキュリティ文字列であり、本当に無害である前記エンティティにその仕事を進めないようにし、トークンが見当たらない場合、これは、それがマルウェアであるというリスク評価のために、この正当なエンティティが間違って部分的模擬データ環境に配置されている可能性が高いシナリオを示しており、その後、前記遅延インタフェースを有する遅延セッションが起動され、トークンが見つかった場合、これはサーバ環境が本物であることを示しており、したがって遅延セッションは無効化される、請求項３１に記載のシステム。
【請求項３３】
前記挙動分析内で、目標マップは、企業システム全体に目標を与えるシステムの目的の階層構造であり、宣言された目標、活動の目標、およびコードベースの目標は、前記疑わしい実体が行っていることが何であれ、本来のシステムの要求と比較され、活動監視では、前記疑わしいエンティティのストレージ、ＣＰＵ処理、およびネットワーク活動が監視され、前記構文モジュールは、所望の機能に関してこのような活動を解釈し、このような機能は、その後、前記目標モジュールによる挙動において意図された目標に変換され、コードベースは、前記疑わしいエンティティのソースコード／プログラミング構造であり、

前記構文モジュールに転送され、前記構文モジュールは、コーディングの構文を理解し、プログラミングコードおよびコードの活動を中間機能連携マップに還元し、前記目標モジュールは、前記疑わしいエンティティの認知された意図、コードベースの目標、および活動の目標の出力を生成し、前記コードベースの目標には、ＬＩＺＡＲＤの構文的プログラミング能力によって引き出された、エンティティの前記既知の目標、機能、管轄範囲および権限が含まれており、前記活動の目標には、ＬＩＺＡＲＤのストレージ、処理およびネットワーク活動の理解によって読み解かれた、エンティティの既知の目標、機能、管轄範囲および権限が含まれており、前記宣言された目標は、エンティティ自体によって宣言された、前記エンティティの想定される目的、機能、管轄範囲および権限であり、前記要求された目標には、エンタープライズシステムが必要とする期待される目的、機能、管轄範囲および権限が含まれており、すべての目標が、比較モジュールにおいて比較され、前記目的の間に不一致があれば、目標の相違のシナリオが呼び出され、修正処置につながる、請求項３１に記載のシステム。

【請求項３４】

前記コンピュータ実装システムは、クリティカルシンキング・メモリおよびパーセプション（ＣＴＭＰ）であり、

ａ）クリティカルルールスコープエクステンダー（ＣＲＳＥ）であって、既知のパーセプションのスコープを受け取り、パーセプションのクリティカルシンキングスコープを含むよう、パーセプションの既知のスコープを拡張する、クリティカルルールスコープエクステンダーと、

ｂ）妥当ルールであって、パーセプションのクリティカルシンキングスコープを利用することにより導き出された妥当ルールを示している、妥当ルールと、

ｃ）ルール実行（ＲＥ）であって、メモリが乱雑フィールドをスキャンすることにより、存在して充足可能であると確認されたルールを、該当する所望のクリティカルシンキングの決定事項を生成するために実行する、ルール実行と、

ｄ）クリティカル決定出力であって、パーセプション観察者エミュレータ（ＰＯＥ）および前記ルール実行の双方が至った結論を比較することにより、ＣＴＭＰの出力全体を決定するための最終ロジックを生成する、クリティカル決定出力をさらに備え、

前記ＰＯＥは、前記観察者のエミュレーションを生成し、パーセプションポイントの候補すべてを、このような様々な観察者エミュレーションを使用してテスト／比較し、

前記ＲＥは、ルールセットの変換を追跡するために使用される、市松模様の平面を備え、平面上のオブジェクトは、任意のセキュリティ状況の複雑さを表しており、一方で「セキュリティの市松模様」に広がるそのようなオブジェクトの動きは、セキュリティルールセットの応答によって管理されるセキュリティ状況の進化を示す、請求項１に記載のシステム。

【請求項３５】

ａ）主観的意見決定であって、選択パターンマッチングアルゴリズム（ＳＰＭＡ）によって与えられる決定である、主観的意見決定と、

ｂ）入力システムメタデータであって、ＳＰＭＡから与えられ、前記アルゴリズムのメカニカルプロセスおよびそのような決定に至った経緯を記述している未処理メタデータを有する、入力システムメタデータと、

ｃ）事由処理であって、プロパティの属性を比較することにより表明を論理的に理解する、事由処理と、

ｄ）ルール処理であって、導き出された結果ルールを、当面の問題のスコープを決定するための参照点として利用する、ルール処理と、

ｅ）メモリウェブであって、充足可能なルールを求めてログをスキャンする、メモリウェブと、

ｆ）未処理パーセプション生成であって、ＳＰＭＡからメタデータログを受け取り、そのようなログはパースされ、そのようなアルゴリズムのパーセプションを表すパーセプションが形成され、前記パーセプションは、複合パーセプションフォーマット（ＰＣＦ）に

格納され、前記ＰＯＥによってエミュレートされ、適用済パーセプションの視点は、ＳＰＭＡによって既に適用され利用されたパーセプションの視点を示している、未処理パーセプションと、

ｇ）自動化パーセプション発見メカニズム（ＡＰＤＭ）であって、適用済パーセプションの視点によって与えられる入力にしたがって形成される、混成パーセプションを生成する創作モジュールを活用し、これによって、前記パーセプションのスコープを拡張することができる、自動化パーセプション発見メカニズムと、

ｈ）自己批判的知識密度（ＳＣＫＤ）であって、報告可能なログの限界を越えた、未知である可能性がある知識のスコープおよび型を推定し、これによって、この結果生じるＣＴＭＰのクリティカルシンキング的な特徴によって、関与する知識のすべての可能なスコープを活用することができ、クリティカルシンキングは、ルールベースの思考の外殻範囲を示している、自己批判的知識密度と、

ｉ）意味付けの導出（ＩＤ）であって、現時点で適用されたパーセプションの視点から意味付けされうる、パーセプションの視点のデータを導出する、意味付けの導出をさらに備え、

前記ＳＰＭＡは、パーセプションおよびルールを介してＣＴＭＰにより実行される前記クリティカルシンキングと並置される、請求項３４に記載のシステム。

【請求項３６】

ａ）リソース管理および割付（ＲＭＡ）であって、調整可能ポリシーは、観察者エミュレーションを実行するために活用されるパーセプションの数を定め、選ばれたパーセプションの優先順位が、重み付けの降順で選択され、前記ポリシーは、パーセンテージ、固定値、あるいは、より複雑な選択アルゴリズムであろうと、切り捨てを選択する方法を定める、リソース管理および割付と、

ｂ）ストレージ検索（ＳＳ）であって、データ拡張ログからの前記ＣＶＦを、パーセプションストレージ（ＰＳ）のデータベース検索における判断基準として使用し、ＰＳでは、パーセプションと、それらの該当する重み付けが、それらのインデックスとしての比較可能可変フォーマット（ＣＶＦ）とともに格納される、ストレージ検索と、

ｃ）メトリック処理であって、前記ＳＰＭＡからの変数割付に対してリバースエンジニアリングを行う、メトリック処理と、

ｄ）パーセプション推論（ＰＤ）であって、割付の回答と、それに対応するシステムメタデータを使用して、前記割付の回答の元のパーセプションを再生する、パーセプション推論と、

ｅ）メタデータカテゴリ化モジュール（ＭＣＭ）であって、デバッグおよびアルゴリズム追跡が、構文ベースの情報カテゴリ化によって個別のカテゴリに分割され、前記カテゴリが、リスクおよび機会と相関関係を有する、個々の割付の回答をまとめ上げて生成するために使用される、メタデータカテゴリ化モジュールと、

ｆ）メトリック合成であって、パーセプションの視点を、メトリックのカテゴリに分割する、メトリック合成と、

ｇ）メトリック変換であって、個々のメトリックをパーセプションの視点全体に戻す、メトリック変換と、

ｈ）メトリック拡張（ＭＥ）であって、多数のさまざまなパーセプションの視点のメトリックを、個々のデータベースに、カテゴリ別に格納する、メトリック拡張と、

ｉ）比較可能可変フォーマットジェネレータ（ＣＶＦＧ）であって、情報ストリームを、比較可能可変フォーマット（ＣＶＦ）に変換する、比較可能可変フォーマットジェネレータをさらに備える、請求項３５に記載のシステム。

【請求項３７】

ａ）パーセプションマッチングであって、ルール構文導出（ＲＳＤ）から受信したパーセプションから、ＣＶＦが形成され、新たに形成されたＣＶＦは、前記ＰＳ内で類似したインデックスを有する、該当するパーセプションを検索するために使用され、一致する候補が、ルール構文生成（ＲＳＧ）に戻される、パーセプションマッチングと、

ｂ）メモリ認識（ＭＲ）であって、入力データから乱雑フィールドが形成される、メモリ認識と、
ｃ）メモリコンセプトのインデックス付けであって、すべてのコンセプトが、個別にインデックスに最適化され、前記インデックスは、乱雑フィールドと連携するために、文字スキャナによって使用される、メモリコンセプトインデックス付けと、
ｄ）ルール充足度パーサ（ＲＦＰ）であって、ルールの個々の部分を、認識のタグとともに受信し、各部分は、メモリ認識によって、乱雑フィールド内で見つかった、または見つからなかったとマークされ、前記ＲＦＰは、どのルール全体、つまり、そのルールの全部分の合成が、乱雑フィールド内で前記ＲＥするに値するほど十分に認識されたのかを、論理的に推論する、ルール充足度パーサと、
ｅ）ルール文法フォーマット分割（ＲＳＦＳ）であって、妥当ルールが分割され、型ごとにまとめられ、これにより、すべての処置、プロパティ、条件、およびオブジェクトが、別々に束ねられる、ルール文法フォーマット分割と、
ｆ）ルール構文導出であって、論理的な「白か黒か」ルールが、メトリックベースのパーセプションに変換され、これにより、多数のルールの複雑な配列が、さまざまな勾配の多数のメトリックにより表現される、単一で一様なパーセプションに変換される、ルール構文導出と、
ｇ）ルール構文生成（ＲＳＧ）であって、パーセプション形式に格納されそのパーセプションの内部メトリック構成に関与している、以前に確認されたパーセプションを受信し、このような勾配ベースのメトリックの測定値が、元のパーセプションの入力／出力される情報のフローを列挙する、二値で論理的なルールセットに変換される、ルール構文生成と、
ｈ）ルール文法フォーマット分割（ＲＳＦＳ）であって、妥当ルールは、観察されているオブジェクトの現実に従うルールセットの正確な明示を表しており、妥当ルールが分割され、型ごとにまとめられ、したがってすべての処置、プロパティ、条件、およびオブジェクトが、別々に束ねられ、これによってシステムは、どの部分が乱雑フィールド内で見つかっていて、どの部分が見つかっていないのかを判別することが可能となる、ルール文法フォーマット分割と、
ｉ）本質的論理的推論であって、論理的原則を用い、そうして誤謬を避けながら、どの種類のルールがパーセプションの範囲内でメトリックの勾配を正確に表しているかを推論する、本質的論理的推論と、
ｊ）メトリックコンテキスト分析であって、メトリックのパーセプションの範囲内で相互関係を分析し、あるメトリックは他のメトリックに様々な大小関係で依存することがあり、この文脈化が、「デジタル」ルールセット形式の範囲内でルールが有するミラー化された相互関係を補足するために使用される、メトリックコンテキスト分析と、
ｋ）ルール構文形式変換（ＲＳＦＣ）であって、ルール構文形式（ＲＳＦ）の構文に従うように、ルールを仕訳け、分割し、直感的決定は、パーセプションを活用することを通じてクリティカルシンキングに携わり、思考的決定は、ルールを活用することを通じてクリティカルシンキングに携わり、パーセプションは、内部形式で定義された形式構文にしたがって、直感的決定から受信したデータであり、充足ルールが、思考的決定から受信したデータで、前記ＲＥからの充足可能なルールセットの集合であり、前記データが、内部形式で定義されている形式構文に則って渡される、ルール構文形式変換をさらに備え、
処置は、既に実行されているかもしれない、実行するかもしれない処置を示し、起動のために考慮されており、プロパティは、何か他のものを記述する何らかのプロパティのような属性を示し、処置、条件、または目的であり、条件は、論理演算または演算子を示し、目的は、それに適用される属性を有することができる標的を示し、
分割ルールフォーマットは、メモリ認識前段階と見なされている、ルール文法フォーマット分割（ＲＳＦＳ）からの出力として使用され、そして、メモリ認識後段階と見なされている、メモリ認識（ＭＲ）からの出力として使用される、請求項３６に記載のシステム。

【請求項３８】
ａ）乱雑フィールドパース（ＣＦＰ）であって、複数のログのフォーマットを、単一のスキャン可能な乱雑フィールドに合成する、乱雑フィールドパースと、
ｂ）追加ルールであって、前記妥当ルールを補足するために、メモリ認識（ＭＲ）から生成される、追加ルールをさらに備え、
パーセプションマッチング（ＰＭ）の内部で、メトリック統計は、パーセプションストレージからの統計情報を提供し、エラー管理は、個々のメトリックのいずれかから生ずる構文エラーおよび／または論理的エラーをパースし、個々のメトリックは、入力パーセプションであった単一のユニットに合成されていたため、個々のメトリックを分離し、ノード比較アルゴリズム（ＮＣＡ）は、２つ以上のＣＶＦのノード構成を受信し、ＣＶＦの各ノードはプロパティの大小を表しており、個々のノードごとに、類似度比較が行われ、総合分散が計算され、分散の数値が小さい場合は、一致度が高いことを表している、請求項３７に記載のシステム。
【請求項３９】
ａ）未処理パーセプション-直感的思考（アナログ）であって、「アナログ」形式にしたがってパーセプションを処理し、前記決定に関係するアナログ形式のパーセプションは、段差のない滑らかな曲線の勾配で格納されている、未処理パーセプション-直感的思考と、
ｂ）未処理ルール-論理的思考（デジタル）であって、「デジタル」形式にしたがってルールを処理し、前記決定に関係するデジタル形式の未処理ルールは、「あいまいな領域」が皆無かそれに近いステップ単位で格納されている、未処理ルール-論理的思考をさらに備え、
未充足ルールは、それらの論理的な依存性にしたがって乱雑フィールド内で十分に認識されていないルールセットであり、充足ルールは、その論理的な依存関係にしたがって、乱雑フィールドで十分に利用可能であると認識されているルールセットであり、
キュー管理（ＱＭ）は、構文的関係再構築（ＳＲＲ）を利用して、個々の部分を最も論理的な順序で分析し、メモリ認識（ＭＲ）の結果にアクセスすることができ、それによって、バイナリのイエス／ノーフロー質問に答えることができ、適切な処置をとることができ、ＱＭは、すべてのルールセグメントを段階的にチェックし、単一のセグメントが乱雑フィールドから欠落し、他のセグメントと適切な関係にない場合、ルールセットは未充足であるとフラグされる、請求項３８に記載のシステム。
【請求項４０】
シーケンシャルメモリ編成は、順番に並べられた情報の「チェーン」のための、最適化された情報ストレージであり、メモリアクセスポイントでは、ノード（ブロック）のそれぞれの幅は、記憶されたオブジェクト（ノード）への観察者の直接到達性を表しており、到達性の範囲では、各文字は、観察者への直接メモリアクセスのポイントを表し、より広い到達性の範囲は、シーケンスノードごとにより多くの到達ポイントが存在し、「順番に」のみ参照され、ランダムに選択されたノードからは参照されないシーケンス長くなるほど、到達性の範囲はより狭くなり（シーケンスサイズとの比較で）、ネストされたサブシーケンスレイヤでは、強い不均一性を示すシーケンスは、相互接続している一連のより短いサブシーケンスで構成されている、請求項３９に記載のシステム。
【請求項４１】
非シーケンシャルメモリ編成は、非シーケンシャルに関連する項目の情報ストレージを扱い、可逆性が、非シーケンシャルな配置と均一なスコープを示す様子を示し、非シーケンシャルな関係が、ノードごとに比較的広いアクセスポイントによって示され、同様の均一性は、ノードの順序がシャッフルされるときに存在し、核となる話題および関連性では、同じ一連のノードが、異なる核（中心のオブジェクト）を除いて繰り返され、この核は、核となる話題が定義されていない場合とは対照的に、残りのノードがより容易にアクセスできるメモリの近隣として機能する、主たる話題を表している、請求項３９に記載のシステム。

【請求項４２】
メモリ認識（ＭＲ）は、既知のコンセプトを認識するために乱雑フィールドをスキャンし、乱雑フィールドは、「ホワイトノイズ」の情報内に任意に潜んでいるコンセプトの「フィールド」であり、メモリコンセプト保持は、フィールド検査のためにインデックス付けおよび参照される準備が整った、認識可能なコンセプトを格納し、３文字スキャナは、乱雑フィールドをスキャンし、ターゲットに対応する３文字セグメントに対してチェックを行い、５文字スキャナは、乱雑フィールドをスキャンし、ターゲットに対応する５文字セグメントに対してチェックを行うが、今度は、フィールド全体にわたってすべての進歩によってチェックされるセグメントは、単語全体であり、乱雑フィールドは、異なる比率でスキャンするように分割され、スキャンの範囲が狭くなるにつれて、精度が向上し、スキャナのフィールド領域が増加するにつれて、より大きい文字スキャナは、精度を犠牲にして認識を実行するので、より効率的になり、メモリコンセプトのインデックス付け（ＭＣＩ）が、未処理のメモリコンセプトが残っていることに応答して、スキャナのサイズを切り替え、ＭＣＩは利用可能なスキャナの中で最大のものから始め、徐々に減少し、それにより、より多くのコンピューティングリソースが発見され、より小さなメモリコンセプトターゲットの存在可能性をチェックすることができる、請求項３９に記載のシステム。
【請求項４３】
フィールド解釈ロジック（ＦＩＬ）は、文字幅の様々な複数のスキャナを管理するロジスティクスを実行し、汎用スコープスキャンが、大型の文字スキャンからロジックを始め、小規模なスケールでの精度を犠牲にしてフィールドの大規模なスコープを少ないリソースで精査し、詳細スコープスキャンは、重要なエリアが特定され、そこに「ズームイン」する必要のある場合に用いられ、それによって、冗長で生産性のない場所では、高コストな高精度のスキャンは用いられないことが保証され、乱雑フィールドでメモリコンセプトの追加の認識を受け取ることは、フィールドスコープが高密度飽和のメモリコンセプトを含むことを示している、請求項３９に記載のシステム。
【請求項４４】
自動化パーセプション発見メカニズム（ＡＰＤＭ）では、パーセプション視点は、スコープ、種別、強度、および一貫性を含む、複数のメトリックによって構成されており、これらのメトリクスは、全体的なパーセプションを構成する複数のパーセプションの側面を定義しており、創作モジュールは、パーセプションの複雑なバリエーションを生成し、パーセプションウェイトは、ＰＯＥによってエミュレートされている間に、パーセプションがどの程度の相対的な影響を有するかを定義しており、両方の入力パーセプションのこの重みは、新しくイテレートされたパーセプションの重みを定義しつつ検討しており、以前の世代のパーセプションから影響を受けた、ハイブリッド化されたメトリックを含む、請求項３９に記載のシステム。
【請求項４５】
ＣＶＦＧの入力は、データバッチであり、生成されたＣＶＦのノード構成によって表されなければならないデータを表している、データの任意の集合であり、データバッチによって定義された個々のユニットのそれぞれをシーケンシャルに使用し、データユニットは、ノードフォーマットに変換され、最終のＣＶＦによって参照されるのと同じ構成の情報を有し、このように変換されたノードは、ステージでそれらの存在をチェックすると、ノードホールドアウトに一時的に格納され、それらが見つからなければ、それらは作成され、発生および使用を含む統計情報で更新され、ホールドアウトを有するすべてのノードが組み立てられ、ＣＶＦとして、モジュールの出力としてプッシュされる、請求項３９に記載のシステム。
【請求項４６】
ノード比較アルゴリズムは、未処理のＣＶＦから読み取られた２つのノード構成を比較し、部分一致モード（ＰＭＭ）では、１つのＣＶＦにアクティブノードがあり、それが比較候補に見つからない（ノードが休止状態である）の場合、この比較にはペナルティが課されず、全部一致モード（ＷＭＭ）では、１つのＣＶＦにアクティブノードがあり、それ

が比較候補に見つからない（ノードが休止状態である）の場合、この比較にはペナルティが課される、請求項３９に記載のシステム。
【請求項４７】
システムメタデータ分割（ＳＭＳ）は、入力システムメタデータを、意味のあるセキュリティ上の因果関係に分割し、サブジェクトスキャン／吸収により、カテゴリ化モジュールからの事前分類コンテナおよび未処理分析結果を使用して、システムメタデータからセキュリティ状況の対象／疑いが抽出され、対象は、セキュリティ応答／変数の関係を導出するための主な参照点として使用され、リスクスキャン／吸収により、セキュリティ状況のリスク要因が、事前に作成された分類コンテナおよび分類モジュールからの未処理分析結果を使用して、システムメタデータから抽出され、リスクは、そのようなリスクを呈している、またはリスクにさらされているターゲットとなる対象に関連しており、応答スキャン／吸収により、カテゴリ化モジュールからの事前に作成された分類コンテナおよび未処理分析結果を使用して、システムメタデータから、入力アルゴリズムによって生成されたセキュリティ状況の応答が抽出され、この応答は、そのような応答に値するとされるセキュリティ対象に関連付けられている、請求項３９に記載のシステム。
【請求項４８】
ＭＣＭでは、フォーマット分割が、メタデータを認識されたフォーマットのルールおよび構文に従って分離し、分類し、ローカルフォーマットルールおよび構文は、ＭＣＭモジュールが予めフォーマットされたメタデータストリームを認識できるようにするための定義を含み、デバッグ追跡は、使用される変数、関数、メソッドおよびクラス、およびそれぞれの入力および出力変数の種別／内容を提供するコーディングレベルのトレースであり、アルゴリズム追跡は、アルゴリズム分析結果と結合されたセキュリティデータを提供するソフトウェアレベルのトレースであり、結果としてのセキュリティ決定（許可／ブロック）は、その決定（正当化）にどうやって到達したかの道筋と、各要素がそのセキュリティ決定を行うのに貢献した適切な重みと一緒に提供される、請求項３９に記載のシステム。
【請求項４９】
メトリック処理（ＭＰ）において、セキュリティ応答Ｘは、ＳＰＭＡにより選ばれる結果としてのセキュリティ応答に寄与する一連のファクタを表し、初期ウェイトはＳＰＭＡによって決定され、パーセプション推論（ＰＤ）は、このセキュリティ応答の一部と、これに対応するシステムメタデータを使用して、セキュリティ応答の元のパーセプションを再現し、多次元型シリーズのパーセプション解釈は、ＰＤがＳＰＭＡのセキュリティ応答を採用して、該当する入力システムメタデータに関連付けすることで、ＳＰＭＡが元々使用しているとおりの知的「デジタルパーセプション」のフルスコープを再生成する様子を表しており、塗り潰し図形、積み上げ量、および多次元型は、知的アルゴリズムの「考え方」をうまく捉えるデジタルパーセプションである、請求項３９に記載のシステム。
【請求項５０】
前記ＰＤでは、セキュリティ応答Ｘは根拠／理由付けの算出への入力として転送され、根拠／理由付けの算出、入出力削減（ＩＯＲ）モジュールの意図の供給を活用することによって、ＳＰＭＡのセキュリティ応答の正当化を決定し、前記ＩＯＲモジュールは、メタデータにリストされたさまざまな関数呼び出しの分割された入出力を使用し、前記メタデータ分割は前記ＭＣＭによって実行される、請求項４９に記載のシステム。
【請求項５１】
ＰＯＥについて、入力システムメタデータは、未処理パーセプション生成（ＲＰ２）によって、ＣＶＦでパーセプションを生成するために使用される初期入力であり、ストレージ検索（ＳＳ）では、データ拡張ログから導出されたＣＶＦ（比較可能可変フォーマット）が、パーセプションストレージ（ＰＳ）のデータベース検索における判定基準として使用され、格付けでは、パーセプションは最終的なウェイトに応じて順序付けられ、データ拡張ログがパーセプションに適用されて、ブロック／許可の推奨を生成し、前記ＳＣＫＤは、未知の知識の期待される上限スコープを定義するために、ログをタグ付けし、データ

パースは、オリジナルのＳＰＭＡによって決定されたオリジナルの許可またはブロックの決定を出力するために、データ拡張ログおよび入力システムメタデータの基本解釈を行い、ＣＴＭＰは、前記ＰＯＥではパーセプションにしたがって決定事項を批判し、ルール実行（ＲＥ）においては、論理的に定義されたルールにしたがって決定事項を批判する、請求項３９に記載のシステム。

【請求項５２】

メトリックの複合度では、円の外側の境界は、個々のメトリックに関する既知の知識のピークを表し、円の外縁に向かうにつれて、メトリックの複雑さがより大きいことを表し、一方、中心はメトリックの複雑さがより小さいことを表し、中央の明るい灰色は、現在のひとまとまりの適用済パーセプション観点のメトリック合成を表し、外側の濃い灰色は、システムによって格納され、一般に知られているメトリックの複合度を表し、ＩＤのゴールは、関連するメトリックの複合度を増やし、それによってパーセプション観点に複合度と量を掛けることができるようになることであり、暗い灰色の表面積は、現在のひとまとまりの適用済パーセプション観点の全範囲と、既知の上限に応じて残されたスコープの量を表し、拡張され複合度が高められると、メトリックはメトリックの複合度として戻され、メトリックの複合度は、メトリック変換の入力として渡され、メトリック変換は、個々のパーセプション観点から全体のパーセプション観点に戻し、それによって、最終出力が、意味付けられたパーセプション観点として組み立てられる、請求項３６に記載のシステム。

【請求項５３】

ＳＣＫＤについて、既知データカテゴリ化（ＫＤＣ）は、既知の情報を入力からカテゴリ的に分割して、適切なＤＢアナロージークエリを実行することができるようにし、情報をカテゴリに分割し、前記分割されたカテゴリは個別に入力をＣＶＦＧに提供し、ＣＶＦＧは、ＣＶＦフォーマットのカテゴリ情報を出力し、これは、ストレージ検索（ＳＳ）によって既知データスコープＤＢにおいて類似性をチェックするために使用され、ＳＳの結果にしたがって既知のデータの該当するスコープが各カテゴリにタグ付けされ、カテゴリ毎の未知の情報のタグ付けされたスコープは、未知データ合成器（ＵＤＣ）でオリジナルの入力の同じストリームに再構築される、請求項３９に記載のシステム。

【請求項５４】

前記コンピュータ実装システムは、辞書的客観性探索（ＬＯＭ）であり、

ａ）初期クエリ推論（ＩＱＲ）であって、質問が転送され、知識保持中枢（ＣＫＲ）を活用して質問の理解および回答／応答においてなくてはならない、欠落した詳細情報を解読するに、処理のために転送される、初期クエリ推論と、

ｂ）調査の明確化（ＳＣ）であって、前記質問および補足質問データが転送され、人間である対象から入力を受け取り、人間である対象に出力を送信し、明確化された質問／表明を形成する、調査の明確化と、

ｃ）表明の構築（ＡＣ）であって、表明または質問の形式で命題を受け取り、その命題に関連するコンセプトの出力を提供する、表明の構築と、

ｄ）回答の提示であって、ＡＣによって引き出された結論を、人間である対象と合理的訴求（ＲＡ）の両方に提示するためのインタフェースである、回答の提示と、

ｅ）階層的マッピング（ＨＭ）であって、関連するコンセプトをマップして、質問／表明の一貫性において、裏付けまたは競合を発見し、話題に一定の立場をとっていることの利点とリスクを計算する、階層的マッピングと、

ｆ）知識保持中枢（ＣＫＲ）であって、ＬＯＭのために知識を参照するためのメインデータベースである、知識保持中枢と、

ｇ）知識検証（ＫＶ）であって、クエリ能力およびＣＫＲへの吸収のために論理的に分割される必要がある、高い確信度および事前批判された知識を受け取る、知識検証と、

ｈ）応答の受け入れであって、ＬＯＭの応答を受け入れるか、批判とともに訴求するかのいずれかを行う、人間である対象に与えられた選択肢であり、応答が受け入れられた場合、それはＫＶによって処理され、確認された（高い確信度の）知識としてＣＫＲに格納

でき、人間である対象が応答を受け入れなければ、人間によって与えられた訴求の理由をチェックして批判する、前記ＲＡに転送される、応答の受け入れと、

ｉ）管理された人工知能的サービスプロバイダ（ＭＡＩＳＰ）であって、ＣＫＲのマスターインスタンスとともに、ＬＯＭのインターネットクラウドインスタンスを実行し、ＬＯＭをフロントエンドサービス、バックエンドサービス、サードパーティアプリケーションの依存関係、情報源、およびＭＮＳＰのクラウドに接続する、管理された人工知能的サービスプロバイダをさらに備える、請求項１に記載のシステム。

【請求項５５】

フロントエンドサービスは、人工知能的パーソナルアシスタント、通信アプリケーションおよびプロトコル、ホームオートメーション、および医療用途を含み、バックエンドサービスには、オンラインショッピング、オンライン交通機関、処方箋注文があり、フロントエンドサービスおよびバックエンドサービスは、情報の転送およびプロトコルの標準化を可能にする、文書化されたＡＰＩインフラストラクチャを介してＬＯＭと相互作用し、ＬＯＭは、自動化された調査機構（ＡＲＭ）を介して外部情報源から知識を取り出す、請求項５４に記載のシステム。

【請求項５６】

言語学的構築（ＬＣ）は、人間である対象および類似したモジュールからの未処理の質問／表明の入力を解釈し、言語構文の論理的な分割を生成し、コンセプト発見（ＣＤ）は、明確化された質問／表明内の関心ポイントを受け取り、ＣＫＲを活用することによって関連するコンセプトを導出し、コンセプトの優先順位付け（ＣＰ）は、該当するコンセプトを受け取り、それらを特定性および一般性を表す論理的な複数の層に整理し、応答分割ロジック（ＲＳＬ）は、ＬＣを活用することで人間の応答を理解し、適切かつ有効な応答を、最初の明確化リクエストと関連づけ、それによって、ＳＣの目的を達成し、ＬＣは、出力フェーズで再活用され、オリジナルの質問／表明を修正し、ＳＣによって受信された補足的情報を含むようにし、コンテキスト構築（ＣＣ）は、表明の構築（ＡＣ）のメタデータと、人間である対象からの証拠を使用して、クリティカルシンキングのためにＣＴＭＰに未処理の事実を提供し、決定事項比較（ＤＣ）は、事前批判された決定事項と批判された後の決定事項との間の重複を判断し、コンセプト互換性検出（ＣＣＤ）は、オリジナルの質問／表明からのコンセプト的な派生事項を比較して、論理的な互換性の結果を確認し、利益／リスク計算（ＢＲＣ）は、ＣＣＤからの互換性の結果を受け取り、コンセプト構成に暗に含まれた変数の傾斜を包含する一様な決定を形成するために、利益とリスクを重み付けし、コンセプト連携（ＣＩ）は、ＡＣのコンセプトに関連する属性を、調査の明確化（ＳＣ）を介して、人間である対象から収集された情報の一部に割り当てる、請求項５５に記載のシステム。

【請求項５７】

前記ＩＱＲの内部では、ＬＣは前記オリジナルの質問／表明を受け取り、質問／表明は言語的に分離されているおり、ＩＱＲはＣＫＲを活用して一度に個々の語句を処理し、ＣＫＲを参照することで、ＩＱＲは、単語／フレーズの曖昧性を考慮しながら、可能な選択肢の候補を考慮する、請求項５６に記載のシステム。

【請求項５８】

調査の明確化（ＳＣ）はＩＱＲ８０２からの入力を受け取り、前記入力には、達成されるべきオリジナルの質問／表明に対する客観的な回答のために、人間の被験者が対応することになる、一連のリクエストされた明確化事項が含まれ、前記明確化事項に対してなされる対応はどれも、応答分割ロジック（ＲＳＬ）に転送され、対応と明確化リクエストを相関させ、リクエストされた明確化事項と並行して、明確化の言語学的連携がＬＣに提供され、前記連携には、リクエストされた明確化事項と言語構造との内部関係が含まれ、この内部関係によって前記ＲＳＬが前記オリジナルの質問／表明を修正でき、それによって、ＬＣが前記明確化された質問を出力する、請求項５６に記載のシステム。

【請求項５９】

前記明確化された質問／表明を受け取った、表明の構築について、ＬＣは、この問題を

関心ポイントに分解し、コンセプト発見に渡し、ＣＤは、ＣＫＲを活用することによって関連するコンセプトを導出し、コンセプトの優先順位付け（ＣＰ）はコンセプトを論理的な複数の層に整理し、最上位層には最も一般的なコンセプトが割り当てられ、より下位の層にはより特定のコンセプトが割り当てられ、最上位層は、モジュールの入力として階層的マッピング（ＨＭ）に転送され、情報の並列転送において、ＨＭは関心ポイントを受信し、この関心ポイントは、その依存モジュールであるコンセプト連携（ＣＩ）によって処理され、ＣＩは、ＣＫＲでインデックス付けされた情報にアクセスすることによって、そのような関心ポイントに属性を割り当て、ＨＭが内部プロセスを完了すると、その最終出力は、導出されたコンセプトの互換性がテストされ、ある立場の利益／リスクが重み付けされて返された後、ＡＣに返される、請求項５６に記載のシステム。

【請求項６０】

ＨＭについて、ＣＩは、２つのコンセプト同士の互換性／競合レベルを識別する、ＣＣＤへの入力を提供し、このような互換性／競合データは、問題について全体論的な統一された立場を取ることに関する、前記互換性と競合を利益とリスクに変換する、ＢＲＣに転送され、そのような立場は、リスク／利益ファクタとともに、モジュールの出力としてＡＣに転送され、情報フローのループを含むシステムは、知性の傾向が、質問／表明の主観的性質として徐々に補足される、徐々に構築された客観的応答、を表しており、ＣＩは、関心ポイントを受け取り、優先順位付けられたコンセプトの最上位層にしたがって、それぞれの関心ポイント解釈する、請求項５９に記載のシステム。

【請求項６１】

ＲＡについて、コアロジックは言語テキストを処理し、結果を返し、前記結果が高い確信度の場合、前記結果はＣＫＲへの適切な吸収のために知識検証（ＫＶ）に渡され、前記結果が低い確信度の場合、前記結果はＡＣへ渡され、の適切な吸収のために知識検証（ＫＶ）に渡され、自己批評のサイクルを継続し、コアロジックは、言語要素のない事前批判された決定としてＬＣからの入力を受け取り、前記決定は主観的意見としてＣＴＭＰに転送され、決定はまた、ＡＣからのメタデータおよび人間である対象からの見込みのある証拠を使用して、未処理の事実をＣＴＭＰに、入力する「客観的事実」として与える、コンテキスト構築（ＣＣ）に転送され、ＣＴＭＰが２つの必須入力を受け取ると、このような情報は「客観的意見」に到達する最良の試みを出力するために処理され、前記意見は、ＲＡ内で、批判された後の決定として取り扱われ、事前批判された決定と批判された後の決定の両方が、両方の決定の間の重複のスコープを決定する決定事項比較（ＤＣ）に転送され、前記不服申し立ては、次に、真実であると認められるか、この訴求が無効である理由を説明するために、対照的要素が改善され、シナリオを認めるのか改善するのかとは無関係に、高い確信度の結果８４６はＫＶに渡され、低い確信度の結果はさらなる分析のためにＡＣ８０８に渡される、請求項５６に記載のシステム。

【請求項６２】

ＣＫＲについて、情報の単位は、単位知識フォーマット（ＵＫＦ）に格納され、ルール構文形式（ＲＳＦ）は、参照ルールの追跡を維持するための構文的標準のセットであり、ＲＳＦ内の複数のルールの単位を利用して、単一の目的または処置を記述することができ、ソース属性は、要求された情報源を追跡する複合データの集合であり、ＵＫＦクラスタは、管轄区域的に分割された情報を定義するためにリンクされたＵＫＦの変種の連鎖で構成されており、ＵＫＦ２には、メインのターゲットされた情報が含まれており、ＵＫＦ１にはタイムスタンプ情報が含まれているため、無限回帰を避けるためにタイムスタンプフィールドそのものは省略されており、ＵＫＦ３にはソース属性情報が含まれているため、無限回帰を避けるためにソースフィールドそのものは省略されており、すべてのＵＫＦ２には少なくとも１つのＵＫＦ１と１つのＵＫＦ３が添付されていなければならない。さもなければ、クラスタ（シーケンス）は不完全とみなされ、そこにある情報は、ＬＯＭシステム全体の汎用ロジックでは処理できず、中央のＵＫＦ２とそれに対応するＵＫＦ１およびＵＫＦ３の間には、リンクされた橋の役割を果たすＵＫＦ２ユニットがあり、一連のＵＫＦクラスタはＫＣＡによって処理され、導出された表明を形成し、知識裏付け分析（Ｋ

ＣＡ）は、ＵＫＦのクラスタ化された情報を、意見のあるスタンスに関する証拠を裏付けるために比較し、ＫＣＡの処理が完了した後、ＣＫＲは、話題についての結論となる、独断的な立場を出力することができる、請求項５６に記載のシステム。

【請求項６３】

ＡＲＭについて、ユーザ活動で表されるように、ユーザがＬＯＭと対話するとき、コンセプトは質問／表明に対する回答／応答に関連して直接的または間接的にもたらされ、ユーザ活動は、リクエストされたがまだ利用不可能なコンセプトのリストに示されるように、ＣＫＲが、それに関する情報がほとんど全くないコンセプトを最終的に生み出すことが期待され、コンセプトのソートおよび優先順位付け（ＣＳＰ）では、コンセプトの定義は、３つの独立したソースから受信され、情報リクエストのリソースに優先順位付けをするために集約され、前記情報源によって提供されたデータは、それらをリクエストしたコンセプトの定義にしたがって情報アグリゲータ（ＩＡ）で受信され、解析さかれ、該当するメタデータは保持され、情報は相互参照分析（ＣＲＡ）に送られ、そこでは、受信された情報がＣＫＲからの既存の知識と比較され、それを考慮して構築される、請求項５６に記載のシステム。

【請求項６４】

個人情報プロファイル（ＰＩＰ）は、多数の潜在的なエンドポイントおよびフロントエンドを介して個々人の個人情報が格納される場所であり、個々人の情報はＣＫＲからは隔離されているが、ＬＯＭシステム全体にわたる汎用ロジックでは使用可能であり、人工知能アプリケーションに関する個人情報は暗号化され、ＵＫＦフォーマットのパーソナルＵＫＦクラスタプールに格納され、情報匿名化プロセス（ＩＡＰ）では、情報は、個人を特定可能な情報が取り除かれた後、ＣＫＲに補充され、相互参照分析（ＣＲＡ）では、受信した情報は、ＣＫＲからの既存の知識と比較され、それを考慮して構築される、請求項５６に記載のシステム。

【請求項６５】

生活の管理と自動化（ＬＡＡ）は、一体化プラットフォーム上で、様々なインターネット対応の機器およびサービスと接続し、積極的意思決定（ＡＤＭ）は、フロントエンドサービス、バックエンドサービス、ＩｏＴデバイスの可用性と機能性を考慮し、ＦＡＲＭにしたがって利用可能な支出ルールと金額を考慮しており、ＦＡＲＭは、人間が前記モジュールに対する判断基準、制限、およびスコープを手作業で定義して、ＡＤＭ８１３Ｄの活動の管轄範囲がどこまでかということについて、ＡＤＭ８１３Ｄに知らせ、暗号通貨での資金がデジタルウォレットに預けられ、ＩｏＴ連携モジュール（ＩＩＭ）は、どのＩｏＴデバイスが利用可能であるかについてのデータベースを維持管理し、データフィード８６２Ｂは、ＩｏＴ対応デバイス８６２ＡがＬＡＡ８１２Ｄに情報を送信するときを表す、請求項５６に記載のシステム。

【請求項６６】

前記システムは、ユーザからの、個人を識別可能なデータのリクエストをモニターすることで、非倫理的および／または違法な物質の有無をチェックする挙動監視（ＢＭ）をさらに備え、メタデータ集約（ＭＤＡ）では、ユーザ関連データが外部サービスから集約され、ユーザのデジタル上の身元を明らかにすることができ、このような情報が、帰納／演繹、最終的にはＰＣＤに転送され、そこでは洗練された分析がＭＮＳＰからの裏付けファクタを用いて実行され、ＰＩＰが宛先である、認証済みのユーザからのすべての情報は、情報トラッキング（ＩＴ）を通過し、挙動ブラックリストに照らしてチェックされ、未然犯罪検知（ＰＣＤ）では、未然犯罪の結論を出すために、演繹的情報および帰納的情報がマージされ分析され、ＰＣＤは、挙動ブラックリストを直接参照するＣＴＭＰを利用することで、帰納および演繹によって生成された立場を検証し、ブラックリスト管理機関（ＢＭＡ）は、ＭＮＳＰのクラウドサービスフレームワーク内で稼働する、請求項５４に記載のシステム。

【請求項６７】

ＬＯＭは、ある個人の生活でパーソナライズされたポートフォリオを管理するように構

成され、ＬＯＭは最初の質問を受け取り、ＬＯＭの内部審議プロセスを介して結論に至り、ＬＯＭは、ＬＯＭがそこからデータを受信して制御できるインターネット対応デバイスに接続するＬＡＡモジュールに接続し、文脈化では、ＬＯＭは申し立てを構成する際に欠落しているリンクを推論し、ＬＯＭはそのロジックにより、オリジナルの表明によって提起されたジレンマを解決するために、この状況に関するある変数をまず知るか仮定するかしなければならないということを解読する、請求項６５に記載のシステム。

【請求項６８】

前記コンピュータ実装システムは、線形量子情報転送（ＬＡＱＩＴ）であり、

ａ）論理的に構築された構文により、再帰的に一貫したカラーシーケンスを繰り返し、

ｂ）英語のアルファベットで翻訳を行うために、前記シーケンスを再帰的に使用し、

アルファベットの「ベース」レイヤを構築するとき、前記カラーシーケンスは、カラーチャネルでは、短縮された不均一なウェイトで使用され、構文定義のために残されているスペースは、将来の潜在的な使用および拡張のために予約されており、

複雑なアルゴリズムが、ＬＡＱＩＴを使ってそのログイベントおよびステータスレポートを報告し、ログイベントおよびステータスレポートは自動的に生成され、前記ステータスレポート／ログレポートを、可搬なテキストベースのＬＡＱＩＴ構文へと変換し、構文的に安全出ない情報はデジタル的に転送され、前記可搬なテキストベースの構文は、非常に読みやすいＬＡＱＩＴの可視構文（線形モード）へ変換され、鍵が人間の記憶に対して最適化されていて、比較的短い図形のシーケンスに基づいており、

局所的に安全でないテキストが送信者によって入力され、受信者に手出され、前記テキストが、可搬な暗号化されたテキストベースのＬＡＱＩＴ構文へと変換され、構文的に安全な情報はデジタル的に転送され、前記データが、可視的に暗号化されたＬＡＱＩＴ構文へと変換され、

インクリメンタル認識効果（ＩＲＥ）が情報伝達のチャネルであり、情報が完全に伝達される前に、情報の単位の完全な形を認識し、この予測可能インデックスの効果が、単語から単語への遷移を表示することによって組み込まれており、近似認識効果（ＰＲＥ）は情報伝達のチャネルであり、壊れているか、混ざっているか、あるいは変更されているかのいずれかであっても、情報の単位の完全な形を認識する、請求項１に記載のシステム。

【請求項６９】

ＬＡＱＩＴの線形モードでは、ブロックは線形モードの「基本レンダリング」バージョンを示し、ポイントは、暗号化の欠如を表示しており、単語セパレータでは、前記図形の色は単語に続く文字を表し、単語と次の単語との間の区切りとして機能し、単一ビューゾーンは、より大きな文字、したがってより少ない情報をともなう、小さなビューゾーンを組み込み、二重ビューゾーンには、ピクセル当たりより多くのアクティブ文字が存在し、陰影カバーは、観察者の主なフォーカスがビューゾーン上にあるように、入って来る文字および外に出て行く文字を曇らせる、請求項６８に記載のシステム。

【請求項７０】

広範囲の暗号化レベルが可能な原子モードにおいては、ベースの主なキャラクタ参照は、どの文字が定義されているかについて一般原理を指定し、キッカーは、ベースと同じ色の範囲で存在し、特定の文字を正確に定義し、読み取り方向では、情報伝達の読み取りは、軌道輪１の頂上にある正方形から始まり、一度軌道輪が完結すると、次の軌道輪の頂上にある正方形から読み込みが続けられ、入口／出口ポータルは、キャラクタ（そのベース）の生成と破壊のポイントであり、該当する軌道に属する、新しいキャラクタが、ポータルから現れ、時計回りにその位置にスライドし、原子核は、その単語に続くキャラクタを定義し、

ワードナビゲーションでは、各ブロックは、画面の左側に単語全体（あるいは、複数の単語を分子モードで）を表しており、ある単語が表示されると、それぞれのブロックが外側に右の方に移動し、その単語が完成するとブロックは後退し、ナビゲーションブロックの色／形は、この単語の最初の文字のベースと同じ色／形であり、センテンスナビゲーションでは、各ブロックは単語のクラスタを表しており、クラスタとは、単語ナビゲーショ

ンペインに収まる最大量の単語であり、原子状態生成は、インクリメンタル認識効果（ＩＲＥ）を誘発する遷移であり、このような遷移により、ベースは入口／出口ポータルから現われ、それらのキッカーは隠され、時計回りに移動してそれらの位置を占め、原子状態拡張は、近似認識効果（ＰＲＥ）を誘発する遷移であり、一度ベースがその位置に達すると、それらのベースは情報状態提示の「拡張」シーケンスにおいて外側に移動し、これにより、キッカーが明らかになり、それによって、情報状態の特定の定義を提示することができ、原子状態破壊は、インクリメンタル認識効果（ＩＲＥ）を誘発する遷移であり、キッカーを再び覆うために、ベースは後退しており（拡張シーケンスを逆転して）、ベースは時計回りにスライドして入口／出口ポータルに達している、請求項６８に記載のシステム。

【請求項７１】

図形難読化では、標準の四角形が５つの視覚的に区別できる図形に置き換えられ、構文内の図形の分散は、原子プロファイルの戦略的ポイントにダッド（偽物）文字を挿入することを可能にし、ダッド文字はメッセージの本当の意図された意味を難読化させ、文字が真であるか偽かを解読することは、安全かつ一時的に転送された解読鍵によって行われ、

リダイレクトボンドでは、ボンドが２つの文字を結合し、読み込みの流れを変更し、典型的な時計回りの読み込みパターンから始まり、合法／非偽の文字を打ち上げ（始まって）着地する（終わる）ボンドに遭遇すると、読み込みパターンを変更して着地文字を再開し、

放射性元素では、文字が偽物であるか否かの評価を覆すことができるいくつかの要素は「音を立てる」ことができ、図形は暗号化で使用可能な図形を示しており、中心要素は、単語の直後に来るキャラクタを定義する、軌道の中心要素を示している、請求項７０に記載のシステム。

【請求項７２】

リダイレクトボンドでは、ボンドは「打ち上げ」文字から始まり、「着地」文字で終わり、どちらの文字も、ダッドであってもなくてもかまわなく、それらのいずれもがダッドでない場合、ボンドは読み取り方向および位置を変更し、片方または両方がダッドである場合、ボンド全体を無視しなければならず、さもなければ、メッセージが正しく解読されず、ボンドキー定義では、情報状態の読み取りの際にボンドに従わなければならない場合、それは、暗号鍵で具体的に定義されているかどうかによって異なる、請求項７１に記載のシステム。

【請求項７３】

シングルクラスタでは、両方の隣接ノードが非放射性であるため、クラスタのスコープが定義され、キーは二重クラスタを有効と指定しているため、前記要素は、それがそもそも放射性でない場合に処理され、ダブルクラスタでは、キー定義はダブルクラスタを活性と定義するため、他のすべてのサイズのクラスタは、メッセージを復号化している間、休止状態であるとみなされ、正しくない解釈は、インタプリタがダブルクラスタを逆順シーケンス（偽陽性）として扱わなかった様子を示している、請求項７１に記載のシステム。

【請求項７４】

分子モードでは、暗号化およびストリーミングが可能であり、秘密辞書攻撃抵抗では、メッセージの誤った解読は、「赤いニシン」という別のメッセージにつながり、分子ごとに複数のアクティブワードを用い、単語は分子プロシージャの間に並行して提示され、これによって、表面積比当たりの情報を増加させるが、一貫した移行速度であり、バイナリおよびストリーミングモードはストリーミングモードを示し、典型的な原子構成では読み取りモードはバイナリであり、バイナリモードは、中心要素が単語に続くキャラクタを定義することを示しており、ストリーミングモードに準拠した暗号化が有効になっている場合を除いて、分子モードもまたバイナリであり、ストリーミングモードは、軌道内で特殊文字を参照する、請求項７１に記載のシステム。

【請求項７５】

前記コンピュータ実装システムは、ベース接続協調攻撃統合ノード（ＢＣＨＡＩＮ）を

伴った普遍的ＢＣＨＡＩＮ全接続（ＵＢＥＣ）であり、
ａ）通信ゲートウェイ（ＣＧ）であって、ＢＣＨＡＩＮノードが、そのハードウェアインタフェースと対話し、その後、他のＢＣＨＡＩＮノードとの通信に至るための、主要なアルゴリズムである、通信ゲートウェイと、
ｂ）ノード統計調査（ＮＳＳ）であって、リモートノードの挙動パターンを解釈する、ノード統計調査と、
ｃ）ノードエスケープインデックスであって、隣接ノードが知覚ノード近傍を回避する可能性を追跡する、ノードエスケープインデックスと、
ｄ）ノード飽和インデックスであって、知覚ノードの検出範囲内にあるノードの量を追跡する、ノード飽和インデックスと、
ｅ）ノード一貫性インデックスであって、知覚ノードによって解釈された、ノードサービスの品質を追跡し、高いノード一貫性インデックスは、周囲の隣接ノードがより多くの可用性稼働時間およびパフォーマンスの一貫性を有する傾向があることを示し、２つの目的で用いられるノードは、一貫性インデックスが低くなる傾向があり、ＢＣＨＡＩＮネットワーク専用のノードは、高い値を示す、ノード一貫性インデックスと、
ｆ）ノードオーバーラップインデックスであって、知覚ノードによって解釈される、ノード同士の互いの重複の量を、互いに追跡する、ノードオーバーラップインデックスをさらに備える、請求項１に記載のシステム。
【請求項７６】
ａ）カスタムチェーン認識モジュール（ＣＲＭ）であって、ノードによって過去に登録された、ＡｐｐｃｈａｉｎｓまたはＭｉｃｒｏｃｈａｉｎｓを含むカスタムチェーンと接続し、ＣＲＭは、ＭｅｔａｃｈａｉｎまたはＭｉｃｒｏｃｈａｉｎのＭｅｔａｃｈａｉｎエミュレータの、Ａｐｐｃｈａｉｎのセクションでアップデートが検出されたとき、ＢＣＨＡＩＮプロトコルの残りの部分を通知する、カスタムチェーン認識モジュールと、
ｂ）コンテンツクレームデリバリ（ＣＣＤ）であって、検証されたＣＣＲを受信し、その後、リクエストを満たすために、該当するＣＣＦを送信する、コンテンツクレームデリバリと、
ｃ）動的ストラテジー適応（ＤＳＡ）であって、創作モジュールを使用して、最適化ストラテジー選択アルゴリズム（ＯＳＳＡ）を介してシステムが好む複雑なストラテジーを混成することによって、新しいストラテジー配置を動的に生成する、ストラテジー生成モジュール（ＳＣＭ）を管理し、新しいストラテジーは、フィールド乱雑解釈（ＦＣＩ）によって提供される入力にしたがって変化し、新しいストラテジーは、フィールド乱雑解釈（ＦＣＩ）によって提供される入力にしたがって変化する、動的ストラテジー適応と、
ｄ）暗号化デジタル経済交流（ＣＤＥＥ）であって、ＵＢＥＣプラットフォームインタフェース（ＵＰＩ）の下でグラフィカルユーザインタフェース（ＧＵＩ）によって管理される様々な経済人格を有し、人格Ａでは、ノードリソースは、消費するものと一致するものだけが消費され、人格Ｂは、利益マージンが所定の値より大きい限り、可能な限り多くのリソースを消費し、人格Ｃは、取引通貨を通じて作業単位を支払い、人格Ｄでは、ノードのリソースは、コンテンツの消費であろうと、金銭的な補償であろうと、極力多くのものを期待してなんら制限なしに消費する、暗号化デジタル経済交流と、
ｅ）仕事現状の解釈（ＣＷＳＩ）であって、Ｍｅｔａｃｈａｉｎのインフラ経済セクションを参照することで、仕事量クレジットに関してこのノードの現在の黒字または赤字を判断する、仕事現状の解釈と、
ｆ）経済的に考慮された労働賦課（ＥＣＷＩ）であって、選択された経済人格を、現行の作業剰余／赤字とともに考慮し、現在より多くの作業が行われなければならないかどうかを評価する、経済的に考慮された労働賦課と、
ｇ）象徴的再帰的知性向上（ＳＲＩＡ）であって、コードの目的を理解することによって、アルゴリズムのソースコードを改善することができる、ＬＩＺＡＲＤと、世代の仮想プログラムのバージョンをエミュレートすることができる、Ｉ２ＧＥと、分散型の方法で複雑なデータ偏重のプログラムを実行できる、無秩序に接続されたノードの巨大なネット

ワークである、ＢＣＨＡＩＮネットワークを含む、異なるアルゴリズムの三者関係である、象徴的再帰的知性向上をさらに備える、請求項７５に記載のシステム。

【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、「サイバースペースにおける秘密オペレーションによる秘密機械学習および報復と題する、２０１６年1月２４日出願の米国仮特許出願第６２２８６４３７号、「論理的推論によるゼロデータベースの演繹型リアルタイム防御」と題する、２０１６年2月１１日出願の米国仮特許出願第６２２９４２５８号、「クラウドおよび階層化情報セキュリティ（ＣＴＩＳ）による重要インフラストラクチャ防護および報復（ＣＩＰＲ）」と題する、２０１６年3月１３日出願の米国仮特許出願第６２３０７５５８号、「クリティカルシンキング・メモリおよびパーセプション（ＣＴＭＰ）」と題する、２０１６年4月１６日出願の米国仮特許出願第６２３２３６５７号、「線形量子情報転送（ＬＡＱＩＴ）」と題する、２０１６年4月２３日出願の米国仮特許出願第６２３２６７２３号、「客観的討論マシン（ＯＤＭ）」と題する、２０１６年5月２５日出願の米国仮特許出願第６２３４１３１０号、「辞書的客観性探索（ＬＯＭ）」と題する、２０１６年１２月２７日出願の米国仮特許出願第６２４３９４０９号、「コンピュータネットワークにおけるセキュリティを管理する方法および装置」と題する、２０１５年5月４日出願の米国仮特許出願第１５１４５８００号、および「永続的慈善活動のシステム」と題する、２０１６年9月１４日出願の米国仮特許出願第１５２６４７４４号、の優先権を主張し、それらの開示を参照することにより、本明細書に記載されているかのように、本明細書に組み入れる。
【０００２】
本発明は、人工知能によるコンピュータセキュリティのシステムに関する。サブシステムは、クラウドベースの重層的情報セキュリティ（ＣＴＩＳ）による重要インフラストラクチャ防護および報復（ＣＩＰＲ）、サイバースペースにおける秘密オペレーションによる秘密機械学習（ＭＡＣＩＮＴ）および報復、論理的推論によるゼロデータベースの演繹型リアルタイム防御（ＬＩＺＡＲＤ）、クリティカルシンキング・メモリおよびパーセプション（ＣＴＭＰ）、辞書的客観性探索（ＬＯＭ）、線形量子情報転送（ＬＡＱＩＴ）、およびベース接続協調攻撃統合ノードを伴った普遍的ＢＣＨＡＩＮ全接続（ＵＢＥＣ）システム、を含む。
【背景技術】
【０００３】
コンピュータネットワークセキュリティに関連する問題は、問題点の複雑さから、人間の専門家に依存することが多かった。コンピュータやネットワーク能力の急速な拡張は、ハッカーをはじめとする、悪意のある実体によって悪用され、結局人間の専門家頼みだった従来の解決策を圧倒してきた。人工知能を用いる戦略が、このような状況が示す限界を克服する解決策となりつつある。しかしながら、この新たな解決策には、人間の思考過程を効果的に模倣し、かつコンピュータハードウェアに実装できるよう調整された先進モデルを必要である。
【発明の概要】
【課題を解決するための手段】
【０００４】
人工知能によるコンピュータセキュリティシステムであり、システムは、プログラム化された命令を格納するメモリ、メモリに接続され、前記プログラム化された命令を実行するプロセッサ、および少なくとも１つのデータベースを備え、システムは、指定された機

能を提供するコンピュータ実装システムを備える。
【０００５】
前記コンピュータ実装システムとは、クラウドおよび階層化情報セキュリティによる重要インフラストラクチャ防護および報復（ＣＩＰＲ／ＣＴＩＳ）であり、
ａ）ハッカーの行動を報告するエージェント達のネットワークを有する信用プラットフォーム、および
ｂ）管理された暗号化セキュリティ、接続性およびコンプライアンスのソリューションおよびサービスを提供する、マネージドネットワークおよびセキュリティサービスプロバイダ（ＭＮＳＰ）をさらに備え、
仮想プライベートネットワーク（ＶＰＮ）は、ＭＮＳＰと信用プラットフォームを接続しており、ＶＰＮは、前記信用プラットフォームとの通信チャネルを提供し、前記ＭＮＳＰは、前記企業ネットワークのすべてのトラフィックを分析できるよう構成され、前記トラフィックは前記ＭＮＳＰにルーティングされる。
【０００６】
前記ＭＮＳＰは、
ａ）論理的推論によるゼロデータベースの演繹型リアルタイム防御（ＬＩＺＡＲＤ）であって、外来コードから目標と機能を導出し、悪意の存在または正当な動機の欠如に反応して、その外来コードをブロックし、それまでの履歴データを参照せず、脅威それ自体を分析する、論理的推論によるゼロデータベースの演繹型リアルタイム防御と、
ｂ）疑似セキュリティ脅威（ＡＳＴ）であって、セキュリティルールセットの効力をテストするための、仮想のセキュリティシナリオを提供する、疑似セキュリティ脅威と、
ｃ）創作モジュールであって、前形状から新たなハイブリッド形状を知的に創作する処理を実行する、創作モジュールと、
ｄ）共謀検知であって、情報連携を見分け、セキュリティ関連の挙動のパターンを抽出し、多数の共謀セキュリティイベントに対する定期的な素性チェックを提供し、一見無関係なセキュリティイベント同士のパターンや関係を判定しようと試みる、共謀検知と、
ｅ）セキュリティ挙動であって、イベントとそのセキュリティ応答を格納、インデックス付けし、前記応答はブロック／許可の決定事項を含む、セキュリティ挙動と、
ｆ）反復型知的成長／知的進化（Ｉ^{2}ＧＥ）であって、ビッグデータとマルウェアシグネチャの認識を活用し、創造性モジュールとともにＡＳＴを活用することでマルウェアの将来起こりうる変化をエミュレートする、反復型知的成長／知的進化と、
ｇ）クリティカルシンキング・メモリ・パーセプション（ＣＴＭＰ）であって、前記ブロック／承認の決定事項を批判し、セキュリティの補完的なレイヤとして機能し、Ｉ^{2}ＧＥ、ＬＩＺＡＲＤ、および信用プラットフォームからの相互参照情報収集を活用する、クリティカルシンキング・メモリ・パーセプションを備え、ＣＴＭＰは、ある事柄についての客観的決定事項を構成する能力を推定し、内部の低い確信度に基づいてなされた決定を表明することを差し控える、クリティカルシンキング・メモリ・パーセプションを備える。
【０００７】
ＬＩＺＡＲＤライトクライアントは、エンタープライズネットワークのデバイスで動作するように構成され、ＭＮＳＰのＬＩＺＡＲＤとの通信を安全に行う。
【０００８】
非武装地帯（ＤＭＺ）は、通常のコンピュータよりセキュリティ上不利な状態にあるＨＴＴＰサーバを有するサブネットワークを備え、このようなセキュリティ上不利な状態に企業ネットワークの残りの部分をさらすことのないようにしている。
【０００９】
前記Ｉ^{2}ＧＥは、並行する複数の進化系統が発達し選択される反復的進化を備え、イテレートされた世代が、同一の疑似セキュリティ脅威（ＡＳＴ）に適応し、最良のパーソナリティトレイトを有する系統が、結局はこのセキュリティ脅威に対して最もよく耐えることになる。

【００１０】
前記ＬＩＺＡＲＤは、
ａ）構文モジュールであって、コンピュータのコードを読み書きするためのフレームワークを提供する、構文モジュールと、
ｂ）目標モジュールであって、前記構文モジュールを用いてコードから目標を導出し、前記目標を、自身の複合目標フォーマットに出力する、目標モジュールと、
ｃ）仮想難読化であって、企業ネットワークとデータベースが、仮想環境内に複製され、機密データが模擬（偽の）データと置き換えられ、ターゲットの挙動に応じて環境がリアルタイム動的に変更され、システム全体としてより多くの偽の要素、またはより多くの本物の要素が含まれる、仮想難読化と、
ｄ）信号擬態であって、仮想難読化の分析が終わったときに報復の形状を提供する、信号擬態と、
ｅ）内部整合性チェックであって、外来コードのすべての内部機能の辻褄が合っていることをチェックする、内部整合性チェックと、
ｆ）外来コード改訂であって、前記構文モジュールと目標モジュールを使用し、外来コードを複合目標フォーマットにまとめる、外来コード改訂と、
ｇ）秘密コード検知であって、データおよび送信パケット内に密かに埋め込まれたコードを検知する、秘密コード検知と、
ｈ）要求マップマッチングであって、マップ化された要求および目標の階層構造であり、外来コードがシステムの目的全体にフィットしているかを判断するために参照される、要求マップマッチングを備え、
書き込みでは、前記構文モジュールは、前記目標モジュールから複合様式の目標を受信し、コードを任意のコード構文で書き込み、ヘルパ機能が前記任意のコードを実際の実行可能コードへと翻訳し、読み込みでは、前記構文モジュールは、前記目標モジュールがこのようなコードの機能の目標を導出できるよう、コードの構文解釈を提供し、
前記信号擬態は、マルウェアがハッカーと通信するための構文を読み解くために、前記構文モジュールを使用し、その後、このような通信を乗っ取り、機密データをハッカーに送ることに成功したという、誤った印象をマルウェアに与え、前記ハッカーは、前記マルウェアのエラーコードもＬＩＺＡＲＤによって送られ、このエラーコードが前記マルウェアから来たもののように思わせ、
前記外来コード改訂は、前記導出された目標を使用するコードセットを構築し、これによって、外来コードから読み解かれた所望の目標だけが企業内で実行され、意図しない機能の実行がシステムにアクセスすることのないことが保証される。
【００１１】
外来コード改訂が外来コードを構文的に再現することで、起こりうる未検知の悪意のエクスプロイトを軽減する様子を示し、組合せメソッドは、宣言された目標を導出された目標と比較し一致させ、前記目標モジュールは、複合目標フォーマットを操作するために使用され、前記導出された目標を用いて、前記要求マップマッチングは、階層的構造を維持管理し、すべての企業の管轄範囲をメンテナンスし、これにより、管轄範囲指向の要求マップの空きに応じて、コードブロックの目的が定義され正当化され、入力された目標が、再帰的デバッグプロセスに取り込まれる。
【００１２】
前記再帰的デバッグが、コードセグメントをループ処理してバグの有無をテストし、バグフィックスを適用し、それでもバグが残っている場合は、前記コードセグメント全体が、オリジナルの外来コードセグメントに置換され、前記オリジナルのコードセグメントは、その後仮想難読化や挙動分析を促進するためにタグ付けされ、前記コードを改訂するために、外来コードを用いて、前記目標モジュールおよび構文モジュールが前記コードのオリジナルの状態を解釈し、改訂バージョンに消えないバグがあるためにオリジナルの外来コードセグメントをインストールする必要がある場合、前記外来コードは前記デバッガから直接参照され、改訂コードでは、セグメントが仮想ランタイム環境によってテストされ、

コーディングバグの有無がチェックされ、前記仮想ランタイム環境はコードセグメントを実行し、実行時エラーの有無をチェックし、コーディングバグを用いて、前記仮想ランタイム環境において生じたエラーが、スコープと種別において定義され、目的の整合を用いて、前記宣言された目的からコードを再び導出することで、前記コーディングバグに対する解決策の候補が考え出され、このようなバグを回避するために、前記コーディングバグのスコープが代替フォーマットの形式に書き換えられ、前記解決策の候補が出力され、他になにも解決策がない場合は、前記コードセグメントに対するコード改訂は喪失され、前記外来コードから直接来る前記オリジナルのコードセグメントが最終コードセットにおいて使用される。

【００１３】

要求マップマッチングの操作ために、ＬＩＺＡＲＤクラウドおよびＬＩＺＡＲＤライトは、企業の管轄範囲部門の階層構造マップを参照し、入力された目標が主張されたものか、前記目標モジュール経由で導出されたものかにかかわらず、要求マップマッチングはコード／関数が前記企業システムの内部で実行するための根拠を確認し、前記階層構造マップのマスターコピーが、ＭＮＳＰのＬＩＺＡＲＤクラウドに格納され、前記マスターコピーを参照することで、要求マップマッチング内の要求インデックスが計算され、そして、予め最適化された前記要求インデックスが、すべてのアクセス可能なエンドポイントのクライアントに配布され、前記要求マップマッチングは最も適切なシステム全体としての要求に関する要求リクエストを受信し、対応する出力は、前記適切な要求を表している複合目標フォーマットである。

【００１４】

企業のＬＡＮインフラストラクチャ全体がＭＮＳＰ内で仮想的に再構築され、前記システムが挙動分析を実行すると、前記ハッカーは現実のＬＡＮインフラおよび仮想クローンバージョンのＬＡＮインフラの双方にある要素に対してさらされ、このような分析の結果がリスクを示す場合、前記ハッカーの仮想クローンインフラへの露出は、実際のデータおよび／またはデバイスが攻略されるリスクを軽減するために増加される。

【００１５】

マルウェアルートシグネチャの新版／変種を生成するために、前記マルウェアルートシグネチャがＡＳＴに与えられ、マルウェアの多型変種がI^2ＧＥから出力され、マルウェア検知に転送される。

【００１６】

前記マルウェア検知は、ユーザスペース、カーネルスペース、およびファームウェア／ハードウェアスペースが設けられたコンピュータの構成の３つのレベルすべてに配置され、前記スペースのすべては、ＬＩＺＡＲＤライトエージェントによって監視される。

【００１７】

前記コンピュータ実装システムは、サイバースペースにおける秘密オペレーションによる秘密機械学習（ＭＡＣＩＮＴ）および報復であって、

ａ）知的情報および構成管理（I^2ＣＭ）であって、知的情報の管理、閲覧、および制御を提供する、知的情報および構成管理と、

ｂ）管理コンソール（ＭＣ）であって、入出力チャネルをユーザに提供する、管理コンソールをさらに備え、

前記I^2ＣＭは、

ｉ）アグリゲーションであって、汎用のレベル判定基準を使用して、不必要で冗長な情報を遮断し、多数のプラットフォームからの情報ストリームをマージ、タグ付けする、アグリゲーションと、

ｉｉ）設定および導入サービスであって、新たな企業の資産（コンピュータ、ノートパソコン、携帯電話）を、正しいセキュリティ設定と通信設定で導入するためのインタフェースである、設定および導入サービスと、

ｉｉｉ）管轄範囲による分割であって、タグ付けされた情報の集積が、管理コンソールのユーザに該当する管轄範囲にしたがって、排他的に分割される、管轄範囲による分割と

、
ｉｖ）脅威による分割であって、個々の脅威に応じて情報を整理する、脅威による分割と、
ｖ）自動化制御であって、ＭＮＳＰクラウド、信用プラットフォーム、または付加的なサードパーティサービスにアクセスする、自動化制御を備える。
【００１８】
ＭＮＳＰクラウドにおいて、挙動分析は、模擬データ環境にいる間のマルウェアの状態と実行された活動を観察し、前記マルウェアが偽データをハッカーのもとへ送信しようとしているとき、送信される信号は、偽のハッカーが受信するようにルーティングされ、ハッカーインタフェースは、前記マルウェアのコード構造を受け取り、前記マルウェアの内部構造についてリバースエンジニアリングを行い、ハッカーインタフェースを出力し、偽のハッカーおよび偽のマルウェアを仮想環境の中でエミュレートし、仮想化された偽のハッカーは、前記マルウェアの次の挙動パターンを観察するために、前記本物のマルウェアに応答信号を送信し、前記ハッカーには、本物のマルウェアの挙動／状態と関係のない偽の応答コードが与えられる。
【００１９】
エクスプロイトスキャンは、犯罪資産の能力と性質を特定し、それによって得られるスキャン結果が、エクスプロイトによって管理され、エクスプロイトは、信用プラットフォームによって、標的となる犯罪システムに潜入する報復エクスプロイトデータベースを経由して送信されたプログラムであり、報復エクスプロイトデータベースは、設置されたバックドアおよび既知の脆弱性としてハードウェアベンダによって提供された、犯罪活動をエクスプロイトする手段を含んでおり、統合科学捜査的証拠データベースが、多数の企業にわたる多数のソースから収集された科学捜査的証拠を含んでいる。
【００２０】
犯罪システムからの二重スパイが、企業ネットワークのファイルを捕捉し、ファイアウォールがログを生成し、ログはログ集約に転送され、ログ集約は、長期／深層スキャンとリアルタイム／表面スキャンに向けて、データをカテゴリ別に分離する。
【００２１】
前記深層スキャンは、共謀検知サブアルゴリズムおよび外来エンティティ管理サブアルゴリズムを活用して、ビッグデータに貢献および連動し、セキュリティチェックポイントからの標準ログが集約され、ログ集約の低制限フィルタにより選択され、イベントインデックス＋トラッキングはイベントの詳細情報を格納し、異常検知は、前記深層スキャンモジュールによって提供された中間データ基づいてイベントインデックスおよびセキュリティ挙動を用いることにより、可能性のあるリスクイベントを決定し、外来エンティティ管理および共謀検知はイベントの分析に関わっている。
【００２２】
前記信用プラットフォームは、任意コンピュータを検索して、その任意コンピュータまたはその関連／近隣サーバ（任意コンピュータが接続するサーバ）が、前記信用プラットフォームに対する、過去に設置した二重または三重のスパイであるかをチェックし、エージェント検索チェックは、信用できる二重スパイインデックス＋トラッキングクラウドおよび、信用できる三重スパイインデックス＋トラッキングクラウドで実行され、前記任意コンピュータに信用されている二重スパイが、その信用されたチャネルを通じてエクスプロイトをプッシュし、エクスプロイトは、機密ファイルを発見しようとし、機密ファイルを検疫し、機密ファイルの正確な状態を信用プラットフォームに送り返し、その後、その機密ファイルを前記犯罪コンピュータから安全に消去しようとする。
【００２３】
ＩＳＰＡＰＩのリクエストが、信用プラットフォーム経由で行われ、ネットワーク監督で、前記任意システムに関するネットワークログと、犯罪コンピュータにファイルが転送された可能性が見つかり、メタデータを使用して、ファイルがどのコンピュータに送られたかを、かなりの確信度をもって決定し、前記ネットワーク監督は、犯罪コンピュータのネ

ットワークの詳細情報を発見し、このような情報を、別ルートで前記信用プラットフォームに送り、前記信用プラットフォームを使用して、ソフトウェアベンダおよびハードウェアベンダが提供するセキュリティＡＰＩを実行し、司法調査を支援することができる、設置されたバックドアをエクスプロイトする方法を示している。

【００２４】

前記信用プラットフォームが、前記犯罪コンピュータに対してソフトウェアまたはファームウェアの更新を行うことにより、新たなバックドアを設置し、隠密であることを守るために、プラセボアップデートが近隣の類似機器にプッシュされ、ターゲットの身元詳細情報が、前記信用プラットフォームに送信され、前記信用プラットフォームは、ソフトウェア／ファームウェア保守者２８７と通信し、プラセボアップデートおよびバックドアアップデートを該当するコンピュータにプッシュし、前記バックドアアップデートは、犯罪コンピュータに既に設置したソフトウェアアップデートシステムを用いることにより、犯罪コンピュータのシステムに新たなバックドアを導入し、プラセボアップデートはバックドアを取り除き、保守者は、バックドアを標的に転送し、加えて標的に平均以上の露出をしているコンピュータにも転送し、バックドアアップデートを通じてエクスプロイトを設置すると、機密ファイルは、そのメタデータ使用履歴を後で分析できるように検疫されコピーされ、捕捉となる科学捜査データが集められ、前記信用プラットフォームにある、エクスプロイトの接点に送られる。

【００２５】

ありとあらゆる変更／アップデートについて犯罪システムをモニターするために、長期優先フラグが信用プラットフォームにプッシュされ、前記企業システムは標的をワラントモジュールに提出し、このワラントモジュールは、系列システムのすべての入力をスキャンして、定義された標的の任意の関連性を検索し、一致するものがあれば、その情報は企業システムに渡され、企業システムは、そのワラントを定義しており、標的へ潜入しようとし、前記入力は、所望の分析モジュールに転送され、分析モジュールが、相互に有益なセキュリティ情報を同期する

【００２６】

前記コンピュータ実装システムは、論理的推論によるゼロデータベースの演繹型リアルタイム防御（ＬＩＺＡＲＤ）であり、

ａ）静的コア（ＳＣ）であって、主に不変のプログラムモジュールを備えている、静的コアと、

ｂ）イテレーションモジュールであって、ダイナミックシェル上のモジュールを変更、作成、および処分し、セキュリティ上のパフォーマンスの参考のために、ＡＳＴを使用し、イテレーションコアを使用して自動コード記述の方法論を処理する、イテレーションモジュールと、

ｃ）差分変更アルゴリズムであって、前記ＡＳＴが見つけた欠陥にしたがって基底バージョンを変更し、差分ロジックが適用された後、新バージョンが提示され、その直後にイテレーションコアが再帰的に呼び出され、ＡＲＴによってテストされたものと同じプロセスを経る、差分変更アルゴリズムと、

ｄ）論理減算アルゴリズムであって、疑似セキュリティ脅威（ＡＳＴ）からダイナミックシェルのバージョンの既知のセキュリティ応答を受信し、ＬＤＡはまた、どのコードセット構成が既知の正しい応答を達成するかを、セキュリティシナリオに合わせて推論する、論理減算アルゴリズムと、

ｅ）ダイナミックシェル（ＤＳ）であって、イテレーションモジュール（ＩＭ）によって自動的にプログラムされたダイナミックプログラムモジュールを主に含む、ダイナミックシェルと、

ｆ）コード検疫であって、外来コードを制限付の仮想環境に隔離する、コード検疫と、

ｇ）秘密コード検知であって、データおよび送信パケット内に密かに埋め込まれたコードを検知する、秘密コード検知と、

ｈ）外来コード改訂であって、外来コードの目標を導出した後、コードの一部あるいは

全部を改訂し、改訂版だけの実行を許可する、外来コード改訂をさらに備え、
すべての企業デバイスはＬＩＺＡＲＤにルーティングされ、企業デバイスを稼働させるすべてのソフトウェアとファームウェアは、あらゆる種類のダウンロード／アップロードを、永続プロキシのようにＬＩＺＡＲＤ経由で実行するようにハードコードされており、ＬＩＺＡＲＤは、移動中のデータ、休止中のデータ、および使用中のデータを含む３種類のデータと相互作用し、ＬＩＺＡＲＤは、ファイル、電子メール、ウェブ、モバイル、クラウド、リムーバブルメディアを含むデータメディアと相互作用する。
【００２７】
前記システムは、
ａ）ＡＳＴオーバーフロー中継であって、前記システムが低確信度の判断しかできないときは、将来のバージョンの改善のために、データがＡＳＴに中継される、ＡＳＴオーバーフロー中継と、
ｂ）内部整合性チェックであって、外来コードのブロックのすべての内部機能の辻褄が合っているかどうかをチェックする、内部整合性チェックと、
ｃ）ミラーテストであって、前記改訂版の入出力の関係が、元のコードのものと同じであることを確かめ、これにより、元のコードに存在する隠されたエクスプロイトはどれも使われなくなり、二度と実行されることがなくなる、ミラーテストと、
ｄ）要求マップマッチングであって、マップ化された要求および目標の階層構造を備え、外来コードが前記システムの目的全体にフィットしているかを判断するために参照される、要求マップマッチングと、
ｅ）実データ同期部であって、混合環境に与えられるデータを、どの優先順位で与えるのかを選択し、これによって、疑われるマルウェアに機密情報をアクセスできなくする、実データ同期部と、
ｆ）データマネージャであって、仮想環境の外部から来るエンティティとデータとの間にある中間者インタフェースである、データマネージャと、
ｇ）仮想難読化であって、仮想化された偽の環境に、徐々にかつ部分的に沈めることで、コードを乱雑にし、制限する、仮想難読化と、
ｈ）秘密輸送モジュールであって、マルウェアに何も知らせず慎重にマルウェアを模擬データ環境に転送する、秘密輸送モジュールと、
ｉ）データリコール追跡であって、疑わしいエンティティからアップロードされたりそこへダウンロードされたりするすべての情報を追跡する、データリコール追跡をさらに備える。
【００２８】
前記システムは、目標比較モジュールであって、４つの異なるタイプの目的を比較し、システムの全体的な目的に対して良い結果をもたらすことにおいて、そのエンティティの存在および挙動が合理的でＬＩＺＡＲＤによって理解されることを保証する、目標比較モジュールを、さらに備える。
【００２９】
前記イテレーションモジュールは、前記ＳＣを使用して、データ返送中継（ＤＲＲ）からの定義された目標にしたがって、ＤＳのコードベースを構文的に変更し、前記改変バージョンのＬＩＺＡＲＤは、前記ＡＳＴによって、多数のさまざまなセキュリティシナリオのもとで、並行してストレステストを受ける。
【００３０】
前記ＳＣの内部では、論理的導出が、初期のより簡易な機能から、必要な機能を論理的に導出し、これにより、機能の依存性のツリー全体が、宣言された複合目標から構築され、
コード翻訳が、構文モジュール機能によって直接読み解かれる任意の汎用コードを、任意に選ばれた既知のコンピュータ言語に変換され、既知のコンピュータ言語から任意のコードへの逆翻訳も行われ、
ロジック削減が、コードに記述されたロジックを、より簡易な形状にまとめて相互に接続された機能のマップを生成し、

複合目標フォーマットが、目標の全体を表している相互に連携する下位目標を格納するための格納フォーマットを表しており、
目標の関連性が、挙動の機能および型のどれがどの種類の目標を指しているかを調べるための、ハードコーティングされた参考資料のことであり、
反復的拡張が、目標の関連性を参照し、詳細と複雑性を追加して、単純なゴールを複合目標に進化させ、
反復型解釈は、相互に接続された機能をループ処理し、かつ、目標の関連性を参照することにより、解釈された目標を生成し、
協力しあうことで未知の外来コードから論理的な目標を導出し、また宣言された機能コードのゴールから実行可能コードを生成する、構文モジュールおよび目標モジュールによって、外側コアが形成され、
外来コードは、ＬＩＺＡＲＤには未知であるコードで、その機能および意図された目標は未知であり、外来コードは内側コアへの入力であり、導出された目標が出力であり、前記導出された目標は、前記目標モジュールにより推定されたものとしての、任意のコードの意図であり、前記導出された目標は、複合目標フォーマットで返される。

【００３１】

前記ＩＭは、セキュリティ上のパフォーマンスの参考のためにＡＳＴを使用し、イテレーションコアを使用して自動コード記述の方法論を処理し、前記ＤＲＲでは、ＬＩＺＡＲＤがやむなく低い確信度で意志決定をしなければならない場合に、悪意の攻撃および常習犯のデータが前記ＡＳＴに中継され、前記イテレーションコアの内部では、差分変更アルゴリズム（ＤＭＡ）が、前記内側コアから、構文／目的プログラミング能力とシステムの目的のガイダンスを受け取り、このようなコードセットを使うことで、前記ＡＲＴが見つけた欠陥にしたがって基底バージョンを変更し、セキュリティテスト結果での欠陥が、前記仮想実行環境を実行している間に前記基底バージョンをパスしたセキュリティ脅威を示すために、可視的に提示される。

【００３２】

前記ＤＭＡの内部では、現在の状態は、ダイナミックシェルのコードセットを、象徴的に相関している図形、サイズ、および位置とともに表しており、これらの図形の種々の構成は、セキュリティ情報収集およびセキュリティ応答の種々の構成を示しており、前記ＡＳＴは、誤りであったり、正しい応答であったりする、現在の状態のありうる応答を提供し、
攻撃ベクトルは、サイバーセキュリティの脅威の象徴的な実証として機能し、方向、サイズ、および色はすべて、攻撃ベクトル、マルウェアのサイズ、マルウェアの種類のような、仮定のセキュリティプロパティに関連しており、前記攻撃ベクトルは、コードセットのセキュリティ応答を表すために、そのコードセットに象徴的にぶつかり、
正しい状態は、ダイナミックシェルのコードブロックから所望のセキュリティ応答を生ずる、前記ＤＭＡのプロセスの最終結果を表しており、前記現在の状態と正しい状態の結果の差異は、種々の攻撃ベクトルの応答の差異に帰し、
前記ＡＳＴは、正しいセキュリティ応答に加えてセキュリティ上の既知の欠陥を提供し、ロジック推論アルゴリズムは、前記ＤＳの過去のバージョンを使用して、正しいセキュリティ応答プログラムと呼ばれる、優秀で十分な設備が整っているダイナミックシェルのバージョンを生成する。

【００３３】

仮想難読化の内部では、疑問の余地のあるコードが密かに、データの半分が模擬データと知的に混合されている環境に割り当てられ、実システム内で稼働しているどの対象も、仮想的隔離により、部分模擬データ環境または完全模擬データ環境に容易かつ秘密裏に転送され、模擬データジェネレータは、偽造かつ無用なデータを作成するためのテンプレートとして、前記実データ同期部を使用し、到来する外来コードの認知におけるリスクの確信度の認知は、ＬＩＺＡＲＤが選ぶ難読化のレベルに影響し、コードが悪意のあるということにおける確信度が高い場合は、多量の模擬データを含む環境が割り当てられ、コードが

悪意のあるということにおける確信度が低い場合は、実システムあるいは１００％模擬データの環境のどちらかが割り当てられる。

【００３４】

データリコール追跡は、疑わしいエンティティからアップロードされたりそこへダウンロードされたりするすべての情報を追跡し、模擬データが正当な企業エンティティに送信された場合、すべての模擬データを呼び戻すコールバックが実行され、実データが、代わりに送信され、コールバックトリガーは、正当な企業エンティティが、データが偽ではないと確認されるまで、特定の情報に対する操作を差し控えるように実装されている。

【００３５】

挙動分析は、修正処置の候補を決定するために、疑わしいエンティティのダウンロードおよびアップロードの挙動を追跡し、実システムは、仮想環境の完全な外部に存在する、前記オリジナルの実データを含み、模擬データを置き換える実データは、実データがフィルタリングされずにデータリコール追跡に提供される場所である。これにより、実データパッチを作成して、前記模擬データを以前の疑わしいエンティティ上の実データと置き換えることができ、仮想的に隔離された環境に沈められているデータマネージャは、前記データリコール追跡から実データパッチを受け取り、無害コードが挙動分析によって悪意を持っていると明らかにされると、修正処置が実行されることで、前記以前の疑わしいエンティティの前記模擬データを、それが表す前記実データに置き換え、シークレットトークンは、ＬＩＺＡＲＤによって生成され割り当てられるセキュリティ文字列であり、本当に無害である前記エンティティにその仕事を進めないようにし、トークンが見当たらない場合、これは、それがマルウェアであるというリスク評価のために、この正当なエンティティが間違って部分的模擬データ環境に配置されている可能性が高いシナリオを示しており、その後、前記遅延インタフェースを有する遅延セッションが起動され、トークンが見つかった場合、これはサーバ環境が本物であることを示しており、したがって遅延セッションは無効化される。

【００３６】

前記挙動分析内で、目標マップは、企業システム全体に目標を与えるシステムの目的の階層構造であり、宣言された目標、活動の目標、およびコードベースの目標は、前記疑わしい実体が行っていることが何であれ、本来のシステムの要求と比較され、活動監視では、前記疑わしいエンティティのストレージ、ＣＰＵ処理、およびネットワーク活動が監視され、前記構文モジュールは、所望の機能に関してこのような活動を解釈し、このような機能は、その後、前記目標モジュールによる挙動において意図された目標に変換され、コードベースは、前記疑わしいエンティティのソースコード／プログラミング構造であり、前記構文モジュールに転送され、前記構文モジュールは、コーディングの構文を理解し、プログラミングコードおよびコードの活動を中間機能連携マップに還元し、前記目標モジュールは、前記疑わしいエンティティの認知された意図、コードベースの目標、および活動の目標の出力を生成し、前記コードベースの目標には、ＬＩＺＡＲＤの構文的プログラミング能力によって引き出された、エンティティの前記既知の目標、機能、管轄範囲および権限が含まれており、前記活動の目標には、ＬＩＺＡＲＤのストレージ、処理およびネットワーク活動の理解によって読み解かれた、エンティティの既知の目標、機能、管轄範囲および権限が含まれており、前記宣言された目標は、エンティティ自体によって宣言された、前記エンティティの想定される目的、機能、管轄範囲および権限であり、前記要求された目標には、エンタープライズシステムが必要とする期待される目的、機能、管轄範囲および権限が含まれており、すべての目標が、比較モジュールにおいて比較され、前記目的の間に不一致があれば、目標の相違のシナリオが呼び出され、修正処置につながる。

【００３７】

前記コンピュータ実装システムは、クリティカルシンキング・メモリおよびパーセプション（ＣＴＭＰ）であり、前記システムはさらに、

ａ）クリティカルルールスコープエクステンダー（ＣＲＳＥ）であって、既知のパーセプションのスコープを受け取り、パーセプションのクリティカルシンキングスコープを含

むよう、パーセプションの既知のスコープを拡張する、クリティカルルールスコープエクステンダーと、
ｂ）妥当ルールであって、パーセプションのクリティカルシンキングスコープを利用することにより導き出された妥当ルールを示している、妥当ルールと、
ｃ）ルール実行（ＲＥ）であって、メモリが乱雑フィールドをスキャンすることにより、存在して充足可能であると確認されたルールを、該当する所望のクリティカルシンキングの決定事項を生成するために実行する、ルール実行と、
ｄ）クリティカル決定出力であって、パーセプション観察者エミュレータ（ＰＯＥ）および前記ルール実行の双方が至った結論を比較することにより、ＣＴＭＰの出力全体を決定するための最終ロジックを生成する、クリティカル決定出力と、をさらに備え、
前記ＰＯＥは、前記観察者のエミュレーションを生成し、パーセプションポイントの候補すべてを、このような様々な観察者エミュレーションを使用してテスト／比較し、
前記ＲＥは、ルールセットの変換を追跡するために使用される、市松模様の平面を備え、平面上のオブジェクトは、任意のセキュリティ状況の複雑さを表しており、一方で「セキュリティの市松模様」に広がるそのようなオブジェクトの動きは、セキュリティルールセットの応答によって管理されるセキュリティ状況の進化を示す。
【００３８】
前記システムはさらに、
ａ）主観的意見決定であって、選択パターンマッチングアルゴリズム（ＳＰＭＡ）によって与えられる決定である、主観的意見決定と、
ｂ）入力システムメタデータであって、ＳＰＭＡから与えられ、前記アルゴリズムのメカニカルプロセスおよびそのような決定に至った経緯を記述している未処理メタデータを有する、入力システムメタデータと、
ｃ）事由処理であって、プロパティの属性を比較することにより表明を論理的に理解する、事由処理と、
ｄ）ルール処理であって、導き出された結果ルールを、当面の問題のスコープを決定するための参照点として利用する、ルール処理と、
ｅ）メモリウェブであって、充足可能なルールを求めてログをスキャンする、メモリウェブと、
ｆ）未処理パーセプション生成であって、ＳＰＭＡからメタデータログを受け取り、そのようなログはパースされ、そのようなアルゴリズムのパーセプションを表すパーセプションが形成され、前記パーセプションは、複合パーセプションフォーマット（ＰＣＦ）に格納され、前記ＰＯＥによってエミュレートされ、適用済パーセプションの視点は、ＳＰＭＡによって既に適用され利用されたパーセプションの視点を示している、未処理パーセプションと、
ｇ）自動化パーセプション発見メカニズム（ＡＰＤＭ）であって、適用済パーセプションの視点によって与えられる入力にしたがって形成される、混成パーセプションを生成する創作モジュールを活用し、これによって、前記パーセプションのスコープを拡張することができる、自動化パーセプション発見メカニズムと、
ｈ）自己批判的知識密度（ＳＣＫＤ）であって、報告可能なログの限界を越えた、未知である可能性がある知識のスコープおよび型を推定し、これによって、この結果生じるＣＴＭＰのクリティカルシンキング的な特徴によって、関与する知識のすべての可能なスコープを活用することができ、クリティカルシンキングが、ルールベースの思考の外殻範囲を表している、自己批判的知識密度と、
ｉ）意味付けの導出（ＩＤ）であって、現時点で適用されたパーセプションの視点から意味付けされうる、パーセプションの視点のデータを導出する、意味付けの導出をさらに備え、
前記ＳＰＭＡは、パーセプションおよびルールを介してＣＴＭＰにより実行される前記クリティカルシンキングと並置される。
【００３９】

前記システムはさらに、
ａ）リソース管理および割付（ＲＭＡ）であって、調整可能ポリシーは、観察者エミュレーションを実行するために活用されるパーセプションの数を定め、選ばれたパーセプションの優先順位が、重み付けの降順で選択され、前記ポリシーは、パーセンテージ、固定値、あるいは、より複雑な選択アルゴリズムであろうと、切り捨てを選択する方法を定める、リソース管理および割付と、
ｂ）ストレージ検索（ＳＳ）であって、データ拡張ログからの前記ＣＶＦを、パーセプションストレージ（ＰＳ）のデータベース検索における判断基準として使用し、ＰＳでは、パーセプションと、それらの該当する重み付けが、それらのインデックスとしての比較可能可変フォーマット（ＣＶＦ）とともに格納される、ストレージ検索と、
ｃ）メトリック処理であって、前記ＳＰＭＡからの変数割付に対してリバースエンジニアリングを行う、メトリック処理と、
ｄ）パーセプション推論（ＰＤ）であって、割付の回答と、それに対応するシステムメタデータを使用して、前記割付の回答の元のパーセプションを再生する、パーセプション推論と、
ｅ）メタデータカテゴリ化モジュール（ＭＣＭ）であって、デバッグおよびアルゴリズム追跡が、構文ベースの情報カテゴリ化によって個別のカテゴリに分割され、前記カテゴリが、リスクおよび機会と相関関係を有する、個々の割付の回答をまとめ上げて生成するために使用される、メタデータカテゴリ化モジュールと、
ｆ）メトリック合成であって、パーセプションの視点を、メトリックのカテゴリに分割する、メトリック合成と、
ｇ）メトリック変換であって、個々のメトリックをパーセプションの視点全体に戻す、メトリック変換と、
ｈ）メトリック拡張（ＭＥ）であって、多数のさまざまなパーセプションの視点のメトリックを、個々のデータベースに、カテゴリ別に格納する、メトリック拡張と、
ｉ）比較可能可変フォーマットジェネレータ（ＣＶＦＧ）であって、情報ストリームを、比較可能可変フォーマット（ＣＶＦ）に変換する、比較可能可変フォーマットジェネレータと、をさらに備える。

【００４０】

前記システムはさらに、
ａ）パーセプションマッチングであって、ルール構文導出（ＲＳＤ）から受信したパーセプションから、ＣＶＦが形成され、新たに形成されたＣＶＦは、前記ＰＳ内で類似したインデックスを有する、該当するパーセプションを検索するために使用され、一致する候補が、ルール構文生成（ＲＳＧ）に戻される、パーセプションマッチングと、
ｂ）メモリ認識（ＭＲ）であって、入力データから乱雑フィールドが形成される、メモリ認識と、
ｃ）メモリコンセプトのインデックス付けであって、すべてのコンセプトが、個別にインデックスに最適化され、前記インデックスは、乱雑フィールドと連携するために、文字スキャナによって使用される、メモリコンセプトインデックス付けと、
ｄ）ルール充足度パーサ（ＲＦＰ）であって、ルールの個々の部分を、認識のタグとともに受信し、各部分は、メモリ認識によって、乱雑フィールド内で見つかった、または見つからなかったとマークされ、前記ＲＦＰは、どのルール全体、つまり、そのルールの全部分の合成が、乱雑フィールド内で前記ＲＥするに値するほど十分に認識されたのかを、論理的に推論する、ルール充足度パーサと、
ｅ）ルール文法フォーマット分割（ＲＳＦＳ）であって、妥当ルールが分割され、型ごとにまとめられ、これにより、すべての処置、プロパティ、条件、およびオブジェクトが、別々に束ねられる、ルール文法フォーマット分割と、
ｆ）ルール構文導出であって、論理的な「白か黒か」ルールが、メトリックベースのパーセプションに変換され、これにより、多数のルールの複雑な配列が、さまざまな勾配の多数のメトリックにより表現される、単一で一様なパーセプションに変換される、ルール

構文導出と、
ｇ）ルール構文生成（ＲＳＧ）であって、パーセプションフォーマットに格納されている、以前に確認されたパーセプションを受信し、パーセプションの内部的なメトリック編成に携わり、このような勾配ベースのメトリックの測定値が、元のパーセプションの入力／出力される情報のフローを列挙する、二値で論理的なルールセットに変換される、ルール構文生成と、
ｈ）ルール文法フォーマット分割（ＲＳＦＳ）であって、妥当ルールは、観察されているオブジェクトの現実に従うルールセットの正確な明示を表しており、妥当ルールが分割され、型ごとにまとめられ、したがってすべての処置、プロパティ、条件、およびオブジェクトが、別々に束ねられ、これによってシステムは、どの部分が乱雑フィールド内で見つかっていて、どの部分が見つかっていないのかを判別することが可能となる、ルール文法フォーマット分割と、
ｉ）本質的論理的推論であって、論理的原則を用い、そうして誤謬を避けながら、どの種類のルールがパーセプションの範囲内でメトリックの勾配を正確に表しているかを推論する、本質的論理的推論と、
ｊ）メトリックコンテキスト分析であって、メトリックのパーセプションの範囲内で相互関係を分析し、あるメトリックは他のメトリックに様々な大小関係で依存することがあり、この文脈化が、「デジタル」ルールセット形式の範囲内でルールが有するミラー化された相互関係を補足するために使用される、メトリックコンテキスト分析と、
ｋ）ルール構文形式変換（ＲＳＦＣ）であって、ルール構文形式（ＲＳＦ）の構文に従うように、ルールを仕訳け、分割し、直感的決定は、パーセプションを活用することを通じてクリティカルシンキングに携わり、思考的決定は、ルールを活用することを通じてクリティカルシンキングに携わり、パーセプションは、内部形式で定義された形式構文にしたがって、直感的決定から受信したデータであり、充足ルールが、思考的決定から受信したデータで、前記ＲＥからの充足可能なルールセットの集合であり、前記データが、内部形式で定義されている形式構文に則って渡される、ルール構文形式変換をさらに備え、
処置は、既に実行されているかもしれない、実行するかもしれない処置を示し、起動のために考慮されており、プロパティは、何か他のものを記述する何らかのプロパティのような属性を示し、処置、条件、または目的であり、条件は、論理演算または演算子を示し、目的は、それに適用される属性を有することができる標的を示し、
分割ルールフォーマットは、メモリ認識前段階と見なされている、ルール文法フォーマット分割（ＲＳＦＳ）からの出力として使用され、そして、メモリ認識後段階と見なされている、メモリ認識（ＭＲ）からの出力として使用される。
【００４１】
前記システムはさらに、
ａ）乱雑フィールドパース（ＣＦＰ）であって、複数のログのフォーマットを、単一のスキャン可能な乱雑フィールドに合成する、乱雑フィールドパースと、
ｂ）追加ルールであって、前記妥当ルールを補足するために、メモリ認識（ＭＲ）から生成される、追加ルールをさらに備え、
パーセプションマッチング（ＰＭ）の内部では、メトリック統計は、パーセプションストレージからの統計情報を提供し、エラー管理は、個々のメトリックのいずれかから生ずる構文エラーおよび／または論理的エラーをパースし、個々のメトリックは、入力パーセプションであった単一のユニットに合成されていたため、個々のメトリックを分離し、ノード比較アルゴリズム（ＮＣＡ）は、２つ以上のＣＶＦのノード構成を受信し、ＣＶＦの各ノードはプロパティの大小を表しており、個々のノードごとに、類似度比較が行われ、総合分散が計算され、分散の数値が小さい場合は、一致度が高いことを表している。
【００４２】
クレームの前記システムは、
ａ）未処理パーセプション-直感的思考（アナログ）であって、「アナログ」形式にしたがってパーセプションを処理し、前記決定に関係するアナログ形式のパーセプションは、

段差のない滑らかな曲線の勾配で格納されている、未処理パーセプションと、
ｂ）未処理ルール-論理的思考（デジタル）であって、「デジタル」形式にしたがってルールを処理し、前記決定に関係するデジタル形式の未処理ルールは、「あいまいな領域」が皆無かそれに近いステップ単位で格納されている、未処理ルール-論理的思考と、をさらに備え、
未充足ルールは、それらの論理的な依存性にしたがって乱雑フィールド内で十分に認識されていないルールセットであり、充足ルールは、その論理的な依存関係にしたがって、乱雑フィールドで十分に利用可能であると認識されているルールセットであり、
キュー管理（ＱＭ）は、構文的関係再構築（ＳＲＲ）を利用して、個々の部分を最も論理的な順序で分析し、メモリ認識（ＭＲ）の結果にアクセスすることができ、それによって、バイナリのイエス／ノーフロー質問に答えることができ、適切な処置をとることができ、ＱＭは、すべてのルールセグメントを段階的にチェックし、単一のセグメントが乱雑フィールドから欠落し、他のセグメントと適切な関係にない場合、ルールセットは未充足であるとフラグされる。

【００４３】
シーケンシャルメモリ編成は、順番に並べられた情報の「チェーン」のための、最適化された情報ストレージであり、メモリアクセスポイントでは、ノード（ブロック）のそれぞれの幅は、記憶されたオブジェクト（ノード）への観察者の直接到達性を表しており、到達性の範囲では、各文字は、観察者への直接メモリアクセスのポイントを表し、より広い到達性の範囲は、シーケンスノードごとにより多くの到達ポイントが存在し、「順番に」のみ参照され、ランダムに選択されたノードからは参照されないシーケンス長くなるほど、到達性の範囲はより狭くなり（シーケンスサイズとの比較で）、ネストされたサブシーケンスレイヤでは、強い不均一性を示すシーケンスは、相互接続している一連のより短いサブシーケンスで構成されている。

【００４４】
非シーケンシャルメモリ編成は、非シーケンシャルに関連する項目の情報ストレージを扱い、可逆性が、非シーケンシャルな配置と均一なスコープを示す様子を示し、非シーケンシャルな関係が、ノードごとに比較的広いアクセスポイントによって示され、同様の均一性は、ノードの順序がシャッフルされるときに存在し、核となる話題および関連性では、同じ一連のノードが、異なる核（中心のオブジェクト）を除いて繰り返され、この核は、核となる話題が定義されていない場合とは対照的に、残りのノードがより容易にアクセスできるメモリの近隣として機能する、主たる話題を表している。

【００４５】
メモリ認識（ＭＲ）は、既知のコンセプトを認識するために乱雑フィールドをスキャンし、乱雑フィールドは、「ホワイトノイズ」の情報内に任意に潜んでいるコンセプトの「フィールド」であり、メモリコンセプト保持は、フィールド検査のためにインデックス付けおよび参照される準備が整った、認識可能なコンセプトを格納し、３文字スキャナは、乱雑フィールドをスキャンし、ターゲットに対応する３文字セグメントに対してチェックを行い、５文字スキャナは、乱雑フィールドをスキャンし、ターゲットに対応する５文字セグメントに対してチェックを行うが、今度は、フィールド全体にわたってすべての進歩によってチェックされるセグメントは、単語全体であり、乱雑フィールドは、異なる比率でスキャンするように分割され、スキャンの範囲が狭くなるにつれて、精度が向上し、スキャナのフィールド領域が増加するにつれて、より大きい文字スキャナは、精度を犠牲にして認識を実行するので、より効率的になり、メモリコンセプトのインデックス付け（ＭＣＩ）が、未処理のメモリコンセプトが残っていることに応答して、スキャナのサイズを切り替え、ＭＣＩ５００は利用可能なスキャナの中で最大のものから始め、徐々に減少し、それにより、より多くのコンピューティングリソースが発見され、より小さなメモリコンセプトターゲットの存在可能性をチェックすることができる。

【００４６】
フィールド解釈ロジック（ＦＩＬ）は、文字幅の様々な複数のスキャナを管理するロジス

ティクスを実行し、汎用スコープスキャンが、大型の文字スキャンからロジックを始め、小規模なスケールでの精度を犠牲にしてフィールドの大規模なスコープを少ないリソースで精査し、詳細スコープスキャンは、重要なエリアが特定され、そこに「ズームイン」する必要のある場合に用いられ、それによって、冗長で生産性のない場所では、高コストな高精度のスキャンは用いられないことが保証され、乱雑フィールドでメモリコンセプトの追加の認識を受け取ることは、フィールドスコープが高密度飽和のメモリコンセプトを含むことを示している。

【００４７】

自動化パーセプション発見メカニズム（ＡＰＤＭ）では、パーセプション視点は、スコープ、種別、強度、および一貫性を含む、複数のメトリックによって構成されており、これらのメトリクスは、全体的なパーセプションを構成する複数のパーセプションの側面を定義しており、創作モジュールは、パーセプションの複雑なバリエーションを生成し、パーセプションウェイトは、ＰＯＥによってエミュレートされている間に、パーセプションがどの程度の相対的な影響を有するかを定義しており、両方の入力パーセプションのこの重みは、新しくイテレートされたパーセプションの重みを定義しつつ検討しており、以前の世代のパーセプションから影響を受けた、ハイブリッド化されたメトリックを含む。

【００４８】

ＣＶＦＧの入力は、データバッチであり、生成されたＣＶＦのノード構成によって表されなければならないデータを表している、データの任意の集合であり、データバッチによって定義された個々のユニットのそれぞれをシーケンシャルに使用し、データユニットは、ノードフォーマットに変換され、最終のＣＶＦによって参照されるのと同じ構成の情報を有し、このように変換されたノードは、ステージでそれらの存在をチェックすると、ノードホールドアウトに一時的に格納され、それらが見つからなければ、それらは作成され、発生および使用を含む統計情報で更新され、ホールドアウトを有するすべてのノードが組み立てられ、ＣＶＦとして、モジュールの出力としてプッシュされる。

【００４９】

ノード比較アルゴリズムは、未処理のＣＶＦから読み取られた２つのノード構成を比較し、部分一致モード（ＰＭＭ）では、１つのＣＶＦにアクティブノードがあり、それが比較候補に見つからない（ノードが休止状態である）の場合、この比較にはペナルティが課されず、全部一致モード（ＷＭＭ）では、１つのＣＶＦにアクティブノードがあり、それが比較候補に見つからない（ノードが休止状態である）の場合、この比較にはペナルティが課される。

【００５０】

システムメタデータ分割（ＳＭＳ）は、入力システムメタデータを、意味のあるセキュリティ上の因果関係に分割し、サブジェクトスキャン／吸収により、カテゴリ化モジュールからの事前分類コンテナおよび未処理分析結果を使用して、システムメタデータからセキュリティ状況の対象／疑いが抽出され、対象は、セキュリティ応答／変数の関係を導出するための主な参照点として使用され、リスクスキャン／吸収により、セキュリティ状況のリスク要因が、事前に作成された分類コンテナおよび分類モジュールからの未処理分析結果を使用して、システムメタデータから抽出され、リスクは、そのようなリスクを呈している、またはリスクにさらされているターゲットとなる対象に関連しており、応答スキャン／吸収により、カテゴリ化モジュールからの事前に作成された分類コンテナおよび未処理分析結果を使用して、システムメタデータから、入力アルゴリズムによって生成されたセキュリティ状況の応答が抽出され、この応答は、そのような応答に値するとされるセキュリティ対象に関連付けられている。

【００５１】

ＭＣＭでは、フォーマット分割が、メタデータを認識されたフォーマットのルールおよび構文に従って分離し、分類し、ローカルフォーマットルールおよび構文は、ＭＣＭモジュールが予めフォーマットされたメタデータストリームを認識できるようにするための定義を含み、デバッグ追跡は、使用される変数、関数、メソッドおよびクラス、およびそれぞ

れの入力および出力変数の種別／内容を提供するコーディングレベルのトレースであり、アルゴリズム追跡は、アルゴリズム分析結果と結合されたセキュリティデータを提供するソフトウェアレベルのトレースであり、結果としてのセキュリティ決定（許可／ブロック）は、その決定（正当化）にどうやって到達したかの道筋と、各要素がそのセキュリティ決定を行うのに貢献した適切な重みと一緒に提供される。

【００５２】

メトリック処理（ＭＰ）において、セキュリティ応答Ｘは、ＳＰＭＡにより選ばれる結果としてのセキュリティ応答に寄与する一連のファクタを表し、初期ウェイトはＳＰＭＡによって決定され、パーセプション推論（ＰＤ）は、このセキュリティ応答の一部と、これに対応するシステムメタデータを使用して、セキュリティ応答の元のパーセプションを再現し、多次元型シリーズのパーセプション解釈は、ＰＤがＳＰＭＡのセキュリティ応答を採用して、該当する入力システムメタデータに関連付けすることで、ＳＰＭＡが元々使用しているとおりの知的「デジタルパーセプション」のフルスコープを再生成する様子を表しており、塗り潰し図形、積み上げ量、および多次元型は、知的アルゴリズムの「考え方」をうまく捉えるデジタルパーセプションである。

【００５３】

前記ＰＤでは、セキュリティ応答Ｘは根拠／理由付けの算出への入力として転送され、根拠／理由付けの算出、入出力削減（ＩＯＲ）モジュールの意図の供給を活用することによって、ＳＰＭＡのセキュリティ応答の正当化を決定し、前記ＩＯＲモジュールは、メタデータにリストされたさまざまな関数呼び出しの分割された入出力を使用し、前記メタデータ分割は前記ＭＣＭによって実行される。

【００５４】

ＰＯＥについて、入力システムメタデータは、未処理パーセプション生成（ＲＰ２）によって、ＣＶＦでパーセプションを生成するために使用される初期入力であり、ストレージ検索（ＳＳ）では、データ拡張ログから導出されたＣＶＦ（比較可能可変フォーマット）が、パーセプションストレージ（ＰＳ）のデータベース検索における判定基準として使用され、格付けでは、パーセプションは最終的なウェイトに応じて順序付けられ、データ拡張ログがパーセプションに適用されて、ブロック／許可の推奨を生成し、前記ＳＣＫＤは、未知の知識の期待される上限スコープを定義するために、ログをタグ付けし、データパースは、オリジナルのＳＰＭＡによって決定されたオリジナルの許可またはブロックの決定を出力するために、データ拡張ログおよび入力システムメタデータの基本解釈を行い、ＣＴＭＰは、前記ＰＯＥではパーセプションにしたがって決定事項を批判し、ルール実行（ＲＥ）においては、論理的に定義されたルールにしたがって決定事項を批判する。

【００５５】

メトリックの複合度では、円の外側の境界は、個々のメトリックに関する既知の知識のピークを表し、円の外縁に向かうにつれて、メトリックの複雑さがより大きいことを表し、一方、中心はメトリックの複雑さがより小さいことを表し、中央の明るい灰色は、現在のひとまとまりの適用済パーセプション観点のメトリック合成を表し、外側の濃い灰色は、システムによって格納され、一般に知られているメトリックの複合度を表し、ＩＤのゴールは、関連するメトリックの複合度を増やし、それによってパーセプション観点に複合度と量を掛けることができるようになることであり、暗い灰色の表面積は、現在のひとまとまりの適用済パーセプション観点の全範囲と、既知の上限に応じて残されたスコープの量を表し、拡張され複合度が高められると、メトリックはメトリックの複合度として戻され、メトリックの複合度は、メトリック変換の入力として渡され、メトリック変換は、個々のパーセプション観点から全体のパーセプション観点に戻し、それによって、最終出力が、意味付けられたパーセプション観点として組み立てられる。

【００５６】

ＳＣＫＤについて、既知データカテゴリ化（ＫＤＣ）は、既知の情報を入力からカテゴリ的に分割して、適切なＤＢアナロージークエリを実行することができるようにし、情報をカテゴリに分割し、前記分割されたカテゴリは個別に入力をＣＶＦＧに提供し、ＣＶＦＧは

、ＣＶＦフォーマットのカテゴリ情報を出力し、これは、ストレージ検索（ＳＳ）によって既知データスコープＤＢにおいて類似性をチェックするために使用され、ＳＳの結果にしたがって既知のデータの該当するスコープが各カテゴリにタグ付けされ、カテゴリ毎の未知の情報のタグ付けされたスコープは、未知データ合成器（ＵＤＣ）でオリジナルの入力の同じストリームに再構築される。

【００５７】

前記コンピュータ実装システムは、辞書的客観性探索（ＬＯＭ）であり、前記システムはさらに、

ａ）初期クエリ推論（ＩＱＲ）であって、質問が転送され、知識保持中枢（ＣＫＲ）を活用して質問の理解および回答／応答においてなくてはならない、欠落した詳細情報を解読するに、処理のために転送される、初期クエリ推論と、

ｂ）調査の明確化（ＳＣ）であって、前記質問および補足質問データが転送され、人間である対象から入力を受け取り、人間である対象に出力を送信し、明確化された質問／表明を形成する、調査の明確化と、

ｃ）表明の構築（ＡＣ）であって、表明または質問の形式で命題を受け取り、その命題に関連するコンセプトの出力を提供する、表明の構築と、

ｄ）回答の提示であって、ＡＣによって引き出された結論を、人間である対象と合理的訴求（ＲＡ）の両方に提示するためのインタフェースである、回答の提示と、

ｅ）階層的マッピング（ＨＭ）であって、関連するコンセプトをマップして、質問／表明の一貫性において、裏付けまたは競合を発見し、話題に一定の立場をとっていることの利点とリスクを計算する、階層的マッピングと、

ｆ）知識保持中枢（ＣＫＲ）であって、ＬＯＭのために知識を参照するためのメインデータベースである、知識保持中枢と、

ｇ）知識検証（ＫＶ）であって、クエリ能力およびＣＫＲへの吸収のために論理的に分割される必要がある、高い確信度および事前批判された知識を受け取る、知識検証と、

ｈ）応答の受け入れであって、ＬＯＭの応答を受け入れるか、批判とともに訴求するかのいずれかを行う、人間である対象に与えられた選択肢であり、応答が受け入れられた場合、それはＫＶによって処理され、確認された（高い確信度の）知識としてＣＫＲに格納でき、人間である対象が応答を受け入れなければ、人間によって与えられた訴求の理由をチェックして批判する、前記ＲＡに転送される、応答の受け入れと、

ｉ）管理された人工知能的サービスプロバイダ（ＭＡＩＳＰ）であって、ＣＫＲのマスターインスタンスとともに、ＬＯＭのインターネットクラウドインスタンスを実行し、ＬＯＭをフロントエンドサービス、バックエンドサービス、サードパーティアプリケーションの依存関係、情報源、およびＭＮＳＰのクラウドに接続する、管理された人工知能的サービスプロバイダをさらに備える。

【００５８】

フロントエンドサービスは、人工知能的パーソナルアシスタント、通信アプリケーションおよびプロトコル、ホームオートメーション、および医療用途を含み、バックエンドサービスには、オンラインショッピング、オンライン交通機関、処方箋注文があり、フロントエンドサービスおよびバックエンドサービスは、情報の転送およびプロトコルの標準化を可能にする、文書化されたＡＰＩインフラストラクチャを介してＬＯＭと相互作用し、ＬＯＭは、自動化された調査機構（ＡＲＭ）を介して外部情報源から知識を取り出す。

【００５９】

言語学的構築（ＬＣ）は、人間である対象および類似したモジュールからの未処理の質問／表明の入力を解釈し、言語構文の論理的な分割を生成し、コンセプト発見（ＣＤ）は、明確化された質問／表明内の関心ポイントを受け取り、ＣＫＲを活用することによって関連するコンセプトを導出し、コンセプトの優先順位付け（ＣＰ）は、該当するコンセプトを受け取り、それらを特定性および一般性を表す論理的な複数の層に整理し、応答分割ロジック（ＲＳＬ）は、ＬＣを活用することで人間の応答を理解し、適切かつ有効な応答を、最初の明確化リクエストと関連づけ、それによって、ＳＣの目的を達成し、ＬＣは、出

力フェーズで再活用され、オリジナルの質問／表明を修正し、ＳＣによって受信された補足的情報を含むようにし、コンテキスト構築（ＣＣ）は、表明の構築（ＡＣ）のメタデータと、人間である対象からの証拠を使用して、クリティカルシンキングのためにＣＴＭＰに未処理の事実を提供し、決定事項比較（ＤＣ）は、事前批判された決定事項と批判された後の決定事項との間の重複を判断し、コンセプト互換性検出（ＣＣＤ）は、オリジナルの質問／表明からのコンセプト的な派生事項を比較して、論理的な互換性の結果を確認し、利益／リスク計算（ＢＲＣ）は、ＣＣＤからの互換性の結果を受け取り、コンセプト構成に暗に含まれた変数の傾斜を包含する一様な決定を形成するために、利益とリスクを重み付けし、コンセプト連携（ＣＩ）は、ＡＣのコンセプトに関連する属性を、調査の明確化（ＳＣ）を介して、人間である対象から収集された情報の一部に割り当てる。

【００６０】

前記ＩＱＲの内部では、ＬＣは前記オリジナルの質問／表明を受け取り、質問／表明は言語的に分離されているおり、ＩＱＲはＣＫＲを活用して一度に個々の語句を処理し、ＣＫＲを参照することで、ＩＱＲは、単語／フレーズの曖昧性を考慮しながら、可能な選択肢の候補を考慮する。

【００６１】

調査の明確化（ＳＣ）はＩＱＲ８０２からの入力を受け取り、前記入力には、達成されるべきオリジナルの質問／表明に対する客観的な回答のために、人間の被験者が対応することになる、一連のリクエストされた明確化事項が含まれ、前記明確化事項に対してなされる対応はどれも、応答分割ロジック（ＲＳＬ）に転送され、対応と明確化リクエストを相関させ、リクエストされた明確化事項と並行して、明確化の言語学的連携がＬＣに提供され、前記連携には、リクエストされた明確化事項と言語構造との内部関係が含まれ、この内部関係によって前記ＲＳＬが前記オリジナルの質問／表明を修正でき、それによって、ＬＣが前記明確化された質問を出力する。

【００６２】

前記明確化された質問／表明を受け取った、表明の構築について、ＬＣは、この問題を関心ポイントに分解し、コンセプト発見に渡し、ＣＤは、ＣＫＲを活用することによって関連するコンセプトを導出し、コンセプトの優先順位付け（ＣＰ）はコンセプトを論理的な複数の層に整理し、最上位層には最も一般的なコンセプトが割り当てられ、より下位の層にはより特定のコンセプトが割り当てられ、最上位層は、モジュールの入力として階層的マッピング（ＨＭ）に転送され、情報の並列転送において、ＨＭは関心ポイントを受信し、この関心ポイントは、その依存モジュールであるコンセプト連携（ＣＩ）によって処理され、ＣＩは、ＣＫＲでインデックス付けされた情報にアクセスすることによって、そのような関心ポイントに属性を割り当て、ＨＭが内部プロセスを完了すると、その最終出力は、導出されたコンセプトの互換性がテストされ、ある立場の利益／リスクが重み付けされて返された後、ＡＣに返される。

【００６３】

ＨＭについて、ＣＩは、２つのコンセプト同士の互換性／競合レベルを識別する、ＣＣＤへの入力を提供し、このような互換性／競合データは、問題について全体論的な統一された立場を取ることに関する、前記互換性と競合を利益とリスクに変換する、ＢＲＣに転送され、そのような立場は、リスク／利益ファクタとともに、モジュールの出力としてＡＣに転送され、情報フローのループを含むシステムは、知性の傾向が、質問／表明の主観的性質として徐々に補足される、徐々に構築された客観的応答、を表しており、ＣＩは、関心ポイントを受け取り、優先順位付けられたコンセプトの最上位層にしたがって、それぞれの関心ポイント解釈する。

【００６４】

ＲＡについて、コアロジックは言語テキストを処理し、結果を返し、前記結果が高い確信度の場合、前記結果はＣＫＲへの適切な吸収のために知識検証（ＫＶ）に渡され、前記結果が低い確信度の場合、前記結果はＡＣへ渡され、の適切な吸収のために知識検証（ＫＶ）に渡され、自己批評のサイクルを継続し、コアロジックは、言語要素のない事前批判さ

れた決定としてＬＣからの入力を受け取り、前記決定は主観的意見としてＣＴＭＰに転送され、決定はまた、ＡＣからのメタデータおよび人間である対象からの見込みのある証拠を使用して、未処理の事実をＣＴＭＰに、入力する「客観的事実」として与える、コンテキスト構築（ＣＣ）に転送され、ＣＴＭＰが２つの必須入力を受け取ると、このような情報は「客観的意見」に到達する最良の試みを出力するために処理され、前記意見は、ＲＡ内で、批判された後の決定として取り扱われ、事前批判された決定と批判された後の決定の両方が、両方の決定の間の重複のスコープを決定する決定事項比較（ＤＣ）に転送され、前記不服申し立ては、次に、真実であると認められるか、この訴求が無効である理由を説明するために、対照的要素が改善され、シナリオを認めるのか改善するのかとは無関係に、高い確信度の結果８４６はＫＶに渡され、低い確信度の結果はさらなる分析のためにＡＣ８０８に渡される。

【００６５】

ＣＫＲについて、情報の単位は、単位知識フォーマット（ＵＫＦ）に格納され、ルール構文形式（ＲＳＦ）は、参照ルールの追跡を維持するための構文的標準のセットであり、ＲＳＦ内の複数のルールの単位を利用して、単一の目的または処置を記述することができ、ソース属性は、要求された情報源を追跡する複合データの集合であり、ＵＫＦクラスタは、管轄区域的に分割された情報を定義するためにリンクされたＵＫＦの変種の連鎖で構成されており、ＵＫＦ２には、メインのターゲットされた情報が含まれており、ＵＫＦ１にはタイムスタンプ情報が含まれているため、無限回帰を避けるためにタイムスタンプフィールドそのものは省略されており、ＵＫＦ３にはソース属性情報が含まれているため、無限回帰を避けるためにソースフィールドそのものは省略されており、すべてのＵＫＦ２には少なくとも１つのＵＫＦ１と１つのＵＫＦ３が添付されていなければならない。さもなければ、クラスタ（シーケンス）は不完全とみなされ、そこにある情報は、ＬＯＭシステム全体の汎用ロジックでは処理できず、中央のＵＫＦ２とそれに対応するＵＫＦ１およびＵＫＦ３の間には、リンクされた橋の役割を果たすＵＫＦ２ユニットがあり、一連のＵＫＦクラスタはＫＣＡによって処理され、導出された表明を形成し、知識裏付け分析（ＫＣＡ）は、ＵＫＦのクラスタ化された情報を、意見のあるスタンスに関する証拠を裏付けるために比較し、ＫＣＡの処理が完了した後、ＣＫＲは、話題についての結論となる、独断的な立場を出力することができる。

【００６６】

ＡＲＭについて、ユーザ活動で表されるように、ユーザがＬＯＭと対話するとき、コンセプトは質問／表明に対する回答／応答に関連して直接的または間接的にもたらされ、ユーザ活動は、リクエストされたがまだ利用不可能なコンセプトのリストに示されるように、ＣＫＲが、それに関する情報がほとんど全くないコンセプトを最終的に生み出すことが期待され、コンセプトのソートおよび優先順位付け（ＣＳＰ）では、コンセプトの定義は、３つの独立したソースから受信され、情報リクエストのリソースに優先順位付けをするために集約され、前記情報源によって提供されたデータは、それらをリクエストしたコンセプトの定義にしたがって情報アグリゲータ（ＩＡ）で受信され、解析さかれ、該当するメタデータは保持され、情報は相互参照分析（ＣＲＡ）に送られ、そこでは、受信された情報がＣＫＲからの既存の知識と比較され、それを考慮して構築される。

【００６７】

個人情報プロファイル（ＰＩＰ）は、多数の潜在的なエンドポイントおよびフロントエンドを介して個々人の個人情報が格納される場所であり、個々人の情報はＣＫＲからは隔離されているが、ＬＯＭシステム全体にわたる汎用ロジックでは使用可能であり、人工知能アプリケーションに関する個人情報は暗号化され、ＵＫＦフォーマットのパーソナルＵＫＦクラスタプールに格納され、情報匿名化プロセス（ＩＡＰ）では、情報は、個人を特定可能な情報が取り除かれた後、ＣＫＲに補充され、相互参照分析（ＣＲＡ）では、受信した情報は、ＣＫＲからの既存の知識と比較され、それを考慮して構築される。

【００６８】

生活の管理と自動化（ＬＡＡ）は、一体化プラットフォーム上で、様々なインターネット

対応の機器およびサービスと接続し、積極的意思決定（ＡＤＭ）は、フロントエンドサービス、バックエンドサービス、ＩｏＴデバイスの可用性と機能性を考慮し、ＦＡＲＭにしたがって利用可能な支出ルールと金額を考慮しており、ＦＡＲＭは、人間が前記モジュールに対する判断基準、制限、およびスコープを手作業で定義して、ＡＤＭ８１３Ｄの活動の管轄範囲がどこまでかということについて、ＡＤＭ８１３Ｄに知らせ、暗号通貨での資金がデジタルウォレットに預けられ、ＩｏＴ連携モジュール（ＩＩＭ）は、どのＩｏＴデバイスが利用可能であるかについてのデータベースを維持管理し、データフィード８６２Ｂは、ＩｏＴ対応デバイス８６２ＡがＬＡＡ８１２Ｄに情報を送信するときを表す。

【００６９】

前記システムは、ユーザからの、個人を識別可能なデータのリクエストをモニターすることで、非倫理的および／または違法な物質の有無をチェックする挙動監視（ＢＭ）をさらに備え、メタデータ集約（ＭＤＡ）では、ユーザ関連データが外部サービスから集約され、ユーザのデジタル上の身元を明らかにすることができ、このような情報が、帰納／演繹、最終的にはＰＣＤに転送され、そこでは洗練された分析がＭＮＳＰからの裏付けファクタを用いて実行され、ＰＩＰが宛先である、認証済みのユーザからのすべての情報は、情報トラッキング（ＩＴ）を通過し、挙動ブラックリストに照らしてチェックされ、未然犯罪検知（ＰＣＤ）では、未然犯罪の結論を出すために、演繹的情報および帰納的情報がマージされ分析され、ＰＣＤは、挙動ブラックリストを直接参照するＣＴＭＰを利用することで、帰納および演繹によって生成された立場を検証し、ブラックリスト管理機関（ＢＭＡ）は、ＭＮＳＰのクラウドサービスフレームワーク内で稼働する。

【００７０】

ＬＯＭは、ある個人の生活でパーソナライズされたポートフォリオを管理するように構成され、ＬＯＭは最初の質問を受け取り、ＬＯＭの内部審議プロセスを介して結論に至り、ＬＯＭは、ＬＯＭがそこからデータを受信して制御できるインターネット対応デバイスに接続するＬＡＡモジュールに接続し、文脈化では、ＬＯＭは申し立てを構成する際に欠落しているリンクを推論し、ＬＯＭはそのロジックにより、オリジナルの表明によって提起されたジレンマを解決するために、この状況に関するある変数をまず知るか仮定するかしなければならないということを解読する。

【００７１】

前記コンピュータ実装システムは、線形量子情報転送（ＬＡＱＩＴ）であり、前記システムは、

ａ）論理的に構築された構文により、再帰的に一貫したカラーシーケンスを繰り返し、

ｂ）英語のアルファベットで翻訳を行うために、前記シーケンスを再帰的に使用し、

アルファベットの「ベース」レイヤを構築するとき、前記カラーシーケンスは、カラーチャネルでは、短縮された不均一なウェイトで使用され、構文定義のために残されているスペースは、将来の潜在的な使用および拡張のために予約されており、

複雑なアルゴリズムが、ＬＡＱＩＴを使ってそのログイベントおよびステータスレポートを報告し、ログイベントおよびステータスレポートは自動的に生成され、前記ステータスレポート／ログレポートを、可搬なテキストベースのＬＡＱＩＴ構文へと変換し、構文的に安全出ない情報はデジタル的に転送され、前記可搬なテキストベースの構文は、非常に読みやすいＬＡＱＩＴの可視構文（線形モード）へ変換され、鍵が人間の記憶に対して最適化されていて、比較的短い図形のシーケンスに基づいており、

局所的に安全でないテキストが送信者によって入力され、受信者に手出され、前記テキストが、可搬な暗号化されたテキストベースのＬＡＱＩＴ構文へと変換され、構文的に安全な情報はデジタル的に転送され、前記データが、可視的に暗号化されたＬＡＱＩＴ構文へと変換され、

インクリメンタル認識効果（ＩＲＥ）が情報伝達のチャネルであり、情報が完全に伝達される前に、情報の単位の完全な形を認識し、この予測可能インデックスの効果が、単語から単語への遷移を表示することによって組み込まれており、近似認識効果（ＰＲＥ）は情報伝達のチャネルであり、壊れているか、混ざっているか、あるいは変更されているかの

いずれかであっても、情報の単位の完全な形を認識する。

【００７２】

ＬＡＱＩＴの線形モードでは、ブロックは線形モードの「基本レンダリング」バージョンを示し、ポイントは、暗号化の欠如を表示しており、単語セパレータでは、前記図形の色は単語に続く文字を表し、単語と次の単語との間の区切りとして機能し、単一ビューゾーンは、より大きな文字、したがってより少ない情報をともなう、小さなビューゾーンを組み込み、二重ビューゾーンには、ピクセル当たりより多くのアクティブ文字が存在し、陰影カバーは、観察者の主なフォーカスがビューゾーン上にあるように、入って来る文字および外に出て行く文字を曇らせる。

【００７３】

広範囲の暗号化レベルが可能な原子モードにおいては、ベースの主なキャラクタ参照は、どの文字が定義されているかについて一般原理を指定し、キッカーは、ベースと同じ色の範囲で存在し、特定の文字を正確に定義し、読み取り方向では、情報伝達の読み取りは、軌道輪１の頂上にある正方形から始まり、一度軌道輪が完結すると、次の軌道輪の頂上にある正方形から読み込みが続けられ、入口／出口ポータルは、キャラクタ（そのベース）の生成と破壊のポイントであり、該当する軌道に属する、新しいキャラクタが、ポータルから現れ、時計回りにその位置にスライドし、原子核は、その単語に続くキャラクタを定義し、

ワードナビゲーションでは、各ブロックは、画面の左側に単語全体（あるいは、複数の単語を分子モードで）を表しており、ある単語が表示されると、それぞれのブロックが外側に右の方に移動し、その単語が完成するとブロックは後退し、ナビゲーションブロックの色／形は、この単語の最初の文字のベースと同じ色／形であり、センテンスナビゲーションでは、各ブロックは単語のクラスタを表しており、クラスタとは、単語ナビゲーションペインに収まる最大量の単語であり、原子状態生成は、インクリメンタル認識効果（ＩＲＥ）を誘発する遷移であり、このような遷移により、ベースは入口／出口ポータルから現われ、それらのキッカーは隠され、時計回りに移動してそれらの位置を占め、原子状態拡張は、近似認識効果（ＰＲＥ）を誘発する遷移であり、一度ベースがその位置に達すると、それらのベースは情報状態提示の「拡張」シーケンスにおいて外側に移動し、これにより、キッカー９２５が明らかになり、それによって、情報状態の特定の定義を提示することができ、原子状態破壊は、インクリメンタル認識効果（ＩＲＥ）を誘発する遷移であり、キッカーを再び覆うために、ベースは後退しており（拡張シーケンスを逆転して）、ベースは時計回りにスライドして入口／出口ポータルに達している。

【００７４】

図形難読化では、標準の四角形が５つの視覚的に区別できる図形に置き換えられ、構文内の図形の分散は、原子プロファイルの戦略的ポイントにダッド（偽物）文字を挿入することを可能にし、ダッド文字はメッセージの本当の意図された意味を難読化させ、文字が真であるか偽かを解読することは、安全かつ一時的に転送された解読鍵によって行われ、

リダイレクトボンドでは、ボンドが２つの文字を結合し、読み込みの流れを変更し、典型的な時計回りの読み込みパターンから始まり、合法／非偽の文字を打ち上げ（始まって）着地する（終わる）ボンドに遭遇すると、読み込みパターンを変更して着地文字を再開し、

放射性元素では、文字が偽物であるか否かの評価を覆すことができるいくつかの要素は「音を立てる」ことができ、図形は暗号化で使用可能な図形を示しており、中心要素は、単語の直後に来るキャラクタを定義する、軌道の中心要素を示している。

【００７５】

リダイレクトボンドでは、ボンドは「打ち上げ」文字から始まり、「着地」文字で終わり、どちらの文字も、ダッドであってもなくてもかまわなく、それらのいずれもがダッドでない場合、ボンドは読み取り方向および位置を変更し、片方または両方がダッドである場合、ボンド全体を無視しなければならず、さもなければ、メッセージが正しく解読されず、ボンドキー定義では、情報状態の読み取りの際にボンドに従わなければならない場合、

それは、暗号鍵で具体的に定義されているかどうかによって異なる。
【００７６】
シングルクラスタでは、両方の隣接ノードが非放射性であるため、クラスタのスコープが定義され、キーは二重クラスタを有効と指定しているため、前記要素は、それがそもそも放射性でない場合に処理され、ダブルクラスタでは、キー定義はダブルクラスタを活性と定義するため、他のすべてのサイズのクラスタは、メッセージを復号化している間、休止状態であるとみなされ、正しくない解釈は、インタプリタがダブルクラスタを逆順シーケンス（偽陽性）として扱わなかった様子を示している。
【００７７】
分子モードでは、暗号化およびストリーミングが可能であり、秘密辞書攻撃抵抗では、メッセージの誤った解読は、「赤いニシン」という別のメッセージにつながり、分子ごとに複数のアクティブワードを用い、単語は分子プロシージャの間に並行して提示され、これによって、表面積比当たりの情報を増加させるが、一貫した移行速度であり、バイナリおよびストリーミングモードはストリーミングモードを示し、典型的な原子構成では読み取りモードはバイナリであり、バイナリモードは、中心要素が単語に続くキャラクタを定義することを示しており、ストリーミングモードに準拠した暗号化が有効になっている場合を除いて、分子モードもまたバイナリであり、ストリーミングモードは、軌道内で特殊文字を参照する。
【００７８】
前記コンピュータ実装システムは、ベース接続協調攻撃統合ノード（ＢＣＨＡＩＮ）を伴った普遍的ＢＣＨＡＩＮ全接続（ＵＢＥＣ）であり、前記システムはさらに、
ａ）通信ゲートウェイ（ＣＧ）であって、ＢＣＨＡＩＮノードが、そのハードウェアインタフェースと対話し、その後、他のＢＣＨＡＩＮノードとの通信に至るための、主要なアルゴリズムである、通信ゲートウェイと、
ｂ）ノード統計調査（ＮＳＳ）であって、リモートノードの挙動パターンを解釈する、ノード統計調査と、
ｃ）ノードエスケープインデックスであって、隣接ノードが知覚ノード近傍を回避する可能性を追跡する、ノードエスケープインデックスと、
ｄ）ノード飽和インデックスであって、知覚ノードの検出範囲内にあるノードの量を追跡する、ノード飽和インデックスと、
ｅ）ノード一貫性インデックスであって、知覚ノードによって解釈された、ノードサービスの品質を追跡し、高いノード一貫性インデックスは、周囲の隣接ノードがより多くの可用性稼働時間およびパフォーマンスの一貫性を有する傾向があることを示し、２つの目的で用いられるノードは、一貫性インデックスが低くなる傾向があり、ＢＣＨＡＩＮネットワーク専用のノードは、高い値を示す、ノード一貫性インデックスと、
ｆ）ノードオーバーラップインデックスであって、知覚ノードによって解釈される、ノード同士の互いの重複の量を、互いに追跡する、ノードオーバーラップインデックスをさらに備える。
【００７９】
前記システムは、
ａ）カスタムチェーン認識モジュール（ＣＲＭ）であって、ノードによって過去に登録された、ＡｐｐｃｈａｉｎｓまたはＭｉｃｒｏｃｈａｉｎｓを含むカスタムチェーンと接続し、ＣＲＭは、ＭｅｔａｃｈａｉｎまたはＭｉｃｒｏｃｈａｉｎのＭｅｔａｃｈａｉｎエミュレータの、Ａｐｐｃｈａｉｎのセクションでアップデートが検出されたとき、ＢＣＨＡＩＮプロトコルの残りの部分を通知する、カスタムチェーン認識モジュールと、
ｂ）コンテンツクレームデリバリ（ＣＣＤ）であって、検証されたＣＣＲを受信し、その後、リクエストを満たすために、該当するＣＣＦを送信する、コンテンツクレームデリバリと、
ｃ）動的ストラテジー適応（ＤＳＡ）であって、創作モジュールを使用して、最適化ストラテジー選択アルゴリズム（ＯＳＳＡ）を介してシステムが好む複雑なストラテジーを

混成することによって、新しいストラテジー配置を動的に生成する、ストラテジー生成モジュール（ＳＣＭ）を管理し、新しいストラテジーは、フィールド乱雑解釈（ＦＣＩ）によって提供される入力にしたがって変化し、新しいストラテジーは、フィールド乱雑解釈（ＦＣＩ）によって提供される入力にしたがって変化する、動的ストラテジー適応と、

ｄ）暗号化デジタル経済交流（ＣＤＥＥ）であって、ＵＢＥＣプラットフォームインタフェース（ＵＰＩ）の下でグラフィカルユーザインタフェース（ＧＵＩ）によって管理される様々な経済人格を有し、人格Ａでは、ノードリソースは、消費するものと一致するものだけが消費され、人格Ｂは、利益マージンが所定の値より大きい限り、可能な限り多くのリソースを消費し、人格Ｃは、取引通貨を通じて作業単位を支払い、人格Ｄでは、ノードのリソースは、コンテンツの消費であろうと、金銭的な補償であろうと、極力多くのものを期待してなんら制限なしに消費する、暗号化デジタル経済交流と、

ｅ）仕事現状の解釈（ＣＷＳＩ）であって、Ｍｅｔａｃｈａｉｎのインフラ経済セクションを参照することで、仕事量クレジットに関してこのノードの現在の黒字または赤字を判断する、仕事現状の解釈と、

ｆ）経済的に考慮された労働賦課（ＥＣＷＩ）であって、選択された経済人格を、現行の作業剰余／赤字とともに考慮し、現在より多くの作業が行われなければならないかどうかを評価する、経済的に考慮された労働賦課と、

ｇ）象徴的再帰的知性向上（ＳＲＩＡ）であって、コードの目的を理解することによって、アルゴリズムのソースコードを改善することができる、ＬＩＺＡＲＤと、世代の仮想プログラムのバージョンをエミュレートすることができる、ｌ２ＧＥと、分散型の方法で複雑なデータ偏重のプログラムを実行できる、無秩序に接続されたノードの巨大なネットワークである、ＢＣＨＡＩＮネットワークを含む、異なるアルゴリズムの三者関係である、象徴的再帰的知性向上と、をさらに備える。

【図面の簡単な説明】

【００８０】

本発明は、以下の添付図面と併せて詳細な説明を読むことで、より十分に理解される。

図１～２６は、クラウドおよび階層化情報セキュリティ（ＣＴＩＳ）による重要インフラストラクチャ防護および報復（ＣＩＰＲ）（合わせてＣＩＰＲ／ＣＴＩＳとして知られる）を示す概略図であり、より詳細には、

【図１】セキュリティの解釈に関する複数の観点に対する定義が、分析のための方法論として提示される様子を示す概略図である。

【図２】セキュリティの解釈に関する複数の観点に対する定義が、分析のための方法論として提示される様子を示す概略図である。

【図３】セキュアＥＩ^{2}（エクストラネット、イントラネット、インターネット）のネットワーキングのための、クラウドベースの管理された暗号化セキュリティサービスアーキテクチャを示す概略図である。

【図４】マネージドネットワークおよびセキュリティサービスプロバイダ（ＭＮＳＰ）の概要を示す概略図である。

【図５】マネージドネットワークおよびセキュリティサービスプロバイダ（ＭＮＳＰ）の概要を示す概略図である。

【図６】マネージドネットワークおよびセキュリティサービスプロバイダ（ＭＮＳＰ）の概要を示す概略図である。

【図７】マネージドネットワークおよびセキュリティサービスプロバイダ（ＭＮＳＰ）の概要を示す概略図である。

【図８】マネージドネットワークおよびセキュリティサービスプロバイダ（ＭＮＳＰ）の概要を示す概略図である。

【図９】ＬＩＺＡＲＤクラウドベースの暗号化セキュリティについてのリアルタイムセキュリティ処理を示す概略図である。

【図１０】エネルギーシステムにおける、クラウドおよび階層化情報セキュリティ（ＣＴＩＳ）による重要インフラストラクチャ防護および報復（ＣＩＰＲ）の例を示す概略図で

ある。
【図１１】ステージ１-初回システム侵入を示す概略図である。
【図１２】ステージ２-初期段階トロイの木馬の配置を示す概略図である。
【図１３】ステージ３-高度な実行可能マルウェアのダウンロードを示す概略図である。
【図１４】ステージ４-侵入防御／予防システムの攻略を示す概略図である。
【図１５】ハッカー所望の挙動および実際のセキュリティ応答を示す概略図である。
【図１６】スケジュールされた内部認証プロトコルアクセス（ＳＩＡＰＡ）を示す概略図である。
【図１７】ルートレベルアクセス権および標準レベルアクセス権を示す概略図である。
【図１８】監督審査を示す概略図である。
【図１９】反復型知的成長／知的進化（Ｉ^{2}ＧＥ）を示す概略図である。
【図２０】インフラシステムを示す概略図である。
【図２１】犯罪システム、インフラシステム、およびパブリックインフラを示す概略図である。
【図２２】外来コード改訂が外来コードを構文的に再現することで、起こりうる未検知の悪意のエクスプロイトを軽減する様子を示す概略図である。
【図２３】外来コード改訂が外来コードを構文的に再現することで、起こりうる未検知の悪意のエクスプロイトを軽減する様子を示す概略図である。
【図２４】再帰的デバッグがコードセグメントをループ処理する様子を示す概略図である。
【図２５】再帰的デバッグがコードセグメントをループ処理する様子を示す概略図である。
【図２６】要求マップマッチングの内部動作原理を示す概略図である。　図２７～図４２は、サイバースペースにおける秘密オペレーションによる秘密機械学習（ＭＡＣＩＮＴ）および報復を示す概略図であり、より詳細には、
【図２７】知的情報の管理、閲覧、および制御図６６に、知的情報の管理、閲覧、および制御を示す概略図である。
【図２８】挙動分析による処置を示す概略図である。
【図２９】犯罪システムおよび犯罪システムに対する報復を示す概略図である。
【図３０】犯罪システムおよび犯罪システムに対する報復を示す概略図である。
【図３１】ＭＡＣＩＮＴのフローを示す概略図である。
【図３２】ＭＡＣＩＮＴのフローを示す概略図である。
【図３３】ＭＡＣＩＮＴ秘密オペレーションの概要および、犯人が企業システムをエクスプロイトする様子を示す概略図である。
【図３４】ビッグデータを使用する長期／深層スキャンの詳細を示す概略図である。
【図３５】信用プラットフォーム上で任意コンピュータが検索される様子を示す概略図である。
【図３６】信用プラットフォームからの既知の二重または三重スパイが、将来の科学捜査的調査に関わるようになる様子を示す概略図である。
【図３７】ＩＳＰのＡＰＩを実行するために信用プラットフォームを使用する様子を示す概略図である。
【図３８】信用プラットフォームを使用して、ソフトウェアベンダおよびハードウェアベンダが提供するセキュリティＡＰＩを実行し、設置されたバックドアをエクスプロイトする方法を示す概略図である。
【図３９】汎用エクスプロイトおよびカスタマイズ可能なエクスプロイが、任意コンピュータおよび犯罪コンピュータに適用される様子を示す概略図である。
【図４０】汎用エクスプロイトおよびカスタマイズ可能なエクスプロイが、任意コンピュータおよび犯罪コンピュータに適用される様子を示す概略図である。
【図４１】汎用エクスプロイトおよびカスタマイズ可能なエクスプロイが、任意コンピュータおよび犯罪コンピュータに適用される様子を示す概略図である。

【図４２】犯罪システムをモニターするために、長期優先フラグが信用プラットフォームにプッシュされる様子を示す概略図である。　図４３～図６８は、論理的推論によるゼロデータベースの演繹型リアルタイム防御（ＬＩＺＡＲＤ）を示す概略図であり、より詳細には、
【図４３】ＬＩＺＡＲＤの依存構造を示す概略図である。
【図４４】ＬＩＺＡＲＤの依存構造を示す概略図である。
【図４５】ＬＩＺＡＲＤの概要を示す概略図である。
【図４６】ＬＩＺＡＲＤに関する主要なアルゴリズムの機能の概要を示す概略図である。
【図４７】静的コア（ＳＣ）の内部動作原理を示す概略図である。
【図４８】内側コアが、システムの必須のコア機能を収容している様子を示す概略図である。
【図４９】ダイナミックシェル（ＤＳ）の内部動作原理を示す概略図である。
【図５０】ダイナミックシェル上のモジュールを知的に変更、作成、および処分するイテレーションモジュール（ＩＭ）を示す概略図である。
【図５１】セキュリティを改善するためにコードを繰り返し実行するためのメインロジックである、イテレーションコアを示す概略図である。
【図５２】差分変更アルゴリズム（ＤＭＡ）の論理プロセスを示す概略図である。
【図５３】差分変更アルゴリズム（ＤＭＡ）の論理プロセスを示す概略図である。
【図５４】差分変更アルゴリズム（ＤＭＡ）の論理プロセスを示す概略図である。
【図５５】差分変更アルゴリズム（ＤＭＡ）の論理プロセスを示す概略図である。
【図５６】差分変更アルゴリズム（ＤＭＡ）の論理プロセスを示す概略図である。
【図５７】差分変更アルゴリズム（ＤＭＡ）の論理プロセスを示す概略図である。
【図５８】仮想難読化の概要を示す概略図である。
【図５９】仮想難読化の監視と応答の側面を示す概略図である。
【図６０】仮想難読化の監視と応答の側面を示す概略図である。
【図６１】仮想難読化の監視と応答の側面を示す概略図である。
【図６２】疑わしいエンティティからアップロードされたりそこへダウンロードされたりするすべての情報を追跡する、データリコール追跡を示す概略図である。
【図６３】疑わしいエンティティからアップロードされたりそこへダウンロードされたりするすべての情報を追跡する、データリコール追跡を示す概略図である。
【図６４】データリコールトリガの内部動作原理を示す概略図である。
【図６５】データリコールトリガの内部動作原理を示す概略図である。
【図６６】極秘データを遮断し、実データと模擬データとを混合するデータ選択を示す概略図である。
【図６７】挙動分析の内部動作原理を示す概略図である。
【図６８】挙動分析の内部動作原理を示す概略図である。　図６９～図１２０は、クリティカルシンキング・メモリおよびパーセプション（ＣＴＭＰ）を示す概略図であり、より詳細には、
【図６９】ＣＴＭＰのメインロジックを示す概略図である。
【図７０】パーセプションの視点を示す概略図である。
【図７１】ＣＴＭＰの依存構造を示す概略図である。
【図７２】ＣＴＭＰの依存構造を示す概略図である。
【図７３】ＣＴＭＰの依存構造を示す概略図である。
【図７４】ＣＴＭＰにおける知的情報を処理する最終ロジックを示す概略図である。
【図７５】直感的／認知的および思考的／論理的の２つの主要な入力がＣＴＭＰを表している単一の最終出力に同化していくことを示す概略図である。
【図７６】オリジナルの選択パターンマッチングアルゴリズム（ＳＰＭＡ）で行われる、知的思考のスコープを示す概略図である。
【図７７】パーセプションおよびルールを介してＣＴＭＰにより実行されるクリティカルシンキングと並置される、従来のＳＰＭＡを示す概略図である。

【図７８】従来の現行ルールと比較して妥当ルールが生成される様子を示す概略図である。
【図７９】パーセプションマッチング（ＰＭ）モジュールを示す概略図である。
【図８０】パーセプションマッチング（ＰＭ）モジュールを示す概略図である。
【図８１】ルール構文導出／生成を示す概略図である。
【図８２】ルール構文導出／生成を示す概略図である。
【図８３】ルール構文導出／生成を示す概略図である。
【図８４】ルール構文導出／生成を示す概略図である。
【図８５】ルール構文導出／生成を示す概略図である。
【図８６】ルール文法フォーマット分割（ＲＳＦＳ）モジュールの動作原理を示す概略図である。
【図８７】ルール文法フォーマット分割（ＲＳＦＳ）モジュールの動作原理を示す概略図である。
【図８８】ルール充足度パーサ（ＲＦＰ）の動作原理を示す概略図である。
【図８９】充足デバッガを示す概略図である。
【図９０】充足デバッガを示す概略図である。
【図９１】ルール実行を示す概略図である。
【図９２】シーケンシャルメモリ編成を示す概略図である。
【図９３】シーケンシャルメモリ編成を示す概略図である。
【図９４】非シーケンシャルメモリ編成を示す概略図である。
【図９５】メモリ認識（ＭＲ）を示す概略図である。
【図９６】メモリ認識（ＭＲ）を示す概略図である。
【図９７】メモリ認識（ＭＲ）を示す概略図である。
【図９８】フィールド解釈ロジック（ＦＩＬ）を示す概略図である。
【図９９】フィールド解釈ロジック（ＦＩＬ）を示す概略図である。
【図１００】自動化パーセプション発見メカニズム（ＡＰＤＭ）を示す概略図である。
【図１０１】自動化パーセプション発見メカニズム（ＡＰＤＭ）を示す概略図である。
【図１０２】未処理パーセプション生成（ＲＰ２）を示す概略図である。
【図１０３】比較可能可変フォーマットジェネレータ（ＣＶＦＧ）の論理フローを示す概略図である。
【図１０４】ノード比較アルゴリズム（ＮＣＡ）を示す概略図である。
【図１０５】システムメタデータ分割（ＳＭＳ）を示す概略図である。
【図１０６】システムメタデータ分割（ＳＭＳ）を示す概略図である。
【図１０７】メタデータカテゴリ化モジュール（ＭＣＭ）を示す概略図である。
【図１０８】メタデータカテゴリ化モジュール（ＭＣＭ）を示す概略図である。
【図１０９】メトリック処理（ＭＰ）を示す概略図である。
【図１１０】パーセプション推論（ＰＤ）の内部設計を示す概略図である。
【図１１１】パーセプション推論（ＰＤ）の内部設計を示す概略図である。
【図１１２】パーセプション観察者エミュレータ（ＰＯＥ）を示す概略図である。
【図１１３】パーセプション観察者エミュレータ（ＰＯＥ）を示す概略図である。
【図１１４】パーセプション観察者エミュレータ（ＰＯＥ）を示す概略図である。
【図１１５】パーセプション観察者エミュレータ（ＰＯＥ）を示す概略図である。
【図１１６】意味付けの導出（ＩＤ）を示す概略図である。
【図１１７】意味付けの導出（ＩＤ）を示す概略図である。
【図１１８】自己批判的知識密度（ＳＣＫＤ）を示す概略図である。
【図１１９】自己批判的知識密度（ＳＣＫＤ）を示す概略図である。
【図１２０】自己批判的知識密度（ＳＣＫＤ）を示す概略図である。　図１２１～１６５は、辞書的客観性探索（ＬＯＭ）を示す概略図であり、より詳細には、
【図１２１】辞書的客観性探索（ＬＯＭ）のメインロジックを示す概略図である。
【図１２２】管理された人工知能的サービスプロバイダ（ＭＡＩＳＰ）を示す概略図であ

る。
【図１２３】管理された人工知能的サービスプロバイダ（ＭＡＩＳＰ）を示す概略図である。
【図１２４】管理された人工知能的サービスプロバイダ（ＭＡＩＳＰ）を示す概略図である。
【図１２５】ＬＯＭの依存構造を示す概略図である。
【図１２６】ＬＯＭの依存構造を示す概略図である。
【図１２７】ＬＯＭの依存構造を示す概略図である。
【図１２８】ＬＯＭの依存構造を示す概略図である。
【図１２９】初期クエリ推論（ＩＱＲ）の内部ロジックを示す概略図である。
【図１３０】初期クエリ推論（ＩＱＲ）の内部ロジックを示す概略図である。
【図１３１】調査の明確化（ＳＣ）を示す概略図である。
【図１３２】表明の構築（ＡＣ）を示す概略図である。
【図１３３】階層的マッピング（ＨＭ）がどのように動作するかの内部的詳細を示す概略図である。
【図１３４】階層的マッピング（ＨＭ）がどのように動作するかの内部的詳細を示す概略図である。
【図１３５】合理的訴求（ＲＡ）の内部詳細を示す概略図である。
【図１３６】合理的訴求（ＲＡ）の内部詳細を示す概略図である。
【図１３７】知識保持中枢（ＣＫＲ）の内部詳細を示す概略図である。
【図１３８】知識保持中枢（ＣＫＲ）の内部詳細を示す概略図である。
【図１３９】自動化された調査機構（ＡＲＭ）を示す概略図である。
【図１４０】文体計量学的スキャニング（ＳＳ）を示す概略図である。
【図１４１】仮説上書きシステム（ＡＯＳ）を示す概略図である。
【図１４２】知的情報および構成管理（Ｉ２ＣＭ）ならびに管理コンソールを示す概略図である。
【図１４３】個人知能プロファイル（ＰＩＰ）を示す概略図である。
【図１４４】生活の管理と自動化（ＬＡＡ）を示す概略図である。
【図１４５】挙動監視（ＢＭ）を示す概略図である。
【図１４６】倫理的・守秘的・合法的（ＥＰＬ）を示す概略図である。
【図１４７】ＬＩＺＡＲＤアルゴリズムの概要を示す概略図である。
【図１４８】反復型知的成長を示す概略図である。
【図１４９】反復的進化を示す概略図である。
【図１５０】反復的進化を示す概略図である。
【図１５１】創作モジュールを示す概略図である。
【図１５２】創作モジュールを示す概略図である。
【図１５３】創作モジュールを示す概略図である。
【図１５４】創作モジュールを示す概略図である。
【図１５５】個人秘書として使用されているＬＯＭを示す概略図である。
【図１５６】個人秘書として使用されているＬＯＭを示す概略図である。
【図１５７】調査ツールとして使用されているＬＯＭを示す概略図である。
【図１５８】提示された理論の利点と欠点を調査するＬＯＭを示す概略図である。
【図１５９】提示された理論の利点と欠点を調査するＬＯＭを示す概略図である。
【図１６０】外交戦争ゲームでのポリシー決定を行うＬＯＭを示す概略図である。
【図１６１】外交戦争ゲームでのポリシー決定を行うＬＯＭを示す概略図である。
【図１６２】調査報道タスクを行うＬＯＭを示す概略図である。
【図１６３】調査報道タスクを行うＬＯＭを示す概略図である。
【図１６４】歴史的検証を行うＬＯＭを示す概略図である。
【図１６５】歴史的検証を行うＬＯＭを示す概略図である。　図１６６～図１７９は、安全で効率的なデジタル指向言語ＬＡＱＩＴを示す概略図であり、より詳細には、

【図１６６】ＬＡＱＩＴのコンセプトを示す概略図である。
【図１６７】使用可能言語の主要種別示す概略図である。
【図１６８】ＬＡＱＩＴの線形モードを示す概略図である。
【図１６９】ＬＡＱＩＴの線形モードを示す概略図である。
【図１７０】原子モードの性質を示す概略図である。
【図１７１】原子モードの性質を示す概略図である。
【図１７２】原子モードの暗号化機能の概要を示す概略図である。
【図１７３】原子モードの暗号化機能の概要を示す概略図である。
【図１７４】原子モードの暗号化機能の概要を示す概略図である。
【図１７５】リダイレクトボンドのメカニズムを示す概略図である。
【図１７６】リダイレクトボンドのメカニズムを示す概略図である。
【図１７７】放射性要素のメカニズム示す概略図である。
【図１７８】放射性要素のメカニズム示す概略図である。
【図１７９】暗号化およびストリーミグが可能になった分子モードを示す概略図である。
図１８０～図１８４は、ＵＢＥＣプラットフォーム、および分散型情報配信システムＢＣＨＡＩＮに接続するフロントエンドのサマリを示す概略図であり、より詳細には、
【図１８０】ＢＣＨＡＩＮ対応アプリケーションを有し、実行するＢＣＨＡＩＮノードを示す概略図である。
【図１８１】ＢＣＨＡＩＮプロトコルのコアロジックを示す概略図である。
【図１８２】ストラテジー生成モジュール（ＳＣＭ）を管理する動的ストラテジー適応（ＤＳＡ）を示す概略図である。
【図１８３】様々な経済人格とともに暗号化デジタル経済交流（ＣＤＥＥ）を示す概略図である。
【図１８４】再帰的知性向上を示す概略図である。
【発明を実施するための形態】
【００８１】
クラウドベースの重層的情報セキュリティ（ＣＴＩＳ）による重要インフラストラクチャ防護および報復（ＣＩＰＲ）

図１～図２は、セキュリティをどう解釈するかに関する複数の観点に対する定義を、分析のための方法論として提示する方法を示す。参照符号１では、ビーコンとエージェントからなるネットワークを用いて攻撃者と常習犯のマップを作成している。このようなマップ／データベースを洗練された予測アルゴリズムと組み合わせることにより、未犯脅威の候補が浮かび上がる。I^2ＧＥ２１はビッグデータおよびマルウェアシグネチャ認識を活用して人的要素を決定する。セキュリティ挙動２０のストレージは、セキュリティイベント、その影響、および適切な応答の先例を形成する。そのような適切な応答は、セキュリティの補完的なレイヤとしてのＣＴＭＰ２２（クリティカルシンキング・メモリ・パーセプション）によって批判される可能性がある。参照符号２は、危険に曝されている資産は何か、どのような損害が発生しうるのかを指している。事例：ある水力発電ダムのすべての水門が開かれる可能性があり、その結果近隣の町が水没し、生命および財産が失われることにつながる。インフラデータベース３は、国全体のインフラ事業に携わる、公的または私的なある企業に関する、機密のあるいは機密でない情報を含む、総合データベースである。インフラ制御４は、ダムの水門や国全体の送電網のワット数など、産業インフラ設備の制御の、考え得る技術的、デジタル的、および／または機械的な意味である。参照符号５では、トラフィックパターンを分析して死角となり得る時間を強調する。このような攻撃は、容易にマスクされて正当なトラフィックに紛れ、それを隠れ蓑とする。次のような質問がされている。常習犯の関心ポイントとなりうる、政治、金融、スポーツ、その他のイベントがあるか？外部エージェントからなる信用プラットフォームのネットワークが、ハッカーの活動および準備について折り返し報告する。
したがって、攻撃のタイミングが推測できる。参照符号６では、次のような質問がなされている。攻撃のターゲットとなり得る、セキュリティ的に脆弱な企業はどこか？地理的な

場所別に、どのようなタイプの企業がセキュリティ的に脆弱なのか？最も脆弱な資産／制御は何か、そしてそれらを保護するために最良の方法は何か？外部エージェントからなる信用プラットフォームのネットワークが、ハッカーの活動および準備について折り返し報告する。したがって、攻撃の場所が推測できる。参照符号７では、次のような質問がなされている。どのような地政学的、地域的、および金融的な圧力が世界に存在して、このような攻撃に資金を提供し、幇助しているのか？誰がどのくらいの利益を得るのか？外部エージェントからなる信用プラットフォームのネットワークが、ハッカーの活動および準備について折り返し報告する。したがって、攻撃の動機が推測できる。参照符号８では、次のような質問がされている。マルウェアにとって悪用可能なポイントや隠れ家となりうるものは何か？このような死角や強化不十分なアクセスポイントがどのように利用され重要な資産およびインフラ制御のポイントを攻略するのか？ＬＩＺＡＲＤ１６は外来コードから目標と機能を導出し、悪意の存在または正当な動機の欠如に反応して、その外来コードをブロックする。ＣＴＭＰ２２は、ブロック／許可の決定について批判的に思考することが可能であり、またセキュリティの補助的レイヤとして機能する。

【００８２】

図３は、セキュアＥＩ^{2}（エクストラネット、イントラネット、インターネット）ネットワーキングのための、クラウドベースの管理暗号化セキュリティサービスアーキテクチャを示している。マネージドネットワークおよびセキュリティサービスプロバイダ（ＭＮＳＰ）９は、に対して管理暗号化セキュリティ、接続性、およびコンプライアンスのソリューションおよびサービスを提供する。信用プラットフォームとは、セキュリティ情報およびサービスを共有することにより相互に便宜を得ている、検証が済んだ複数の会社およびシステムのグループである。ハードウェア・ソフトウェアベンダー１１は、業界的に認知されたハードウェア・ソフトウェアのメーカー（たとえば、インテル、サムスン、マイクロソフト、シマンテック、アップルなど）である。この文脈では、これらのベンダは、あらゆる可能なアクセス手段および／または、それらベンダの製品に対して制限付き容量または全容量でバックドアアクセスを可能にするエクスプロイトの手段を、信用プラットフォームに提供する。これは、信用プラットフォームがそのパートナーおよび共同セキュリティ部門と協力して遂行させたい、考えられるセキュリティおよび／または懲罰的なプロセスのために可能になった。仮想プライベートネットワーク（ＶＰＮ）１２は、ＭＮＳＰ９、信用プラットフォーム、およびそれらの提携パートナーとの間で安全かつ業務的に分離された通信を可能とする、業界標準技術である。エクストラネットによって、デジタル要素があたかもそれらが同じ付近にあるかのように、仮想的に共有可能となる（たとえば、ＬＡＮ）。したがって、これら二つの技術を組み合わせることにより、パートナー間の効率的で安全な通信が促進され、信用プラットフォームの運用が向上する。セキュリティサービスプロバイダ１３は、デジタルセキュリティのストラテジーおよびソリューションを提供している公的および／または私的企業の集合である。セキュリティサービスプロバイダ１３のソリューションおよび製品は、契約によりまとめられており、これは、独自のセキュリティ情報（たとえば、新たなマルウェアのシグネチャ）やセキュリティ分析による恩恵を信用プラットフォームが受けられるようにするためである。このようなセキュリティ強度の向上は、つまるところ、セキュリティサービスプロバイダ自体にとって利益となる。サードパーティ脅威情報供給（３ＰＴＩ）１４とは、セキュリティ情報（たとえば、新たなマルウェアのシグネチャ）の相互共有のことである。中央集権型ハブ信用プラットフォームは、このようなセキュリティ情報の送受信および吸収の中央集権型ハブとして機能する。多数の情報が供給されることにより、セキュリティ絡みの挙動についてのより高度なパターンを（セキュリティサービスプロバイダを活用することによって）、情報協力を見分ける分析モジュール（たとえば、共謀検知１９）を通じて得ることが可能である。法執行機関１５は、州レベル（たとえば、ニューヨーク市警本部（ＮＹＰＤ））であれ、国家レベル（たとえば、米国連邦捜査局（ＦＢＩ））であれ、あるいは国際レベル（たとえば、国際刑事警察機構（ＩＮＴＥＲＰＯＬ））であれ、該当する法執行部門を指す。クラッカーに対する報復を容易にする、または完遂するために、通信が開始され、セキュ

リティ情報が送受信される。この報復とは、典型的には然るべき容疑者の場所を特定して逮捕し、該当する裁判所で裁判にかけることである。

【００８３】

図４～図８は、マネージドネットワークおよびセキュリティサービスプロバイダ（ＭＮＳＰ）９および内部のサブモジュール間関係の概要を示す。ＬＩＺＡＲＤ１６は、それまでの履歴データを参照せず、脅威それ自体を分析する。疑似セキュリティ脅威（ＡＳＴ）１７は、セキュリティルールセットの効力をテストするための、仮想のセキュリティシナリオを提供する。各セキュリティ脅威は、セキュリティシナリオの意味のある比較が行えるように、重大度および型において一貫している。創作モジュールは、前形状から新たなハイブリッド形状を知的に創作する処理を実行する。創作モジュールは、多数のアルゴリズムに処理を提供するプラグインモジュールとして使用される。共謀検知１９は、複数の「共謀」セキュリティイベントに対する定期的な素性チェックを提供し、一見無関係なセキュリティイベント間のパターンや相関関係を判定しようと試みる。セキュリティ挙動２０：イベントと、それぞれのセキュリティ応答とトレイトが、今後の問い合わせのために格納されインデックス付けされる。I^2ＧＥ２１はビッグデータ的な、ＭＮＳＰ９の遡及分析部である。標準的なシグネチャ追跡能力のなかで、I^2ＧＥはＡＳＴを創作モジュールとともに活用することで、マルウェアの将来の変種候補をエミュレートすることが可能である。ＣＴＭＰ２２は複数のソース（たとえば、I^2ＧＥ，ＬＩＺＡＲＤ，信用プラットフォームなど）からの相互参照情報収集を活用し、パーセプションの予想と現実について学習する。ＣＴＭＰは、ある事柄についての客観的決定を形成する能力を見積り、そしてある決定が内部の低い確信度に基づいてなされた場合、それを断言することは控える。管理コンソール（ＭＣ）２３は、複雑ではあるが半自動のシステムをモニターし制御する、人間向けの知的インタフェースである。知的情報および構成管理（I^2ＣＭ）２４には、情報のフローと許可されたシステム活用を制御する機能の組み合わせが含まれている。

エネルギーネットワーク取引所２５は、エネルギー供給者、生産者、購入者をなど結ぶ巨大なプライベートエクストラネットである。エネルギーネットワーク取引所では、供給者、生産者、購入者がなど、それらに共通する業種に関するセキュリティ情報を交換できる。エネルギーネットワーク取引所は、ＶＰＮ／エクストラネット１２経由でＭＮＳＰクラウド９と通信する。このようなクラウドベースの通信は、次の点で双方向のセキュリティ分析を可能としている。１）重要なセキュリティ情報データが、エネルギーネットワーク取引所からＭＮＳＰクラウドに提供される、および２）重要なセキュリティ修正処置が、ＭＮＳＰクラウドからエネルギーネットワーク取引所に提供されるすべてのEI^2（エクスプローラー、イントラネット、インターネット）のネットワークトラフィックは、常にＶＰＮ１２を経由してＭＮＳＰクラウドへとルーティングされている。すべてのサービスにおいてＭＮＳＰによって利用される認証および暗号化技術は、国家標準（たとえば、ＦｅｄＲＡＭＰ（Ｆｅｄｅｒａｌ Ｒｉｓｋ ａｎｄ Ａｕｔｈｏｒｉｚａｔｉｏｎ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｇｒａｍ：米国連邦政府のリスク・認証管理プログラム）、ＮＩＳＴ（Ｎａｔｉｏｎａｌ Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｓｔａｎｄａｒｄｓ ａｎｄ Ｔｅｃｈｎｏｌｏｇｙ：米国国立標準技術研究所）、ＯＭＢ（Ｏｆｆｉｃｅ ｏｆ Ｍａｎａｇｅｍｅｎｔ ａｎｄ Ｂｕｄｇｅｔ：アメリカ合衆国行政管理予算局）など）および国際標準（ＥＴＳＩ（Ｅｕｒｏｐｅａｎ Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ Ｓｔａｎｄａｒｄｓ Ｉｎｓｔｉｔｕｔｅ：欧州通信規格協会）、ＩＳＯ／ＩＥＣ（Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｏｒｇａｎｉｚａｔｉｏｎ ｆｏｒ Ｓｔａｎｄａｒｄｉｚａｔｉｏｎ／Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｅｌｅｃｔｒｏｔｅｃｈｎｉｃａｌ Ｃｏｍｍｉｓｓｉｏｎ：国際電気標準会議／国際電気標準会議），ＩＥＴＦ（Ｉｎｔｅｒｎｅｔ Ｅｎｇｉｎｅｅｒｉｎｇ ＴａｓｋＦｏｒｃｅ：インターネット技術標準化委員会）、ＩＥＥＥ（Ｔｈｅ Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｅｌｅｃｔｒｉｃａｌ ａｎｄ Ｅｌｅｃｔｒｏｎｉｃｓ Ｅｎｇｉｎｅｅｒｓ，Ｉｎｃ．：米国電気電子学会）など）、ならびに暗号化要件（たとえば、ＦＩＰＳ（Ｆｅｄｅｒａｌ Ｉｎｆｏｒｍａｔｉｏｎ Ｐｒｏｃｅｓｓｉｎｇ Ｓｔａｎｄａｒｄｓ：連邦情報処理標準）など）に準拠している。イント

ラネット２６（暗号化されたレイヤ２／３ＶＰＮ）は、企業（エネルギー会社）のプライベートネットワーク２７の範囲内で安全な内部接続を整備している。これによって、ＬＩＺＡＲＤライトクライアント４３は、ＭＮＳＰクラウド９にあるＬＩＺＡＲＤクラウド１６と安全に通信可能な状態で、企業インフラ内で動作可能となる。参照符号２７は、プライベートネットワークのローカルノードを示している。そのような私設ネットワークは複数の場所を提供している（場所Ａ、Ｂ、およびＣとしてラベル付けされている）。各プライベートネットワークには、異なる技術基盤による仕組みが存在していてよく、たとえば、サーバクラスタ（拠点Ｃ）、あるいはモバイル機器とプライベートＷｉ－Ｆｉ接続を有する従業員共有オフィス（拠点Ａ）となどしてよい。プライベートネットワークの各ノードには、自前の管理コンソール（ＭＣ）２３が備わっている。携帯メディア機器２８は、プライベートネットワークひいてはイントラネット２６に安全に接続するよう構成されており、したがって、これらの機器は安全なＶＰＮ／エクストラネット接続１２を経由して間接的にＭＮＳＰ９と接続している。この安全な接続を使用しているときは、すべてのトラフィックはＭＮＳＰを経由するようルーティングされ、配備されたリアルタイムで遡及的なセキュリティ分析アルゴリズムに最大限さらされるようになっている。このような携帯機器であれは、安全なプライベートネットワークの中でも、街中のコーヒーショップのＷｉ－Ｆｉアクセス環境でも、この安全な接続を維持することができる。非武装地帯（ＤＭＺ）２９は、通常のコンピュータよりセキュリティ上不利な状態にあるＨＴＴＰサーバを有するサブネットワークである。ＨＴＴＰサーバがセキュリティ上不利な状態にあるのはセキュリティに対する怠慢によるものではなく、公開サーバのソフトウェアおよびハードウェアの編成が複雑だからである。セキュリティを厳しくしようと最大限の努力はしているにもかかわらず、攻撃される可能性のあるポイントは非常に多い。したがって、このようなセキュリティ上不利な状態に当該プライベートネットワーク（拠点Ｃ）の残りの以外の部分をさらすことのないよう、このサーバは非武装地帯に設置されている。このように分離することにより、ＨＴＴＰサーバは、プライベートネットワークの内部にあって非武装地帯にはない他の装置とは通信できない。ＬＩＺＡＲＤライトクライアント４３はＨＴＴＰサーバにインストールされているため、ＤＭＺの内側で動作可能である。ＤＭＺポリシーには、ＭＣ２３がＨＴＴＰサーバおよびＤＭＺにアクセスできるよう、例外が設けられている。ライトクライアントは、イベント１２および２６から形成された暗号化されたチャネルを介してＭＮＳＰと通信する。参照符号３０において、これらのサーバはプライベートネットワーク内に隔離されているが、ＤＭＺ２９からは見えている。これにより、プライベートネットワークの内側にある装置は互いに通信可能となる。これらのサーバはそれぞれ、ＬＩＺＡＲＤライトクライアント４３の独立したインスタンスを備えている。インターネット３１は、ＭＮＳＰ９とＬＩＺＡＲＤライトクライアントを稼働させている企業の各デバイス２８の間の情報伝達の媒体であるということで参照されている。インターネットは、企業のデバイスにとって最もリスクに左右されやすいセキュリティ脅威の源であり、それはローカルエリアネットワーク（ＬＡＮ）で発生するローカルな場所での脅威とは異なる。この高いセキュリティリスクにより、各機器上のすべての情報伝達はプロキシのように振る舞うＭＮＳＰへとルーティングされる。ＶＰＮ／エクストラネット１２があることにより、インターネットからの、常習犯の可能性のある者には暗号化された情報のみしか見ることができない。サードパーティ脅威情報供給（３ＰＴＩ）３２は、既存の契約上の義務にしたがいサードパーティによって提供される、カスタマイズされた情報の入力を表している。反復的進化アルゴリズム３３：並行する複数の進化系統が発達し選択される。イテレートされた世代が、同一の疑似セキュリティ脅威（ＡＳＴ）に適応し、最良のパーソナリティトレイトを有する系統が、最終的にはこのセキュリティ脅威に対して最も良く耐えることになる。進化系統３４：仮想的に収められ隔離された一連のルールセットの世代である。進化の特徴および基準は、このような系統パーソナリティＸによって定義される。

【００８４】

図９は、ＬＩＺＡＲＤクラウドベースの暗号化セキュリティについてのリアルタイムセキ

ュリティ処理を示している。構文モジュール３５が、コンピュータのコードを読み書きするためのフレームワークを提供している。書き込みでは、構文モジュールがＰＭ（目標モジュール）から複合フォーマットの目標を受信し、コードを任意のコードの構文で書き込み、それによって、ヘルパ機能がこの任意のコードを（所望の言語に依存して）実際の実行可能コードへと翻訳できる。読み込みでは、構文モジュールは、ＰＭが、コードの機能性の目標を導出できるよう、このコードの構文解釈を提供する。目標モジュール３６は、構文モジュール３５を用いてコードから目標を導出し、この目標を、自身の「複合目標フォーマット」に出力する。この目標は、ＳＭ（構文モジュール）によって解釈されたコードブロックの、意図された機能性を十分に記述している（このコードがデータに密かに埋め込まれていても）。仮想難読化３７では、企業ネットワークとデータベースが仮想環境内に複製され、機密データが模擬（偽の）データと置き換えられる。ターゲットの挙動に従って、環境がリアルタイムで動的に変更され、システム全体としてのより多くの偽の要素、またはより多くの現実の要素が含まれる。信号擬態３８は、仮想難読化（保護）が分析的に完結したときに通常使用される、報復の形式を提供する。信号擬態は、マルウェアがハッカーと通信するための構文を読み解くために、構文モジュールを使用する。信号擬態は、その後この通信を乗っ取り、機密データをハッカーに送ることに成功したという、誤った印象をマルウェアに与える（この機密データが仮想のハッカー像に対して送信された偽データだったとしても）。ＬＩＺＡＲＤは、マルウェアのエラーコードも現実のハッカーに送信し、このエラーコードがマルウェアから来たもののように思わせる。これによって、ハッカーの時間とリソースが、誤ったデバッグ作業という、脱線した作業に流用させられ、ついには、マルウェアが機能しなかったという誤った印象をもちながら、機能しているマルウェアを放棄させる。内部整合性チェック３９が、外来コードのすべての内部機能の辻褄が合っていることがチェックする。外来コード全体としての目標と内部的に相容れないコードの断片が存在しないことが確かめられる。外来コード改訂４０が、構文モジュールと目標モジュールを使用し、外来コードを複合目標フォーマットにまとめる。その後、導出された目標を使用するコードセットを構築する。これによって、外来コードから読み解かれた所望の目標だけが企業内で実行され、意図しない機能が実行されることでシステムにアクセスすることのないことが保証される。秘密コード検知４１が、データおよび送信パケットに密かに埋め込まれたコードを検知する。要求マップマッチング４２は、マップ化された要求および目標の階層構造であり、外来コードがシステムの目的全体にフィットしているかを判断するために参照される。ＬＩＺＡＲＤライトクライアント４３は、仮想難読化２０８や信号擬態などのリソースを大量に消費する機能を省いた、ＬＩＺＡＲＤプログラムの軽量バージョンである。シグネチャデータベースを照会用に使用しない客観的・演繹的な脅威分析を活用することで、最小限のコンピュータリソースを使用して瞬時でリアルタイムな脅威分析を行っている。複数のログ４４によって、エネルギー会社のシステム４８は標準ソフトウェアエラー出力／アクセスログ、オペレーティングシステムログ、モニタリングプローブのなどログを作成する複数のポイントを有している。これらのログは、詳細で応答の早いセキュリティ分析を行うためにローカルパターンマッチングアルゴリズム４６およびＣＴＭＰ２２へ供給される。エネルギー会社に存在するすべての内部および外部トラフィックであるトラフィック４５では、ローカルパターンマッチングアルゴリズム４６は、ウイルス対策、適応ファイアウォールのなどセキュリティの初期レイヤを提供する業界標準のソフトウェアからなっている。修正処置４７は、セキュリティ上の問題／リスクを解決するため最初に理解されるローカルパターンマッチングアルゴリズム４６により引き受けられることになる。修正処置には、ポート、ファイル転送、管理機能要求などをブロックすることが含まれている。エネルギー会社は、これらの専門化されたセキュリティアルゴリズム群からは隔離されたシステム４８を有しており、このシステムは自身のログとトラフィック情報も送信している。これは、これらのアルゴリズムならびにＬＩＺＡＲＤ１６、I^2ＧＥ２１、およびＣＴＭＰ２２がＭＮＳＰクラウド９に設置されているからである。このように分離することにより、一元化データベースモデルを提供することが可能となる。このことは、セキュリティデータ／トレンドのプールを

より大きくすることにつながり、したがって、より包括的な分析につながる。

【００８５】

図１１を参照すると、犯罪システムは、標的システムへの利用可能な侵入チャネルをスキャンする。可能であれば、犯罪システムは、小さなペイロードを送り届けるためにこのチャネルを攻略する。犯罪システム４９は犯罪者の一団によって使用され、パートナーのシステム５１、よって最終的にはインフラシステム５４に向けてマルウェア攻撃を仕掛ける。マルウェア源５０は、悪意のあるコード（マルウェア）の非活性形式のコンテナである。このコードがいったん標的となるインフラシステム５４に到達する（または到達を試みる）とマルウェアが始動し、予め決められた通りまたはオンデマンドで悪意のあるタスクを実行する。パートナーのシステム５１は、インフラ企業（エネルギー会社）とパートナー会社の間で交わされた契約上の合意に従って、インフラシステムとの間で情報を交換する。このような合意は、ある種のビジネス上の業務、たとえばサプライチェーンマネジメントサービスや、在庫追跡のやりとりなど、を反映している。合意済みのサービスを充足する際、両者は従前の合意済みセキュリティ標準に従って電子的に情報を交換する。マルウェア源５０は、犯罪システム４９を稼働させている悪意のある一団に成り代わって、パートナーのシステムに潜入するためのエクスプロイトを見つけようとする。このようにして、マルウェアはその最終感染目標であるインフラシステム５４に到達することができる。このようにして、パートナーのシステムは、マルウェア源５０に端を発する代理感染プロセスにおいて利用されている。パートナーのシステム５１とインフラシステム５４の間の多数の通信チャネルの中で、チャネル５２がマルウェア源５０に端を発するマルウェアによって攻略されている。チャネル／プロトコル５３を参照すると、これはパートナーのシステム５１と、攻略されていないインフラシステム５４との間の通信チャネルを示している。これらのチャネルはファイルシステム接続、データベース接続、メールルーティング、ＶＯＩＰ接続をなど含む。インフラシステム５４は、インフラデータベース５７およびインフラ制御５６に直接アクセスできるエネルギー会社の業務における重要な要素である。標準的なセキュリティ手続きとして、業界標準の侵入防御システム５５が実装されている。インフラ制御５６は、エネルギー関連の設備を接続するデジタルインタフェースである。インフラ制御は、たとえば、水力発電ダムの水門の開閉や、ソーラーパネル群が向いている角度をなど含んでいる。インフラデータベース５７は、インフラシステムおよびエネルギー会社全体としての核となるオペレーションの詳細に関する機密情報を有している。このような情報は、連絡先情報、従業員のシフト履歴、エネルギー設備の文書および設計図を含み得る。

【００８６】

図１２を参照すると、攻略されたチャネル５２によって、非常に狭いエクスプロイトの機会の窓が提供される。それにより、非常に単純なトロイの木馬が標的システムにアップロードされ、エクスプロイト実行の機会を拡げる。トロイの木馬５８はマルウェア源５０から発生し、攻略されたチャネル５２を通ってその標的であるインフラシステム５４に到着する。トロイの木馬の目的は、高度な実行可能マルウェアのペイロード（より複雑であり、データをなど盗み出す実際の悪意のコードを含んでいる）を標的システムにインストールできるように、エクスプロイトによってもたらされる機会を与えることである。

【００８７】

図１３は、トロイの木馬がシステムをさらに悪用したあと、自身が新たに開いたチャネルを通じて大規模な実行可能マルウェアパッケージがシステムに安全にアップロードされる様子を示している。高度な実行可能マルウェア５９はインフラシステム５４、したがって機密データベースおよびインフラ制御５６に転送される。高度な実行可能マルウェアはトロイの木馬が前回のエクスプロイトで築いたデジタル的な通路を使用して自信の目的地に到達する。

【００８８】

図１４は、高度な実行可能マルウェア５０がＩＤＳを攻略することにより、機密インフラ情報および制御ポイントが、検知されない犯罪システムに個別にダウンロードされる様子

を示している。ハッカー所望の挙動６０において、ハッカー６５は正当に許可されたアクセス認証情報とともに、ある会社従業員の信頼できる認証情報の入手に成功している。このハッカーは、これらの認証情報を使用することで、従業員の使用に限定されたＬＡＮへの、目立たず認識不能のアクセス権を得ようと考えている。このハッカーは、「あまりにも遅すぎる」セキュリティ応答の裏をかこうと考えている。このエンドポイントセキュリティクライアントがクラウドセキュリティサービスへデータを中継することに成功したとしても、遡及的な分析を行うセキュリティソリューションだと、侵入の初期段階からリアルタイムに脅威を除去・管理するのではなく、ダメージコントロールを管理できるのみである。実際のセキュリティ応答６１では、ＬＩＺＡＲＤライトクライアント（エンドポイントでの使用）は、資格情報のログインとシステムアクセスの使用の必要性、機能、目的を明白に証明することができない。この資格情報を有するユーザが本当に意図された正当なユーザであるかどうかはまだ不明であるため、このユーザは部分的に仮想／疑似環境に置かれている。この環境は、ユーザの挙動を分析しながらリアルタイムに機密データへの露出を動的に変更できる。挙動分析６２はハッカー６５について実行され、現実のＬＡＮインフラ６４および仮想的にクローンされたＬＡＮインフラ６４の双方に存在する、ハッカーが接する要素に基づいて実行される。ハッカーは、攻略した認証情報６３を用いて、エネルギー会社のノートパソコン２８、ひいてはこのラップトップが接続するＬＡＮインフラ６４への、管理者権限でのアクセスを与えるアクセス認証情報を得ている。これらの認証情報は、暗号化されていないメールを傍受する、ローカルに格納された認証情報を有する暗号化されていない企業デバイスを盗むなどによって、最初に攻略された可能性がある。ＬＡＮインフラ６４は、ローカルネットワーク（有線および／または無線）を通じて接続されている一揃いの企業デバイスを表している。このＬＡＮインフラには、プリンタ、サーバ、タブレット、電話がなど含まれる。このＬＡＮインフラ全体は、ＭＮＳＰクラウド９内で仮想的に再構成されている（仮想ルーターＩＰ割り当て、仮想プリンタ、仮想サーバなど）。このシステムが挙動分析６２を実行すると、ハッカーは現実のＬＡＮインフラおよび仮想的にクローンされたバージョンのＬＡＮインフラの双方にある要素に対してさらされる。そのような分析の結果がリスクを示した場合は、実際のデータおよび／または機器が危険にさらされるリスクを軽減するために、（実際のインフラではなく）偽のインフラへのハッカーの被害が増加する。ハッカー６５は、攻略した認証情報６３によって可能となった初期の侵入を通じて機密情報にアクセスし盗み出すことを考えている、悪意のある行為を行う者である。パスワードセット６６を用いて、３つのパスワードのセットが認証アクセスに割り当てられている。これらのパスワードは個別に格納されることはなく、常に一つのセットで現れる。従業員はＳＩＡＰＡから一時的に割り当てられたプロトコルにしたがい、これら３つのパスワードの組み合わせを入力しなければならない。スケジュールされた内部認証プロトコルアクセス（ＳＩＡＰＡ）６７により、個々の従業員のログインポータル用の認証プロトコルが週／月単位で変更される。このプロトコルは、（認証のために予め割り当てられている）パスワードＡ、Ｂ、およびＣのセットからパスワードＡおよびＣを選択することである可能性がある。認証方法の変更を一定期間毎（毎月曜日または毎月一日）にスケジュールすることによって、（ある正当な従業員が古いプロトコルを使用したことで模擬データ環境３９４から抜け出せないといった）疑陽性のイベントを最小限に留める認証プロトコルを切り替えることに従業員は慣れている。新しいプロトコルがハッカーによって攻略されるリスクを相殺するために、従業員は、その新しいプロトコルを、破棄され再び見ることができなくなるまえに一度だけ見ることができる。この最初で最後の閲覧は、生体情報／網膜／電話へのショートメッセージといった、特別な多要素認証を必要とする。従業員は、３つのパスワードのうち入力すべきものを表している１つまたは２つの文字を記憶することを要求されるだけである。第１週６８を参照すると、パスワードＡおよびＢのみを除くどのパスワードも模擬データ環境３９４をトリガする。第２週６９を参照すると、パスワードＡおよびＣのみを除くどのパスワードも模擬データ環境をトリガする。第３週７０を参照すると、パスワードＢのみを除くどのパスワードも模擬データ環境をトリガする。第４週７１を参照すると、どのパスワードも模擬

データ環境をトリガする。ＳＩＡＰＡ７２では、認証プロトコルは秘密のまま維持されており、一時的なアナウンスにアクセスできるもののみが、正しいプロトコルを知っている。ＬＡＮインフラの仮想クローン７３において、ハッカー６５は、正しいパスワードを省くのではなく３つすべてのパスワードを入力するため、このハッカーは、重要なデータまたは機能を一切含まないＭＮＳＰクラウド９内のコピー環境に、何も知らされずに転送される。ハッカーが実際のシステムに潜入できていると信じている一方で、科学捜査的証拠および挙動分析が集められる。「間違ったプロトコルが使用される」というケースシナリオ７４を参照すると、ハッカーは、正しいプロトコルを知る術がないので、正しいプロトコルを使用しなかった。まして、ある特定のパスワードを省くという特別なプロトコルがあることなど、ハッカーは予想すらしなかった。参照符号７５を参照すると、ハッカーは正当な認証情報を首尾良く盗みだしており、機密データを盗み出すべく、この会社のシステムへログインすることを考えている。企業内部監督部署７６は、管理委員会ならびに技術指導センターからなる。企業内部監督部署は、監視ならびに悪意のある可能性のある挙動を許可／ブロックする機能の最上位レイヤである。従業員ＢとＤ７７は犯罪者ではなく（彼らは企業の利益に専ら充実である）、ルートレベル機能８０を許可する三者協同の有資格従業員として選ばれている。従業員Ａ７８は、三者協同プロセス８０には選ばれていない。この理由としては、従業員Ａがこの会社での十分な就業経験、技術的経験を有していないこと、あるいは前科があった、あるいは、この会社に対する共謀を考慮していたかもしれない他の従業員とあまりに親しくしていたことなどが可能性としてある。従業員Ｃ（犯罪者）７９は、悪意のある目的を実行すべく、ルートレベル機能／活動にアクセスしようと試みる。このルートレベル機能８０は、個々のルートレベルアクセスについて３人の従業員の合意と許可がなければ実行できない。従業員Ｃは唯一悪意を持った従業員であるが、３人の従業員すべてが、このようなルートレベル機能が実行された結果に対して等しく責任を負っている。このことにより、注意と懐疑的な態度の企業風土が促され、また、従業員達は、まずこの手続きについてあらかじめ知っているため、悪意のある挙動を行うことが強力に阻止される。従業員ＥとＦ８１は、そもそも要求されたルートレベル機能を実行するためのルートレベルアクセス権もなければ許可することもないので、三者協同プロセス８０には選ばれていない。監督審査８２は、人工的（意図的）な遅延によってもたらされた時間を使い、要求された行為を審査し批評する。ルートレベル活動８３が１時間遅延され、監督部署にこの要求された行為を審査と、明示的にその行為に対して許可またはブロックさせるための機会が与えられる。監督部署がある決定を下すことができなかった場合、ポリシーはデフォルトアクション（許可またはブロック）を定義することができる。監督審査８４は、（３人の従業員の）全員一致の決定に達しなかった理由が何かを特定する。実行されたルートレベル活動８５を参照すると、協調と監督の監視システムを通過すると、誰が何を許可したのかについての記録が安全に維持されている状態で、ルートレベル活動が実行されている。このように、ルートレベル活動が、この会社の最良の利益に反するものであると判明した場合、詳細な調査が行われる。参照符号８６では、三者協同が失敗（全員一致の決定に達しなかった）ため、ルートレベル活動がキャンセルされている。参照符号８７では、ルートレベルアクセス権を有する、選ばれた３人の従業員全員が、あるルートレベル活動に対して全員一致で許可している。もしこのルートレベル活動が実際は悪意のものであったとしたら、３人の従業員全員が、この会社に対する共謀に関与している必要があっただろう。このことは起こりそうにないとはいえ、それでも起こる可能性はあるので、ルートレベル活動８３が１時間遅延され、監督部署がこの活動を審査する機会が与えられる（参照符号７６および８２を参照）。参照符号８８では、三者協同のために選ばれた、１人以上の有資格従業員が、リクエストされたルートレベル活動を却下した。したがって、全員一致の決定に達しなかったので、ルートレベル活動そのものもキャンセル８９され、ルートレベル活動８５もキャンセルされた。進化パターンデータベース９０は、以前に発見され、処理されたセキュリティリスクのパターンを含んでいる。これらのパターンは、現在のマルウェアの状態が変形していく進化の考えられる手段を列挙している。シグネチャ９１の新版／変種を生成するために、マルウェアルートシグネ

チャ９１がＡＳＴ１７に与えられる。マルウェアの多型変種９２がＩ^{2}ＧＥから出力され、マルウェア検知システム９５に転送される。インフラシステム９３は、物理的にそのインフラの構内に存在している。インフラシステムは一般的には水力発電プラントや送電網といったインフラ機能を管理している。インフラコンピュータ９４は、インフラシステム９３からのインフラ機能を実行可能にする機能あるいはその機能の一部を実行する、特定のコンピュータである。マルウェア検知ソフトウェア９５は、インフラコンピュータの構成における３つのレベルすべてに配置されている。インフラコンピュータには、ユーザスペース９７、カーネルスペース９９、およびファームウェア／ハードウェアスペース１０１が設けられている。これは、３つのレベルのそれぞれ専用に配備されたＬＩＺＡＲＤライトエージェントで実行されるマルウェア検出の展開に対応する。進化経路３４を介してイテレートされたマルウェア９６の形態は、ドライバ（カーネル空間９９内部に存在する）内に見出される。ユーザスペース９７は、メインストリームの開発アプリケーションのために設けられている。ユーザスペースはマルウェアを使って潜入するのが最も容易なスペースであるが、マルウェアを検知および強制検疫するのが最も容易なスペースでもある。ユーザスペースにおける活動のすべてはＬＩＺＡＲＤライトによって効率的にモニターされている。ユーザスペース内のアプリケーション９８には、マイクロソフトオフィス、スカイプ、Ｑｕｉｃｋｅｎなどのようなプログラムが含まれうる。カーネルスペース９９は、その大部分がアップル、マイクロソフト、リナックスファウンデーションのようなオペレーティングシステムベンダによって整備されている。カーネルスペースはユーザスペースよりは潜入が難しいが、それぞれのインフラがカーネルに変更を加えない限り、その責任の大部分はベンダに属している。カーネルにおける活動のすべて（レジストリの変更（マイクロソフトのＯＳの場合）、メモリ管理、ネットワークインタフェースの管理など）は、ＬＩＺＡＲＤライトによって効率的にモニターされている。ドライバ１００は、インフラコンピュータ９４が周辺機器およびハードウェア（マウス、キーボード、指紋スキャナなど）との対話を可能にしている。ファームウェア／ハードウェアスペース１０１は、その全体が、ファームウェア／
ハードウェアのベンダによって整備されている。マルウェアにとっては、対応するハードウェアに直接物理的にアクセスする（たとえば、マザーボードから古いＢＩＯＳチップを抜き取って新しいチップを半田付けする）ことなしに影響を与えるのは極めて困難である。ファームウェアの活動のいくつかは、ＬＩＺＡＲＤライトによってモニターされているが、ハードウェアの設定に依存している。ＢＩＯＳ１０２（ファームウェアの一種）は、オペレーティングシステムがそれを基に構築される最初のソフトウェアレイヤである。パブリックインフラ１０３は、未知かつ攻略される可能性のあるデジタルインフラ（ＩＳＰルーター、ファイバーケーブルなど）のことである。エージェント１０４は、パブリックインフラに仕掛けられており、信用プラットフォームのデータベースに格納されているコールバックチャネルの既知の記述（ポート、プロトコル種別など）と連動することにより、既知のコールバックチャネルをモニターしている。エージェントは、ハートビート信号の有無を確認し、信用プラットフォームに知らせることにより、マルウェア源を活用する。自動発見およびライトクライアントのインストール１０５によって、ＭＮＳＰ９のＬＩＺＡＲＤクラウドは、ＬＩＺＡＲＤに応答信号（ハンドシェイク）を送らないエンドポイントシステム（たとえば、ラップトップ）を検知する。このエンドポイントは、発見されＩ^{2}ＣＭ２４（知的情報および構成管理）によって分類され次第、同期される。したがって、ＬＩＺＡＲＤクラウドは、ＬＩＺＡＲＤライトクライアントがインストール／起動されていないことを（ＳＳＨリモートルートシェル経由）検知し、ルートシェルを使用して強制的にＬＩＺＡＲＤライトクライアント４３をインストールし、ＬＩＺＡＲＤライトクライアントが正しく起動されていることを保証する。ライトクライアント４３がエントリデバイスにインストールされていないため、マルウェア１０６Ａが最初に侵入する。ライトクライアント４３は、システムのほぼすべての可能なインスタンスにインストールされるが、すべての送受信のトラフィックが、ＬＩＺＡＲＤクラウドを備えるＭＮＳＰを通過するようルーティングされている。初期のエクスプロイト１０７では、エクスプロイトの

最初の侵入が検知されると、エクスプロイトが秘密のコールバックチャネル１０６Ｂを開通できるようになる前にブロックされる可能性がある。チャネル１０６Ｂは、マルウェア１０６Ｂがその本拠地と個別に通信するための、他には知られていない通信経路である。このことは、信号をマスキングして正当なｈｔｔｐまたはｈｔｔｐｓアプリケーショントラフィックに見せることを含む。様々なベンダ１０８が、ソフトウェア、ハードウェア、ファイアフォール、サービス、金融および重要なインフラへの秘密アクセスなどの有用なリソースを提供しており、パブリックインフラにエージェント１０４を仕掛けることが可能になっている。マルウェアによって、特定のサイズおよび周波数をもつハートビート信号が、コールバックチャネル１０６Ｂ経由で、一定間隔で送出され、秘密のコールバックチャネル経由でマルウェアの出所／忠誠の源に向けられている。この信号は、マルウェア源５０に今後のエクスプロイトおよび連携攻撃を決定できるようにするために、マルウェアの状況／能力を示している。このマルウェア源は、悪意とともにハッキング能力を有する組織であれば、その組織がブラックハットハッキングシンジケートであろうが国家政府であろうが、その組織を示している。すべての送受信トラフィックがＶＰＮトンネル経由でＭＮＳＰクラウド／ＬＩＺＡＲＤを通過するようルーティングされているので、マルウェア１０６Ａおよびハートビート信号（チャネル１０６Ｂ内部）は、ＭＮＳＰクラウド９で稼働するＬＩＺＡＲＤによって検知される。

【００８９】

図２２～図２３は、外来コード改訂が外来コードを構文的に再現することで、起こりうる未検知の悪意のエクスプロイトを軽減する様子を示している。組合せメソッド１１３は、宣言された目標１１２Ａ（可能であれば、企業ポリシー１４７によれば、任意の場合もある）を導出された目標１１２Ｂと比較し一致させる。組合せメソッドは、目標モジュール３６を使用することで複合目標フォーマットを操作し、結果として生じた一致または不一致のケースシナリオを得る。導出された目標１１２Ｂを用いて、要求マップマッチングは階層的構造を維持管理し、すべての企業の要求の管轄範囲を維持管理する。したがって、管轄範囲指向の要求マップ１１４の空きに応じて、コードブロックの目的が定義され正当化される。入力された目標１１５は、再帰的デバッグ１１９のプロセス（目標・構文モジュールを活用する）へ取り込まれるものである。複数の入力（たとえば、目標）をマージせず、目標の入力一回ごとに、別々で並行したインスタンスが初期化される。最終セキュリティチェック１１６は、構文モジュール３５および目標モジュール３６を活用して汎用の「健全さ」チェックを行うことでプログラミングにおける悪用可能なあらゆるポイントをガードし、さらに最終出力１１７をＶＰＮ／エクストラネットに転送する。

【００９０】

図２４～図２５は、再帰的デバッグ１１９がコードセグメントをループ処理してバグをテストし、可能な場合はバグフィックス１２９（ソリューション）を適用する様子を示している。もしバグが残っている場合は、そのコードセグメント全体が、オリジナルの（外来）コードセグメント１２１に置換１２３されるオリジナルコードセグメントはその後、仮想難読化や挙動分析といった付加的なセキュリティレイヤーを可能にするためにタグ付けされる。コードを改訂するために、目標モジュール３６および構文モジュール３５が外来コード１２０を用いてコードのオリジナルの状態を解釈する。改訂バージョンに消えないバグがあるためにオリジナルの（外来）コードセグメントをインストールする必要がある場合、外来コード１２０はデバッガから直接参照される。改訂コード１２２のセグメント１２１が、仮想ランタイム環境１３１によってテストされ、コーディングバグ１３２の有無がチェックされる。この環境１３１は、関数やクラスといったコードセグメント１２１を実行し、ランタイムエラー（構文エラー、バッファオーバーフロー、間違った関数呼び出しなど）の有無をチェックする。どのようなコーディングエラーも修正を目的として処理される。コーディングバグ１３２を用いて、仮想ランタイム環境において生じたエラーは、スコープと種別において定義される。関連するすべてのコーディング内容が与えられ、解決策を可能にする。目的の整合１２４により，この関数やクラスの宣言された目的からコードを再び導出することで、コーディングバグ１３２に対して可能性のある解決策が

考え出される。このバグを回避するために、コーディングバグのスコープが代替フォーマットの形式に書き換えられる。可能性のある解決策が出力され、他になにも解決策がない場合は、コードセグメント１２１のためのコード改訂は喪失され、オリジナルのコードセグメント（外来コードから直接もってきた）が最終コードセットにおいて使用される。典型的には、１回のループで、コードバグ１３２はコーディングの解決策を複数回受け取る。このバグ１３２を解決することにおいてコーディングの解決策がすべて尽きた場合、解決策は喪失され、オリジナルの外来コード１３３が使用される。仮想難読化や挙動分析のなど付加的なセキュリティ対策の決定を可能なものにするために、コードセグメント１２１は、外来であるとタグ付け１３６されることがある。たとえば、改訂されたコードブロックが、高度な外来コードセグメントを含む場合、このコードブロックは模擬データ環境３９４に配置される可能性がより高い。コードセグメントキャッシング１３０により、個々のコードセグメント（関数／クラス）がキャッシュされ、複数の改訂作業で再利用されることでＬＩＺＡＲＤクラウドのリソース効率が高まる。クラウドではすべてのトラフィックがＶＰＮ経由で集中するので、このキャッシュは非常によく活用される。改訂コードセグメントプロバイダ１２８により、事前に改訂されたコードセグメント１２１が与えられ、コーディングバグがその解決策をコードセグメントに適用１２９できるようにする。

【００９１】

図２６は、目標管轄範囲を検証する要求マップマッチング１１４の内部動作原理を示す。ＬＩＺＡＲＤクラウドおよびＬＩＺＡＲＤライトは、企業の管轄範囲部門の階層構造マップ１５０を参照する。この参照は、コード／関数の目標を正当化するために行われ、妥当な根拠を欠いている場合は、このようなコード／関数をブロックすることがある。入力された目標１３９が主張されたものか（目標モジュール３５経由で）導出されたものかにかかわらず、要求マップマッチング１１４はコード／関数が企業のシステムの内部で実行するための根拠を確認する。階層構造マップ１５０のマスターコピーが、該当する登録された企業のアカウントでＭＮＳＰ９のＬＩＺＡＲＤクラウドに格納されている。マスターコピーを参照することで、要求マップマッチング１１４の要求インデックス１４５が計算される。そして、予め最適化された（階層構造そのものではない）要求インデックスが、すべてのアクセス可能なエンドポイントのクライアントに配布される。要求マップマッチングは最も適切なシステム全体としての要求に関する要求リクエスト１４０を受信する。対応する出力は、この適切な要求を表している複合目標フォーマット３２５である。そして、要求判断基準＋優先順位選別１４３を用いて、適切な要求が適切な企業ポリシーの範囲内において検索される。このようなポリシー１４７は、各管轄範囲が持っている要求の種別とカテゴリを規定している。要求は、メールのやりとり、ソフトウェアのインストール要求など様々であり得る。ポリシー１４７は、企業にとっての要求の優先順位は何であるかを決めている。各部門に関連付けられた定義にしたがって、その定義に対応する部署と要求が関連付けられる。このようにして、パーミッションチェックが実行される。事例：要求マップマッチングが、従業員全員の履歴書をダウンロードしたいという人事部のリクエストを許可した。理由は、今は従業員の能力に応じて各々の業績を年次評価する時期だからである。初期パース１４８により、各管轄範囲部門が、要求の参照のためにダウンロードされる。部門要求の計算１４９により、各部門に関連付けられた定義にしたがい、要求が各対応する部署と関連付けられる。このようにして、パーミッションチェックが実行される。事例：要求マップマッチングが、従業員全員の履歴書をダウンロードしたいという人事部のリクエストを許可した。理由は、今は階層構造マップで定義された管轄範囲に応じて従業員の業績を年次評価する時期だからである。

サイバースペースにおける秘密オペレーションによる秘密機械学習（ＭＡＣＩＮＴ）および報復

【００９２】

図２７に、知的情報の管理、閲覧、および制御を示す。アグリゲーション１５２を参照すると、多数のプラットフォームから情報ストリームがマージされ、タグ付けされつつ、汎用のレベル判定基準を使用して、不必要で冗長な情報が遮断されている。設定および導入

サービス１５３は、新たな企業の資産（コンピュータ、ノートパソコン、携帯電話）を、正しいセキュリティ設定と通信設定で導入するためのインタフェースである。あるデバイスが追加され設定が行われた後、セキュリティ設定と通信設定は、管理フィードバック制御を仲立ちに、管理コンソールを通じて微調整される。設定および導入サービスは、新たな顧客／クライアントのユーザアカウントの導入も管理している。この導入は、ハードウェアとユーザアカウント、インタフェースのカスタマイズ、顧客／クライアント変数（たとえば、ビジネスタイプ、製品タイプなど）のリストとの関連付けを含んでもよい。管轄範囲による分割１５４によって、タグ付けされた情報のプールが、管理コンソールのユーザに該当する管轄範囲にしたがって、排他的に分割される。脅威による分割１５５によって、個々の脅威にしたがって情報が整理される。あらゆる型のデータは、ある（多少の情報を追加する）脅威と関係付けられるか、あるいは削除される。知的文脈化１５６とラベル付けされたプロセスのこの段階に至ると、残ったデータは、一群の島々のように見える。セキュリティ分析の熟達のために、各プラットフォーム間で相互関係が結ばれる。脅威パターンを読み解くため、（ＬＩＺＡＲＤ１６とは対照的に、I^2ＧＥ２１から）履歴データがアクセスされ、ＣＴＭＰが、クリティカルシンキング分析のために使用される。脅威ジレンマ管理１５７によって、サイバーセキュリティの脅威が、俯瞰図（全体像）から認知される。このような脅威は、グラフィカルに表現するために、管理コンソールに渡される。脅威の仕組みに関連する、計算された測定値が、最終的に多数のプラットフォームからマージされているので、より多くの情報を得た状態で、脅威を管理する上での判断が自動的に実行される。自動化制御１５８は、ＭＮＳＰ９、ＴＰ、３ＰＳの管理に関する制御を行うことにアルゴリズムがアクセスすることを表している。管理フィードバック制御１５９は、ポリシー決定、科学捜査、脅威の調査をなど容易にするために使用できる、すべてのＭＮＳＰクラウド、信用プラットフォーム１０、追加のサードパーティサービス（３ＰＳ）に基づくサービスの、ハイレベルな制御を提供している。このような管理制御は最終的に、カスタマイズ可能な適切な画像と効率的なプレゼンテーションとともに、管理コンソール（ＭＣ）上に明示される。これによって、必要に応じて拡大して詳細を見ることのできる単一のインタフェースから直接、システム（ＭＮＳＰ、ＴＰ、３ＰＳ）全体が効率的に制御・操作可能になっている。手動制御１６０は、ＭＮＳＰ９、ＴＰ（信用プラットフォーム）、３ＰＳ（サードパーティサービス）の管理に関する制御を行うことに人間がアクセスすることを表している。ダイレクトマネジメント１６１が、ヒューマンインターフェースを提供するために、手動制御を活用している。カテゴリおよび管轄範囲１６２によって、管理コンソールのユーザは、自分の管轄範囲および情報カテゴリアクセスの範囲を定義したログイン認証情報を使用する。すべてのデータベクタの候補１６３は、移動中のデータ、休止中のデータ、および使用中のデータですべてである。カスタマイズ可能な画像１６４は、企業のさまざまな部署（経理、金融、人事、ＩＴ、法務、セキュリティ／総括監察官、プライバシー／情報公開、労働組合、など）および当事者（それぞれの部署のスタッフ、管理職、幹部）、加えて、サードパーティパートナー、法執行機関がなど使用するためのものである。統合単一ビュー１６５は、監視、ログ採取、レポート発行、イベントの関係付け、アラートの処理、ポリシー／ルールセット生成、修正処置、アルゴリズム調整、サービスプロビジョニング（新しい顧客／変更）、信用プラットフォームの利用、加えて、サードパーティサービス（サードパーティサービスプロバイダおよびサードパーティサービスベンダをからのレポートおよびアラート／ログ、をなど受信することを含む）など、機能の候補のすべての、単一ビューである。全方面セキュリティの統合ビュー１６５は、画像は、境界、企業、データセンター、クラウド、リムーバブルメディア、モバイルデバイスをなど表す画像の集合である。サイバーセキュリティチーム１６７は、多数のシステムの活動および状況を全体にわたって監視する、有資格の専門家達である。知的情報処理およびＡＩによる判断が行われているので、経験年数の少ない人員を少人数だけ雇うことができるため、コストを下げることが可能である。このチームの第一の目的は、大量の分析ポイントを処理しつつ、システムが所望の判断基準にしたがって発達し向上していることを検証することにおいて、万一の時に頼りになるものとなることであ

る。挙動分析１６８は、１００％模擬データの環境３９４にいる間のマルウェア１６９の状態と行われた活動を観察している。このマルウェアが偽データ１７０とやりとりをしている間、挙動分析は、活動時間（たとえば、事務所が閉まっている毎日曜日のみ活動）中に観察されたパターン、ファイルアクセス権のリクエスト、リクエストされたルート管理者関数をなど記録する。マルウェア１６９がハッカー１７７によって仕掛けられている。ハッカーは標的システムにマルウェアを仕掛けることができたと信じているが、このマルウェアは１００％模擬データの環境３９４に何も知らされずに転送され隔離される。偽データ１７０では、マルウェア１６９は偽データのコピーをデジタル的に所有している。このデータが本物であるという印象のもとで、マルウェアはこのコピーを所有しており、マルウェアひいてはハッカー１７７はデータが本物か偽物かということは気にとめていない。マルウェアが偽データをハッカーのもとへ送信しようとしているとき、その送信される信号は、マルウェアが期待している本物のハッカーではなく、偽のハッカー１７４が受信するようにルーティングされる。ハッカーインタフェース１７１によって、（管轄範囲的にＬＩＺＡＲＤシステムに属する）構文モジュール３５および目的モジュール３６が、マルウェア１６９のコード構造を受信する。これらのモジュールは、マルウェアの内部構造についてリバースエンジニアリングを行い、ハッカーインタフェースを出力する。このインタフェースは、マルウェアとハッカーとの間で使われる通信方法、マルウェアがハッカーに対して期待していること（たとえば、指令を受信するなど）、およびハッカーがマルウェアに対して期待していること（たとえば、ステータスレポートなど）を細部にわたって説明する。このような情報によって、偽のハッカー１７４および偽のマルウェア１７２を仮想環境１７３の中でエミュレートすることができる。挙動分析１６８がマルウェア１６９の挙動を一度十分に学習すると、ＭＮＳＰ９の信号擬態機能が、ハッカー１７７のように振る舞うプログラムをエミュレートすることができる。このエミュレートには、本物のマルウェア１６９、偽データ１７０、および偽のハッカー１７４の間に存在する通信プロトコルが含まれる。エミュレートされた信号応答１７５によって、仮想化された偽のハッカー１７４は応答信号を本物のマルウェア１６９に送信することで、本物のマルウェアに、その仕事がうまくいったか失敗したかのどちらか印象を与える。このような信号は、マルウェアの挙動についての指令および／または最新のステータス情報のリクエストを含むことがある。このことは、さらなる挙動分析の調査、マルウェアの次の挙動パターンを観察するために行われる。調査が完結すると、このマルウェアを有する模擬データ環境３９４は、凍結あるいは破壊できる。エミュレートされた応答コード１７６によって、ハッカーは、本物のマルウェアの挙動／状態と関係のない偽の応答コードが与えられる。所望の報復戦術によって、偽のエラーコードまたは偽の成功コードを送信することができる。偽のエラーコードは、マルウェアが（実際には動作していても）動作していないという印象をハッカーに与え、無関係なもののデバッグという無用な作業のためにハッカーの時間を費やすことになる。エラーコードが正しいと、ハッカーが新しい形態のマルウェアを作製することに注意をそらす可能性が低くなり、そのかわりに現在のマルウェアとさらなる可能な改良に集中することになる。このようなマルウェアはすでに攻略され、ＬＩＺＡＲＤが把握しているので、ハッカーは、攻略されたマルウェアがうまく作動していると思い込んでこのマルウェアにエネルギーを費やしている。ハッカー１７７は自身が仕掛けたマルウェアが標的システムに首尾良く潜入していると未だに信じている。実際には、マルウェアは仮想環境の中に隔離されている。その同じ仮想環境は、このマルウェアについて挙動分析１６８の役割を果たすことで、マルウェアがハッカーと通信する方法と構文を（その通信が双方向性であれ全方向性であれ）エミュレートしている。犯罪資産１７８は、犯罪資金１８４を使って行われた、犯罪システム４９のハッキングや悪意のある活動を手助けするための投資を表している。このような資産１７８は、典型的には計算機能力とインターネット接続を示しており、これら２つの資産に強力な投資を行っていることで、より高度で手の込んだハッキング能力を可能としている。犯罪コード１７９を用いて、信用プラットフォームのエージェントがエクスプロイトスキャンを実行し、可能な限り多くの科学捜査的証拠を集める。犯罪コンピュータ１８０を用いて、ＡＶＸ命令でＣＰＵをオーバ

ーフローさせるＣＰＵエクスプロイトが実行される。この実行により、発熱が増加し、電力消費量が増加し、ＣＰＵの劣化がより進み、犯罪プロセスのための処理能力がより使用不能になる。犯罪資産１７８の能力と性質を特定するために、それに対するプロイトスキャン１８１が実行される。スキャンの結果はエクスプロイト１８５によって管理され、信用プラットフォーム１０に転送される。エクスプロイト１８５は、ＭＡＣＩＮＴの図２７～図４４で列挙するように、標的となる犯罪システムに潜入する報復エクスプロイトデータベース１８７を経由して信用プラットフォームによって送信されたプログラムである。電力および冷却のための支出が大幅に増加し、犯罪資金１８４を枯渇させる。コンピュータをシャットダウンさせることで犯罪活動を厳しく阻止する。新たなコンピュータを購入することで、犯罪資金により負担がかかり、さらに、その新たなコンピュータも、それまでのコンピュータのようにエクスプロイトされやすい。報復エクスプロイトデータベース１８７は、ハードウェアベンダ１８６が設置されたバックドアおよび既知の脆弱性として提供する犯罪活動をエクスプロイトする手段を含んでいる。統合科学捜査的証拠データベース１８８は、多数の企業にわたる多数のソースから収集された科学捜査的証拠を含んでいる。このようにして、最も強力で考えうる訴訟事例が犯罪企業に対して確立され、該当する裁判所において提示される。標的の選択１８９によって、ある標的に対して十分な科学捜査的証拠を揃えた後、その標的が報復のためのみに選択される。これには、監視（たとえば６か月間）による審査のために法医学訴訟が係属するための最低限の時間要件が含まれる場合がある。証拠は高度に自己補強的なものでなければならず、個々のイベントは、無実の標的を攻撃することへの恐怖感や法的な影響から外れた報復の役割を果たすためには使われない。ターゲット検証１９０によって、以下のものを含む、考えうるいかなる秘匿の方法（街中のカフェ、ＴＯＲネットワークなど）より優れた複数の方法を使って疑わしい犯罪システムが検証される。

・物理的な場所ＧＰＳを利用できるクラウドサービスが裏付け作業において助けとなる（たとえば、長い間の習慣になっている、Ｄｒｏｘｂｏｘにサインインした場所）
・物理的なデバイスＭＡＣアドレス、（メーカー／ベンダからの）シリアル
・人物の検証セキュリティシステム上の生体認証データを使用する、正面のカメラで写真を撮影する、複数のプラットフォームにわたって一貫したログイン認証情報の裏付け作業

【００９３】

図３３は、ＭＡＣＩＮＴ秘密オペレーションの概要を示しており、犯人が企業システムを悪用する様子を示している。企業システム２２８は、企業のインフラおよび財産の全体的なスコープおよび管轄範囲を定義している。企業コンピュータ２２７は、機密情報２１４を含んでおり、自身の典型的にスケジュールされたタスクのために企業ネットワーク２１９に依存していることから、企業システム２２８の重要な部分である。潜伏二重スパイ２１５は、休眠状態にあってターゲットコンピュータ２２７で「眠っている」悪意のあるソフトウェアである。二重スパイは活性がないため、被害が発生していない場合に検知することは、プログラマやサイバーセキュリティのアナリストにとって非常に難しい。犯罪システム４９のハッカーが二重スパイ２１５を使用するための機会を見つけると、機密ファイル２１４のコピーがエージェント２１５により何も知らされずに捕捉される。この段階で、ハッカーは痕跡が残るよう自身をさらしているが、それは、アドミニストレーターが認知していない状態でエージェント２１５をインストールする機会を十全に利用すべき時（たとえば、ファイル２１４に価値がある場合）のためのハッカー自身の判断によるものである。段階２１６では、捕捉したファイルは、暗号化を経由し、企業ネットワークの外側にある犯罪者の宛先サーバに送られる。このような暗号化（たとえば、ｈｔｔｐｓ）は、ポリシーによって許可されている。このため、この送信は、すぐにはブロックされない。捕捉したファイル２１４は、企業システム２２８を離れて任意のシステム２６２、ひいては犯罪システム４９に入るために、企業ネットワーク２１９のネットワークインフラに渡される。このネットワークインフラはＬＡＮルーター２１７とファイアウォール２１８として表され、これらはマルウェアにとって、捕捉したファイル２１４を企業システムの外側へ移送可能となる前の、最後の通過障壁である。業界標準のファイアウォール２１８

（この例では捕捉したファイル２１４を盗み出すことを妨げないとされている）はログ集約２２０へ転送されるログを生成する。このログ集約は、その後、長期／深層スキャン２２１とリアルタイム／表面スキャン２２２の両方について、データをカテゴリ別に分離する。結果なし２２３のケースシナリオによると、リアルタイムスキャン２２２は、悪意のある活動をほぼ即時に認識して、それを実行する前に停止させるために、準備は不十分である。マルウェアとのつながりを発見２２４によると、長期スキャン２２１は、分析により多くの時間を掛けることが出来るという利点を有するので、悪意のある挙動を最終的に認識する。時間が潤沢にあるので、長期スキャン２２１は、より複雑なアルゴリズムとより多くのデータポイントを用いて徹底した調査が可能となっている。ボットネットに攻略されたセクタ２２５によって、任意のサードパーティのシステムに属する、あるコンピュータが使用され、機密ファイル２２６を転送し、調査を逃れて当該任意のサードパーティに濡れ衣を着せる。窃盗犯は、その存在を隠し続けながら、彼らのボットネット２２６を通じて機密ファイル２２６を受け取り、続いて非合法な恐喝や利益のためそのファイルを使用する。犯罪コンピュータのアイデンティティ（たとえば、ＩＰアドレス）の残りの可能性のある痕跡は、任意のコンピュータ２３８に残る可能性のみがあるが、その任意のコンピュータには、企業システム２２８の管理者および調査者がアクセスすることができない。

【００９４】

図３４は、ビッグデータ２３１を用いる長期／深層スキャン２３０をより詳細に示している。深層スキャン２３０は、「共謀検知」および「外来エンティティ管理」の２つのサブアルゴリズムを活用して、ビッグデータ２３１に貢献および連動する。中間結果が、最終結果に責任のある異常検知にプッシュされる。ファイアウォールやセントラルサーバのようなセキュリティチェックポイントからの標準ログが集約され、ログ集約２２０の低制限フィルタにより選択される。イベントインデックス＋トラッキング２３５により、イベントの詳細、たとえばＩＰアドレス、ＭＡＣアドレス、ベンダＩＤ、シリアル番号、時刻、日付、ＤＮＳがなど格納される。これらの詳細はローカルデータベースとクラウド共有データベースの両方に存在する（データについてこれらのデータベースは同一ではない）。ローカルに保存されたこれらのエントリが、他の企業の便宜になるように、クラウドデータベースに（企業によるポリシー制限付きで）プッシュされる。その見返りとして、有用なイベント情報がローカル分析のために受信される。信用できるサードパーティ２３５に登録されたある企業は、すでにボットネットによる侵害を経験しており、そのようなリスクを軽減する予防のための詳細な情報を提供することができる。セキュリティ挙動２３６によって、セキュリティ行動ガイドラインが、ローカルデータベースとクラウド共有データベース（データについてこれらのデータベースは同一ではない）に格納される。このような行動ガイドラインはシステムの安全を保証するための行動の要点を定義している。たとえば、あるＩＰアドレスがシステムにアクセスし、そのＩＰアドレスが、イベントインデックスによれば１０回に６回はボットネットに関連している場合、このＩＰアドレスを３０日間禁止し、この期間中にＩＰアドレスがシステムにアクセスしようとするいかなる試みもマークするために、ログシステムに優先フラグを設定する。ローカルに保存されたこれらのガイドラインが、他の企業の便宜になるように、クラウドデータベースに（企業によるポリシー制限付きで）プッシュされる。その見返りとして、有用なイベント情報がローカル分析のために受信される。異常検知２３７によって、イベントインデックスおよびセキュリティ挙動は、深層スキャンモジュールによって提供された中間データにしたがって使用され、機密ファイルが未認証のエージェントによって企業ネットワーク外の任意システムに転送されるような、可能性のあるリスクイベントを決定する。任意コンピュータ２３８が、この侵害に関与した宛先サーバとして示され、強調され、ＭＡＣアドレス／最後の既知のＩＰアドレス２３９、国、稼働時間パターンなどの既知の特性によって定義される。このような分析は、主に外来エンティティ管理２３２モジュールを必要とする。このシステムは、こうしてそのようなコンピュータがボットネットに関与している可能性２４０を決定することができる。このような分析は、主に共謀検知１９を必要とする。

【００９５】
図３５は、信用プラットフォーム１０上で任意コンピュータが検索されて、その任意コンピュータまたはその関連／近隣サーバ（この任意コンピュータが接続するサーバ）が、信用プラットフォーム１０に対する、過去に設置した二重または三重のスパイであるかをチェックする様子を示している。ステージ２４２は、ＭＡＣアドレス／ＩＰアドレス２３９などの任意コンピュータ２３８の既知の情報が、イベントインデックス＋トラッキング２３５およびクラウドバージョン２３２で照会するために送られる様子を表している。信用プラットフォーム１０から動作するこのクラウドバージョンは、将来の脅威と、ＭＡＣアドレス、ＩＰアドレス、アクセスのタイムスタンプなどの脅威パターンを識別するためにイベントの詳細を追跡する。このような照会２４２の結果がシステムコレクションの詳細２４３に送信される。この詳細には、元の任意コンピュータ２３８の詳細、定期的にコンピュータ２３とパケットを受信および／または送信しているコンピュータ／システム、およびコンピュータ２３８に物理的に近接しているシステムが含まれている。そして、これらの詳細は、上述のこれらのコンピュータ／システムがたまたま二重スパイ２４７や三重スパイ２４６となっているかどうかを確認するステージ２４６および２４７に転送される。このようなスパイ検索調査は、信用できる二重スパイインデックス＋トラッキングクラウド２４４および信用できる三重スパイインデックス＋トラッキングクラウド２４５で実行される。二重スパイインデックス２４４は、信用プラットフォームおよびその系列組織によってコントロールされた潜伏スパイをインストールしたシステムのリストを含んでいる。三重スパイインデックス２４５は、悪意のある活動および展開を監視するために、犯罪シンジケート（たとえば、ボットネット）によって攻略されたが、トラステッドプラットフォーム１０によって個別に攻略されたシステムのリストを含む。これら２つのクラウドはそれぞれ結果を出力し、アクティブで重要なスパイのリスト２４８に集められる。
【００９６】
図３６は、信用プラットフォーム１０からの既知の二重または三重スパイが、将来の科学捜査的調査に関わるようになる様子を示している。スパイのリストから転送されて２４８、適切な二重スパイ２５２が起動される２４９。二重スパイのコンピュータ２５１（これは任意コンピュータ２３８に信用されている）は、信用されているチャネル２５４を通じてエクスプロイト２５３をプッシュする。任意コンピュータ２３８に無事に配置されると、エクスプロイト２５３は機密ファイル２４１の行動を追跡し、今では犯罪コンピュータ２２９だと知られているところへ送信されたことを知る。このエクスプロイトは、チャネル２５５で初めて２１６ファイル２４１を転送するために使用されたのと同じ経路をつたって、犯罪コンピュータ２２９上に定着しようとする。エクスプロイト２５３は次に機密ファイル２５１を発見しようとし、それを検疫し、その正確な状態を信用プラットフォーム１０に送り返し、次に、その機密ファイルを犯罪コンピュータから安全に消去しようとする。信用プラットフォーム１０は次にこの検疫されたファイルを、科学捜査の目的で、（原本のファイルを所有していた）元の企業システム２２８へ転送する。エクスプロイト２５３が機密ファイル２４１を取り返すことができたことは常に保証されるわけではないが、少なくともエクスプロイトは犯罪コンピュータ２２９とシステム４９について特定可能な情報２３９を転送することはできた。
【００９７】
図３７は、信用プラットフォーム１０が任意コンピュータ２３８に関するＩＳＰ（インターネット・サービス・プロバイダ）２５７のＡＰＩをどのように利用するかを示している。さらなる司法調査にむけて任意システム２６２を試して攻略するために、ネットワーク監督２６１が使用される。企業システム２２８は、任意コンピュータ２３８についての限定的な情報２５９を知っているだけであり、犯罪コンピュータ２２９およびシステム４９についての情報を探す。ＩＳＰ２５７のＡＰＩリクエストが、信用プラットフォーム１０で生成される。ネットワーク監督２６１では、任意システム２６２に関するシステムネットワークログが見つかり、さらには、犯罪コンピュータ２２９（として後に認識されるもの）にファイルが転送されたらしいことがわかる。ログの履歴は、機密ファイル２４１の

正確かつ完全な構成を記録しているほどは詳細ではないが、メタデータ２６０を使用して、ファイルがどのコンピュータに送られたかを、かなりの確信度をもって決定することができる。ネットワーク監督２６１は、犯罪コンピュータ２２９のネットワークの詳しい情報２５８を発見し、このような情報を、別ルートで信用プラットフォーム１０に送り、次に企業システム２２８に通知する。

【００９８】

図３８は、信用プラットフォーム１０を使用して、ソフトウェアベンダ２６８およびハードウェアベンダ２７２が提供するセキュリティＡＰＩを実行し、司法調査を支援することができる、設置されたバックドアをエクスプロイトする方法を示している。ステージ２６３において、犯罪コンピュータ２２９の既知の身元の詳細情報は、バックドアＡＰＩを実行するために信用プラットフォーム１０に転送される。この詳細情報は、ＭＡＣアドレス／ＩＰアドレス２３９および犯罪コンピュータの、疑いのあるソフトウェア＋ハードウェアを含み得る。信用プラットフォーム１０は次に、エクスプロイト２５３を系列組織のソフトウェアベンダ２６８およびハードウェアベンダ２７２に、休眠状態で（エクスプロイトのコードが転送されるが実行されない）伝送する。これらのベンダには、ステージ２６３で企業システム２２８に疑わしいとされた、犯罪コンピュータ２２９の疑いのあるソフトウェア２６９およびハードウェア２７３も伝送される。ベンダは、設置されたソフトウェアバックドア２７０およびハードウェアバックドア２７４のリストを維持管理しており、そのリストには、それらのバックドアを起動する方法、採用されている認証方法、それらのバックドアで可能なことおよび制限事項といった情報が含まれている。これらのバックドアはすべて内部的に隔離されており、ベンダ内部からは秘密にされているため、信用プラットフォームはこれらのバックドアを扱うための機密情報を受け取っていないが、バックドアからの助けを得るエクスプロイト２５３を提供する。ソフトウェアバックドア２６７またはハードウェアバックドア２７１の設置に成功すると、エクスプロイト２５３は犯罪コンピュータ２２９に別個にインストールされる。機密ファイル２４１は、そのメタデータ使用履歴を後で分析できるように検疫されコピーされる。犯罪コンピュータに残っている機密ファイルのコピーは、その後安全に消去される。その他のあらゆる補足的な科学捜査的証拠となるようなものが集められる。これらの科学捜査的データはすべて、信用プラットフォーム１０にある、エクスプロイト２５３の接点に返送される。その後、犯罪コンピュータ２２９で見つかった機密ファイル２４１、およびこのファイル２４１の最初の窃盗に関わった者達に対する証拠を有する犯罪システムに関わったそれらの人物の身元を含む科学捜査的証拠２６５は、企業システム２２８へ転送される。このようにして、最初の窃盗の間に犯罪者達のシステムから削除されると、企業システム２２８はこのファイル２４１を回復でき、身元の詳細２６４は、損害賠償額の形での報復を模索することと、今後の攻撃のリスクを軽減させるために犯罪システム４９のボットネットを無力化することを可能とする。

【００９９】

図３９～図４１は、汎用エクスプロイト２８２およびカスタマイズ可能なエクスプロイト２８３が、任意コンピュータ２３８および犯罪コンピュータ２２９に適用される様子を示している。汎用エクスプロイト２８２は、独立したサイバーセキュリティの調査を通じて企業システム２８０によって収集整理された、ソフトウェアエクスプロイト、ファームウェアエクスプロイト、およびハードウェアエクスプロイトのコレクションである。エクスプロイトのカスタマイズ２８３では、エクスプロイトは、標的についての既知の情報にしたがってカスタマイズされる。エクスプロイト２５３は、成功する確率が最も高いものが最初に、成功する可能性が最も低いものが最後になる順で配布される。犯罪コンピュータ２２９に関する有用な情報のコレクション２８４は、カスタマイズ２８３に転送される。この情報は、犯罪コンピュータ２２９によって使用されている、ＭＡＣアドレス／ＩＰアドレス２３９および疑いのあるソフトウェア＋ハードウェア２８５のような、既知のコンピュータ情報を含んでいる。プロキシマネージメント２８６は、エクスプロイトの試みに使われるプロキシを知的に選択するアルゴリズムとデータベースの組み合わせである。プ

ロキシネットワーク２７９は、個々のシステムについてその身元を隠すことを可能とする、一群のプロキシノード２７８である。ノードは、このようなデジタル通信を渡すことで、見かけの発信者になる。あるノードの総合的なパフォーマンス、あるノードの可用性、およびあるノードの現在の作業負荷にしたがい、各ノードはプロキシマネージメント２８６によって知的に選択される。犯罪コンピュータ２２９および／または任意コンピュータ２３８の、見込みのある３つのエクスプロイトポイントが試される。犯罪コンピュータ２２９に対するエクスプロイトが失敗した場合、エクスプロイトはそれでも科学捜査的調査全体を可能にするものなので、どちらにしても任意コンピュータ２３８に対するエクスプロイトが行われる。第一の方法は、直接エクスプロイトすること、第２の方法は任意コンピュータのボットネットトンネル２７６経由、そして第３の方法は犯罪システムがボットネット２７７をインストールするために使用したエクスプロイトの独自の手段（ならびに、他の未使用のエクスプロイトポイント）である。ボットネットトンネル２７６は、犯罪コンピュータ２２９と、ボットネット２４０のアクティブな部分との間で使用された通信の確立された手段である。エクスプロイトが生成したいかなる科学捜査のデータも、ステージ２７５にて企業システム２２８に送信される。

【０１００】

図４１は、信用プラットフォーム１０の特別なＡＰＩが使用されて犯罪コンピュータ２２９に対してソフトウェアまたはファームウェアの更新２８９を行うことにより、新たなバックドアを設置する様子を示している。隠密であることを守るために、プラセボアップデート２８８が近隣の類似機器にプッシュされる。企業システム２２８は、ターゲットの身元詳細情報２９７を信用プラットフォーム１０に送信する。このような詳細情報には、ＭＡＣアドレス／ＩＰアドレス２３９が含まれている。信用プラットフォーム１０は、ソフトウェア／ファームウェア保守者２８７と通信し、プラセボアップデート２８８およびバックドアアップデート２８９を該当するコンピュータにプッシュする。このバックドアアップデートは、犯罪コンピュータ２２９に既に設置したソフトウェアアップデートシステムを使用することにより、犯罪コンピュータ２２９のシステムに新たなバックドアを導入する。このようなアップデートは、オペレーティングシステム、ＢＩＯＳ（ファームウェア）、ワープロのような特定のソフトウェアのために行われることがある。プラセボアップデート２８８は、セキュリティが攻略されないようバックドアを取り除くが、バックドアアップデート２８９と同一の詳細および特徴（たとえば、アップデートナンバー／コード）を示すことで、バックドアの隠密性が維持された環境を喚起する。保守者２８７は、バックドア２９５を標的に転送し、加えて標的に平均以上の露出をしているコンピュータにも転送する。このようなさらなるコンピュータ２９６は、犯罪システム４９のインフラに属するものであってもよいし、犯罪コンピュータ２２９と同じローカルネットワーク上にあるものであってもよい。このようなさらなるコンピュータ２９６をエクスプロイトすることにより、直接攻撃が不可能な場合（たとえば、オペレーティングシステムの更新をオフにする場合など）に、犯罪コンピュータ２２９への侵入経路を得る機会が増える。すると、エクスプロイト２５３は、近くのコンピュータ２９６上に自身を設置することができる場合、標的への異なる侵入点を検討することができる。標的に対して平均的に露出している関与コンピュータ２９１に対して、プラセボアップデート２２８が送り込まれる。露出していることは、共有ネットワーク（たとえば、仮想プライベートネットワークなど）または共有サービスプラットフォーム（たとえば、ファイル共有など）を共有するものとして理解することができる。関与システム２９０は、同じ会社の法的構造などによって所有されるなど、犯罪システム４９に戦略的に結び付けられてもよい。近隣システム２９２に属する近隣コンピュータ２９３は、標的犯罪コンピュータ２２９と物理的位置が近い（同じ地区など）ため、プラセボアップデートがなされる。近い将来に保守者２８７が配布する予定の定期的なアップデート（または調査に適していて実行可能なもの）はないものの、時間的制約のある科学捜査的調査を可能にするために、関与システム２９０および近隣システム２９２の双方に対してプラセボアップデート２８８がなされる。ソフトウェア／ファームウェアの改良を意図した定期的なアップデートがあるケースシナリオでは、

関与システム２９０および近隣システム２９２は、バックドアアップデート２８９に関する認知された正当性を検証するためにプラセボアップデートをする必要はない。代わりに、バックドアアップデート２８９は、犯罪コンピュータ２２９およびさらなるコンピュータ２９６を標的とした正当なアップデートの一部に仕掛けることができる。バックドアアップデート２９５を通じてエクスプロイト２５３の設置が成功すると、機密ファイル２４１は、そのメタデータ使用履歴を後で分析できるよう検疫されてコピーされる。犯罪者コンピュータ２２９上の残りのコピーは、その後、確実に消去される。補足となる科学捜査的証拠はいずれも集められる。その後、科学捜査データは、信用プラットフォーム１０にある、エクスプロイトの接点に送信される。データが信用プラットフォーム１０で検証されると、結果２８１で企業システム２２８に転送される。

【０１０１】

図４２は、ありとあらゆる変更／アップデートについて犯罪システムをモニターするために、長期優先フラグが信用プラットフォームにプッシュされる様子を示している。調査を容易にするために、新規の開発は、長い期間優先的に監視される。まず、企業システム２２８は、信用プラットフォーム１０のサブセットであるワラントモジュール３００に、標的２９７（識別可能な詳細情報２３９を含む）を提出する。このワラントモジュールは、すべての系列システム３０３の入力２９９をスキャンして、定義された標的２９７の任意の関連性を検索する。一致するものがあれば、その情報は企業システム２２８に渡され、企業システムは、そのワラントを定義しており、標的２９７へ潜入しようとしている。情報入力２９９は、信用プラットフォーム１０の系列システムが報告した情報であり、通常はいくつかの所望の分析を受けることになる。また、信用プラットフォーム１０で認定と評判を得ることを唯一の目的とした入力が提出されることもある。系列システム３０３は、自身の入力を信用プラットフォーム１０に提出する。これは、標的２９７をモニターしようとする企業システム２２８に有利に働く。これによって、これらの系列システム３０３のうちの１つが標的または標的に関係するものに遭遇した可能性が、それがポジティブ、ニュートラル、またはネガティブな相互作用であろうと、高まる。そのような入力２９９は、所望の分析モジュール３０１に転送され、分析モジュールは、相互に有益なセキュリティ情報を同期させるための、信用プラットフォーム１０のほとんどの機能を表す。系列システム３０３は、セキュリティリクエストを送信し、セキュリティ情報を交換する。標的２９７または標的に関係するもの関係する情報が見つかると、その情報もまた、ワラントモジュール３００に並行して転送される。分析モジュール３０１の情報出力３０２は、系列システム３０３に転送され、要求されたタスクまたは機能を完了する。標的２９７に関するワラントモジュール３００によって学習された有用な情報は、企業システム２２８の法医学調査の一部として結果２９８に転送される。

論理的推論によるゼロデータベースの演繹型リアルタイム防御（ＬＩＺＡＲＤ）

【０１０２】

図４３および図４４は、ＬＩＺＡＲＤ（論理的推論によるゼロデータベースの演繹型リアルタイム防御）の依存構造を示している。静的コア１９３は、主に不変のプログラムモジュールが人間のプログラマによってハードコードされている場所である。イテレーションモジュール１９４は、ダイナミックシェル１９８上のモジュールを知的に変更、作成、および処分する。イテレーションモジュールは、セキュリティ上のパフォーマンスの参考のために、疑似セキュリティ脅威（ＡＳＴ）を使用し、イテレーションコアを使用して自動コード記述の方法論を処理している。図５１に示すように、イテレーションコア１９５は、セキュリティを改善するためにダイナミックシェルを繰り返し実行するためのメインロジックである。差分変更アルゴリズム１９６は、ＡＳＴが見つけた欠陥にしたがって基底バージョンを修正する。差分ロジックが適用された後、新バージョンが提示され、その直後にイテレーションコアが再帰的に呼び出され、ＡＲＴによってテストされたものと同じプロセスを経る。論理減算アルゴリズム（ＬＤＡ）１９７は、疑似セキュリティ脅威（ＡＳＴ）からダイナミックシェルのバージョンの既知のセキュリティ応答を受信する。ＬＤ

Ａはまた、どのコードセット構成が既知の正しい応答をなし得るかを、（ＡＳＴによって提供される）セキュリティシナリオに合わせて推論する。ダイナミックシェル１９８は、イテレーションモジュールによって自動的にプログラムされたダイナミックプログラムモジュールを主に含む。コード検疫１９９が、外来コードを制限付の仮想環境（たとえば、シャーレ）に隔離する。秘密コード検知４１が、データおよび送信パケット内に密かに埋め込まれたコードを検知する。ＡＳＴオーバーフロー中継２０１では、システムが低確信度の判断しかできないときは、将来のバージョンの改善のために、データがＡＳＴに中継される。内部整合性チェック２０２が、外来コードのブロックのすべての内部機能の辻褄が合っているかどうかをチェックする。外来コード全体としての目標と内部的に相容れないコードの断片が存在しないことが確かめられる。外来コード改訂２０３では、外来コードの目標が導出された後、コードの一部あるいは全部が改訂され、改訂版だけが実行を許可される。ミラーテストが、改訂版の入出力挙動が、元のコードのものと同じであることを確かめる。このようにして、元のコードに存在する任意の隠されたエクスプロイトは使われなくなり、二度と実行されることがない。要求マップマッチング２０４が、外来コードがシステムの目的全体（たとえば、パズル）にフィットしているかを判断するために、マップ化された要求および目標の階層構造が参照される。実データ同期部２０５は、混合環境に与えられるデータを、どの優先順位で与えるのかを知的に選択している、２つのレイヤのうちの１つである（もう一つはデータマネージャである）。このようにして、極秘情報は疑われるマルウェアからはアクセスできず、周知で信用できることが確立されたコードだけに利用可能となる。データマネージャ２０６は、仮想環境の外部から来るエンティティとデータとの間にある中間者インタフェースである。フレームワークコーディネーター２０７は、すべての入力、出力、スレッドの産出、および半人工アルゴリズムまたは人工アルゴリズムの診断をすべて管理する。仮想難読化２０８が、仮想化された偽の環境に、徐々にかつ部分的に沈めることで、コードを乱雑にし、制限する。秘密輸送モジュール２０９が、マルウェアに何も知らせず慎重にマルウェアを模擬データ環境３９４に転送する。目標比較モジュール２１０では、４つの異なるタイプの目的を比較し、システムの全体的な目的に対して良い結果をもたらすことにおいて、そのエンティティの存在および挙動が合理的でＬＩＺＡＲＤによって理解されることを保証する。目的において大きく逸脱している可能性のあるものは、悪意のある行動を示す。模擬データジェネレータ２１１は、実データと区別できないように設計された偽データを作成する。たとえば、ひとまとまりの社会保障番号である。仮想環境マネージャ２１２は、模擬データの比率、利用可能なシステム機能、ネットワーク通信オプション、ストレージオプションなどの変数を含む、仮想環境の構築を管理する。データリコールトラッキング２１３は、疑わしいエンティティ４１５からアップロードされ、疑わしいエンティティ４１５にダウンロードされたすべての情報を追跡する。これは、機密情報がマルウェアに転送される可能性があるというセキュリティリスクを軽減するために行われる。このセキュリティチェックは、正当な企業プロセスが偽データを受信するというロジスティックな問題も緩和する。模擬データが正当な（であると現時点ではわかっている）企業エンティティに送信された場合、すべての模擬データを呼び戻す「コールバック」が実行され、（元々リクエストされた）実データが送信される。

【０１０３】

図４５は、動的に成長するデータベースの直接的な助けなしにリアルタイムで潜在的なサイバーセキュリティの脅威をすべてブロックすることができる集中監督アルゴリズムである、ＬＩＺＡＲＤ（論理的推論によるゼロデータベースの演繹型リアルタイム防御）の概要を示す。システムへのデータ／アクセス権が許可されているかどうかの判断は、知る必要のある場合のみ、機能が必要である場合のみ、そして目的重視という基準で許可される。コードブロックまたはデータが、ハードコーディングされたシステムの目標を達成するための機能／目標を提供できない場合、そのコードブロックまたはデータは、仮想的隔離および難読化を含む秘密の方法で拒否される。ＬＩＺＡＲＤには、コンピュータコードを読み書きできる構文的なインタプリタが装備されている。目標導出機能と組み合わせるこ

とで、見た目には害のないデータに密かに埋め込まれたコードブロックであっても、コードブロックからゴール指向の挙動を導き出すことができる。公衆喫茶店にある会社の電話のように、企業の敷地内ないものであっても、すべての企業デバイスは、ＬＩＺＡＲＤ経由でルーティングされる。企業の資産を稼働させるすべてのソフトウェアとファームウェアは、あらゆる種類のダウンロード／アップロードを、永続プロキシのようにＬＩＺＡＲＤ経由で実行するようにハードコードされている。永続プロキシポリシーの非遵守は、忠実な資産に関する密告ポリシーによって緩和される。企業システム内で発生するデジタル転送は、ＬＩＺＡＲＤ経由で中継するようハードコードされたハードウェアを経由しなければならないため、悪意のコードは安全な場所が見つからず、永続プロキシポリシーを無視する攻略されたコンピュータと共同作業することもできない。ＬＩＺＡＲＤはイテレーションモジュール（ＩＭ）と共生関係にある。ＩＭは、ハードコーディングされたゴール指向のタスクとＬＩＺＡＲＤの構文把握能力をクローンする。そして、これらの構文機能を使用して、ハードコーディングされた目標に合うようＬＩＺＡＲＤを変更する。疑似セキュリティ脅威（ＡＳＴ）モジュールは、ＬＩＺＡＲＤの様々なバリエーションをストレステストにかけるための並列仮想環境に関与する。最高の得点を得たバリエーションが次の正式バージョンとして選択される。ＬＩＺＡＲＤは、サイバーセキュリティソリューションの現状を脱却する革新的なモデルを提供する。高度な論理的推論機能により、現代のサイバーセキュリティ防御に関する「あまりにも遅すぎる」パラダイムを超えて、瞬時で正確なセキュリティ上の決定を行うことが可能となる。ＬＩＺＡＲＤは、移動中のデータ、休止中のデータ、および使用中のデータの３種類のデータと相互作用する。ＬＩＺＡＲＤは、ファイル、電子メール、ウェブ、モバイル、クラウド、リムーバブルメディア（ＵＳＢ）の６種類のデータメディア（ベクトルとも呼ばれる）と相互作用する。企業システム２２８は、ＨＴＴＰやＤＮＳなどのインフラ内で実行されているサーバのタイプを示している。モバイル機器３０５は、街中のコーヒーショップ３０６内で動作しつつも、ＬＩＺＡＲＤライトクライアント４３を介して企業システム２２８のデジタルインフラに接続されているところが示されている。そのようなＬＩＺＡＲＤライトクライアント４３は、暗号化されたＬＩＺＡＲＤクラウド３０８にその後接続するインターネット３０４へのゲートウェイとして機能する。

【０１０４】

図４６は、ＬＩＺＡＲＤに関する主要なアルゴリズムの機能の概要を示している。ＬＩＺＡＲＤの外側ダイナミックシェル（ＤＳ）３１３は、イテレーションを通じた変化を最も受けやすい機能のセクションである。自身の目的を達成するために大きな計算量を必要とするモジュールは、通常、このシェル３１３に属する。というのも、これらのモジュールは、プログラマのチームが直接扱える計算量のレベルを凌駕するからである。イテレーションモジュール３１４は、静的コア（ＳＣ）３１５を使用して、「決定されたゴール」に定義された目標およびデータ返送中継（ＤＲＲ）３１７からのデータにしたがって、ＤＳ３１３のコードベースを構文的に変更する。この改変バージョンのＬＩＺＡＲＤは、疑似セキュリティ脅威（ＡＳＴ）１７によって、多数のさまざまなセキュリティシナリオのもとで（並行して）ストレステストを受ける。最も成功したバージョンが、実稼働バージョンとして採用される。ＬＩＺＡＲＤのこのＳＣ３１５は、自動化されたイテレーションによる変化を最も受けにくく、その代わりに人間のプログラマによって直接変えられる。特に、内側コア３３４とも呼ばれる最も内側の四角形は、自動化されたイテレーションの影響を全く受けない。この最も内側の層３３４は、ＬＩＺＡＲＤの方向および全体的な能力を差配する樹木の根のようなものである。汎用動的モジュール（ＧＤＭ）３１６は、自動化された自己プログラミングの影響を最も頻繁に受け、したがってダイナミックシェル３１３の管轄に属するモジュールのゾーンである。ＧＤＭ３１６で実行されるこのようなプログラムは、常時「ベータ」状態（必ずしも安定しておらず、作業中の未完成品）にある。ＬＩＺＡＲＤが行った判断の確信度が低い場合、ＬＩＺＡＲＤは、今後のＬＩＺＡＲＤのバージョンを改善するために、該当するデータをデータ返送中継（ＤＲＲ）３１７経由でＡＳＴ１７に中継する。ＬＩＺＡＲＤ自身は、判断を行うためのデータに直接頼ること

はなく、脅威を進化させることに関するデータが、将来のＬＩＺＡＲＤのバージョンが行うかもしれない演繹的な意思決定に、間接的に寄与できる。ラベル３４２は、コードの設計において、人間による作業がより関与すると、コードはより静的になる（非常に緩やかに変化する）様子を示している。イテレーションモジュール（ＩＭ）３１４がコードをプログラムするほど、そのコードはより動的かつ流動的になる。構文モジュール３５および目的モジュール３６は、ＳＣ３１５内から機能するように示されている。

【０１０５】

図４７は、静的コア（ＳＣ）３１５の内部動作原理を示している。論理的導出３２０が、論理的に必要な機能を、初期のより簡易な機能から導出する。最終的な結果として、機能の依存性のツリー全体が、宣言された複合目標から構築される。コード翻訳３２１が、構文モジュール機能によって直接読み解かれる任意の（汎用）コードを、任意に選ばれた既知のコンピュータ言語に変換する。既知のコンピュータ言語から任意のコードへの逆翻訳も行われる。ルールおよび構文３２２は、統語構造の解釈および生成を助ける静的な定義を含んでいる。たとえば、Ｃ＋＋プログラミング言語のルールおよび構文は、ルール及び構文３２２に格納できる。ロジック削減３２３が、コードに記述されたロジックを、より簡易な形状にまとめて相互に接続された機能のマップを生成する。記述コード３２４は最終出力、実行可能なプログラムである。対して、コードのゴール３３２は入力である。複合目標フォーマットが３２５は、目標の全体を表している相互に連携する下位目標を格納するための格納フォーマットを表している。目標の関連性３２６とは、挙動の機能および型のどれがどの種類の目標を指しているかを調べるための、ハードコーティングされた参考資料のことである。反復的拡張３２７は、目標の関連性を参照し、詳細と複雑性を追加して、単純なゴールを複合目標に進化させる。反復的解釈３２８は、相互に接続された機能をループ処理し、かつ、目標の関連性３２６を参照することにより、解釈された目標を生成する。外側コア３２９は、協力しあうことで未知の外来コードから論理的な目標を導出し、また宣言された機能コードのゴールから実行可能コードを生成する、構文モジュールおよび目標モジュールによって、主に形成される。外来コード３３０は、ＬＩＺＡＲＤには未知であるコードで、その機能および意図された目標は未知である。外来コード３３０が内側コアへの入力であり、導出された目標３３１は出力である。目標３３１は、目標モジュール３６により推定されたものとしての、任意のコード３３０の意図である。目標３３１は、複合目標フォーマット３２５で返される。

【０１０６】

図４８は、内側コア３３４が、該当するサイバーセキュリティの専門家３１９によって、メンテナンス３１８のプラットフォーム経由で直接かつ独占的にプログラムされた、システムの必須のコア機能を収容する様子を示している。コアコード３３５は、ＬＩＺＡＲＤを稼働するのに必要な、ごく基本的な基盤である。コア３３６において、基本的なフレームワークおよびライブラリ３３６は、圧縮や比較の機能のような、ＬＩＺＡＲＤを運用するのに必要とされる機能のすべてを保持している。コア３３６において、スレッド管理およびロードバランシング３３７は、ＬＩＺＡＲＤに一群のクラスタを効率的に支配することを可能にしているのに対し、通信および暗号化プロトコルは、求められた暗号化の種類（たとえば、ＡＥＳ、ＲＳＡなど）を定義している。コア３３６において、メモリ管理３３９によって、ＬＩＺＡＲＤによって解釈され処理されたデータを、サーバのランダムアクセスメモリー（ＲＡＭ）内で効率的に管理することができる。システムの目標３３６は、セキュリティポリシー３４０および企業のゴール３４１を含んでいる。セキュリティポリシー３４０は、（一人または多くの）サイバーセキュリティアナリストによって、ＬＩＺＡＲＤをカスタム変数に応じて運用するために参照される可能性のあるガイドとして、手動で設計されている。よってＬＩＺＡＲＤは、安全でなく禁止されている処置であると見做されていることと、容認できることのどちらを正しいとすべきかについてのスタンダードを有している。たとえば、それは、組織外の受信者にメールを送信することを禁止するための、あるいはパスワードの入力を３回間違えたときにアカウントをロックするための、企業のセキュリティポリシー３４０の範囲内であることもしれない。企業のゴール３

４１は、どの種の総合インフラをその企業が達成したいと考えているかについての、より広範な特徴を定義している。ゴール３４１は主に、企業のインフラのコンテキストに関してどのような機能をＬＩＺＡＲＤが備えていなければならないか、そしてどのような能力をＬＩＺＡＲＤが示さなければならないかということについて、ダイナミックシェル３１３の自己プログラミングを方向付けるのに使用される。

【０１０７】

図４９は、ダイナミックシェル（ＤＳ）３１３の内部動作原理を示している。ＬＩＺＡＲＤのこのセクションは、主として人工知能プログラミングモジュール（イテレーションモジュール）によって操作される。外側シェル３４５にあるモジュールは、システム全体の意思決定に及ぼす影響が軽微な、新規で実験的なモジュールである。内部シェル３４４は、ＬＩＺＡＲＤの本体であり、ＬＩＺＡＲＤの知的能力の多くがここで運用されている。新規で実験的なアルゴリズム３４３の「ベータ版」にはソフトウェアスペースが割り当てられ、そこでは、人間や人工知能あるいはその両方によって、新規なモジュールの機能上の要求をプログラムおよびテストすることができる。

【０１０８】

図５０は、ダイナミックシェル上のモジュールを知的に変更、作成、および処分するイテレーションモジュール（ＩＭ）を示している。イテレーションモジュールは、セキュリティ上のパフォーマンスの参考のために、疑似セキュリティ脅威（ＡＳＴ）１７を使用し、イテレーションコア３４７を使用して自動コード記述の方法論を処理している。データ返送中継（ＤＲＲ）３１７では、ＬＩＺＡＲＤがやむなく低い確信度で意志決定をしなければならない場合に、悪意の攻撃および常習犯のデータがＡＳＴ１７に中継される。ＡＳＴ１７は、イテレーションプロセスを実行可能にするために、シミュレートされたセキュリティ脅威を伴う仮想テスト環境を生成する。詐欺的で悪意のあるサイバー活動の自然な進化の先を行くように、ＡＳＴ１７の疑似的な進化は、十分に行われる。静的コアクローニング３４６では、セミダイナミック外側コア３２９を備えている静的コア３１５が、イテレーションのガイダンスのための判断基準として使用される。このイテレーションは外側コア３２９を部分的に変更するため、自己プログラミングが人工知能ループにおいて完全なサイクルとなる。イテレーションコア３４７は、疑似的なセキュリティシナリオおよびシステムの目的のガイダンスを受け取り、ダイナミックシェル３１３を改変する。イテレーションコア３４７は、多くのバージョンを生成する。疑似的なセキュリティテストにおいて最良の結果を出したバージョンがアップロードされ、ステージ３４８でダイナミックシェルの、実稼働するバージョンとなる。

【０１０９】

図５１は、セキュリティを改善するためにコードを繰り返し実行するためのメインロジックである、イテレーションコア３４７を示している。再帰的イテレーション３５０では、基底バージョンが新バージョンに置き換わった状態で、操作コア３４７の新しいインスタンスが呼び出される。このような置き換えは、コアコード３３５のサブセットであるスレッド管理およびロードバランシング３３７から導出された、スレッド管理３４９によって管理されている。差分変更アルゴリズム（ＤＭＡ）３５３は、内側コア３３４から、構文／目的プログラミング能力３５１とシステムの目的のガイダンス３５２を受け取る。これら２つの入力は、基本フレームワークとライブラリ３３６、ならびにセキュリティポリシー３４０／企業のゴール３４１と相互に関係がある。そして、差分変更アルゴリズムはこのようなコードセットを使うことで、ＡＲＴ１７が見つけた欠陥にしたがって基底バージョン３５６を変更する。差分ロジックが適用された後、新バージョン３５５が提示され、その直後にイテレーションコア３４７が再帰的に呼び出され、ＡＲＴ１７によってテストされたものと同じプロセスを経る。キューイングされたセキュリティシナリオ３６０は、すべての既知のセキュリティポイントについて、ダイナミックシェル３１３の包括的なテストをまとめて行う、複数のシナリオである。アクティブなセキュリティシナリオ群３６１について、隔離された仮想実行環境３５７において、現在アクティブなセキュリティシナリオでダイナミックシェル３１３がテストされている。このような環境３５７は、本番

システムから完全に切り離された仮想インスタンスである。この環境は、悪意の攻撃や侵入を人為的に実行する。セキュリティテスト結果での欠陥３６２が、仮想実行環境３５７を実行している間に基底バージョンを「パスした」セキュリティ脅威を示すために、可視的に提示される。その後、発見されている欠陥はどれもＤＭＡ３５３に転送され、これらの欠陥を取り除こうとする新バージョンの生成を促進する。

【０１１０】

図５２～５７は、差分変更アルゴリズム（ＤＭＡ）３５３の論理プロセスを示している。現在の状態３６５は、ダイナミックシェル３１３のコードセットを、象徴的に相関している図形、サイズ、および位置とともに表している。これらの図形の種々の構成は、セキュリティ情報収集およびセキュリティ反応の種々の構成を示している。ＡＳＴ１７は、誤りであったり、正しい応答（たとえば、このファイルはウイルスなので検疫する）であったりする、現在の状態３６５のありうる応答を提供する。攻撃ベクトル３７０（すべて点線で描かれた矢印）は、サイバーセキュリティの脅威の象徴的な実証として機能する。方向、サイズ、および色はすべて、攻撃ベクトル、マルウェアのサイズ、マルウェアの種類のような、仮定のセキュリティプロパティに関連している。攻撃ベクトルは、コードセットのセキュリティ応答を表すために、そのコードセットに象徴的に「ぶつかる」。Ｒｅｆ．Ａ３６７は、攻撃ベクトルを通過させる特定のセキュリティ構成を示しており、このセキュリティ構成は、正しいセキュリティ応答であるかもしれないし、そうでないかもしれない。Ｒｅｆ．Ｂ３６８は、正しいかもしれないし間違ってもいるかもしれないが、Ｒｅｆ．Ａの代わりの応答タイプを示しているセキュリティ構成で跳ね返っている攻撃ベクトルを示している。Ｒｅｆ．Ｃ３６９は、攻撃ベクトルを元の場所に送り返すセキュリティ応答を示しており、このセキュリティ応答は、正しいセキュリティ応答であるかもしれないし、そうでないかもしれない。図５３について、正しい状態３５４は、ダイナミックシェル３１３のコードブロックから所望のセキュリティ応答を生ずる、差分変更アルゴリズム３５３のプロセスの最終結果を表している。正しい状態３５４は、ダイナミックシェル３１３の新バージョン３５５を再帰的にイテレートすること３５０によって生成される。たとえ現在の状態３６５と正しい状態３５４にわずかな差異があっても、これらの差異は結果として全く異なる攻撃ベクトル３７０の応答になり得る。Ｒｅｆ．Ａ３６７が攻撃ベクトルの通過を許す一方で、Ｒｅｆ．Ａ３７１（正しいセキュリティ応答）は、攻撃ベクトルを直角に跳ね返している。現在の状態３６５および正しい状態３５４の双方におけるＲｅｆ．Ｂへの攻撃ベクトルの応答は、そのままにされている。Ｒｅｆ．Ｃ３７３については、Ｒｅｆ．Ｃ３６９とは異なる位置にいるものの、攻撃ベクトルをやはり元のソースに送り返している。これら攻撃ベクトルのプレゼンテーションのすべては、セキュリティ脅威のロジスティクスな管理を示し、またそれに対応している。図５４は、ＡＳＴ１７により与えられた一連の攻撃である、ＡＳＴセキュリティ攻撃ベクトル３７５を示している。正しいセキュリティ応答３７６は、攻撃ベクトル３７０に関する所望のセキュリティ応答を示している。このような正しいセキュリティ応答を生成するコードセット（各図形）は、この段階ではまだ知られていないので、示されていない。図５５は、正しいダイナミックシェル応答攻撃３７８に対する劣悪なセキュリティ応答を示す、現在のダイナミックシェル応答攻撃３７７を示している。このような正しい応答３７８がロジック推論アルゴリズム（ＬＤＡ）１９７によって生成される。図５６は、ＬＤＡ１９７が正しい攻撃の応答３７８に合致するように、正しいセキュリティセットアップを推論する様子を示す。静的コア３１５はシステムフレームワーク／ガイダンス３５２および構文／目的自動プログラム能力３５１をＬＤＡ３７９に提供することで、ＬＤＡに正しい応答攻撃３７８を生成するセキュリティプログラムを構築できるようにする。ステージ３８１で、ダイナミックシェル３１３の基底バージョン３５６がＬＤＡ３７９に提供される。このようなバージョンは、低水準で効果のないセキュリティ応答を生成するセキュリティ応答プログラム３８２として表されている。このプログラム３８２は、ＬＤＡ３７９への入力として提供される。ＬＤＡは、静的コア３１５から構文／目的機能３５１を使用して、誤ったセキュリティ応答プログラム３８２から構築し、正しい応答攻撃３７８に適合するようにする。よって

、正しいセキュリティ応答プログラム３８３が生成され、ダイナミックシェル３１３の新バージョンと見做される。イテレーションコア３４７の再帰的イテレーション３５０を経由するプロセスは、ＡＳＴ１７によって使用可能になったセキュリティ情報のすべてで一杯になるまで、ダイナミックシェル３１３のセキュリティ能力を継続的に更新する。図５７は、ＡＳＴ１７がセキュリティ上の既知の欠陥３６４を正しいセキュリティ応答３８４と共に提供するときの、このプロセスの単純化された概要を示している。ＡＳＴ１７は、セキュリティ上の既知の欠陥３６４および応答３８４を提供可能であるが、このような正しい応答３８４を生成する有効で動くプログラムを構築することはできない。したがって、ＬＤＡ３７９は、ダイナミックシェル３１３の過去（基底）のバージョン３５６を使用して、正しいセキュリティ応答プログラム３８５として知られる、優秀で十分な設備が整っているダイナミックシェルのバージョン３５５を生成する。「プログラム」という言葉の使用は、ダイナミックシェル３１３内で動作する多くの異なる機能およびサブモジュールの全体的な機能を表している。

【０１１１】

図５８は、仮想難読化の概要を示している。以下の仮想難読化よび模擬データ生成の能力は、暗号化されたクラウドプラットフォームに展開され、サイバーセキュリティの従業員が皆無かそれに近い中小企業で使用されることになる。このセキュリティシステムはまた、大企業のデータセンターに直接インストールされる。このケースシナリオにおいて、マルウェア３８５はインターネット３０４から来て業界標準のファイアウォール／侵入検知システム／ウイルス対策をなどバイパスする。セキュリティイテレーションのこの段階では、このコードブロック３８５の意図／目的についてのＬＩＺＡＲＤ１６の査定の確信度は低い。これらの状況は、最悪のケースシナリオと想定される。無害なプロセスが、使用する資格を有する非常に重要なデータの使用を拒まれるリスクを緩和するため、そして、悪意のあるコードが機密データを有することを許してしまうリスクを回避するため、疑問の余地のあるコード３８５が密かに、データの半分が模擬（偽の）データと知的に混合されている環境に割り当てられる。実システム３８８は、典型的な管理アクセス要件を除いて実データ３８９に無制限であることを表している。実システム３８８内で稼働しているどの対象も、仮想的隔離３９０により、部分模擬データ環境３９１または完全模擬データ環境３９４に容易かつ秘密裏に転送される。実データ同期部３８６は、混合環境に与えられるデータを、どの優先順位で与えるのかを知的に選択している、２つのレイヤのうちの一つである（もう一つはデータマネージャ４０１である）。このようにして、極秘情報は疑われるマルウェアからはアクセスできず、周知で信用できることが確立されたコードだけに利用可能となる。模擬データジェネレータ３８７は、偽造かつ無用なデータを作成するためのテンプレートとして、実データ同期部３８６を使用している。データ型、データフォーマット、データ密度、データ詳細などの属性が、実データ３８９から模倣され、システム全体にうまく統合されたように見える、本物に見えるデータを有するデータベース（不適切で奇異なデータがない）が生成される。到来する外来コードの認知におけるリスクの確信度の認知は、ＬＩＺＡＲＤ１６が選ぶ難読化のレベルに影響する。コードが悪意のあるということにおける確信度が高い場合は、多量の模擬データを含む環境が割り当てられる。コードが悪意のあるということにおける確信度が低い場合は、実システム３８８（疑わしきは罰せずと考慮されている）あるいは１００％模擬データの環境３９４（デフォルトで信用できないと考慮されている）のどちらかが割り当てられる。セキュリティ挙動におけるこのようなカスタマイズの選択肢は、セキュリティポリシー３４０で定義される。これは、内側コア３４０のサブセットであるシステムの目標３３６のサブセットである。高度にモニターされたネットワークインタフェース３９２が、模擬データ３９３を含む環境で使用される。このような安全なインタフェースを使用することにより、仮想的隔離３９０と連動して、模擬データを含む環境が実システム３８８のような制限された環境にリークすることから保護している。このような隔離３９０は、仮想化技術を使用することで、ランダムアクセスメモリー（ＲＡＭ）およびＣＰＵスレッドを完全に分離し混合することから保護し、それぞれの環境をそれ自体として隔離している。

【０１１２】
図５９～図６１は、仮想難読化の監視と応答の側面を示している。このようなシステムは、マルウェアの挙動に応じてマルウェア３８５を監視および管理する。ＬＩＺＡＲＤは、初めは、現在の洗練されたイテレーションレベルで、マルウェアであるかもしれないしそうでないかもしれないコードブロックを認識する。マルウェアでない場合、ＬＩＺＡＲＤはこのコードブロックを５０％模擬データ３９１で構成される実システムの仮想クローンにプッシュする。このことは、マルウェアではないと判明した場合に、システムおよび企業の機能が厳しく妨げられないように行われる（たとえば、誤った社会保障番号が提供されるなど）。図示の例において、コードブロックは実際にはマルウェア３８５であるが、この段階では、この脅威およびエクスプロイトの方法が新規で未知の性質を有しているため、ＬＩＺＡＲＤはまだ確信ができていない。図６０は、ＬＩＺＡＲＤがマルウェア３８５をマルウェアであるかどうかまだ確信できていないことから、マルウェア３８５が仮想的に隔離された３８０模擬データ環境３９１に沈められる様子を具体的に示している。データマネージャ４０１は、実際のデータと模擬データとを知的に混合し、極秘データを露出させないようにする。データマネージャ４０１は、マルウェア３８５によって生成された情報を模擬データストレージ４００にアップロード４０２し、以前に格納された模擬データをダウンロード３９８して実データ３９７と融合させる。このようにして、マルウェアは実データストレージ３９７への書き込みアクセス権を持たず、機密情報を上書きできない。マルウェア３８５は仮想的に隔離されている３８０ので、データマネージャ４０１にのみさらされている。この仮想的隔離によって、マルウェアにはデータマネージャ４０１をバイパスして実データ３９７のすべてにアクセスすることが禁止される。挙動分析４０３は、修正処置の候補を決定するために疑わしいコードブロックのダウンロード３９８およびアップロード４０２の挙動を追跡する。挙動分析４０３は、ＬＩＺＡＲＤの元々の疑惑を確認または否定することに役立つよう、マルウェア３８５がありのままの姿でどのように動作しているかを監視する。マルウェアの動作を監視することで、ＬＩＺＡＲＤは、その外来コードが確かにマルウェアであるという当初の疑惑を確認する。マルウェア３８５は、秘密輸送モジュール３９５を介して、何も知らされずに慎重に１００％模擬データ仮想環境３９４に転送される。マルウェアがすでに増殖していて、５０％模擬データ環境３９１で感染を実行している場合の用心に、仮想環境全体が予防措置として安全に破壊（マルウェアを含めて）されている。この段階では、マルウェア３８５は今や機密情報に触れることなく模擬環境３９４に完全に沈められる。ダイナミックシェル３１３の将来可能なバージョンを改善するために、秘密の通信チャネルを介した、マルウェアとその本拠地で行われている可能性のある通信（たとえば、ハートビート信号）は監視される。このようなマルウェアの挙動情報は、データ返送中継（ＤＲＲ）３１７を介してＡＳＴ１７に転送され、将来のバージョンの役に立つ。このようにして、ＤＳ３１３は、類似のマルウェア３８５をやむなく５０％模擬データ環境（盗まれている正当なデータに関するリスクを依然として含んでいる）に再度配置するのではなく、類似のマルウェア３８５に関するより確信のある決定をすることができる。

【０１１３】
図６２および図６３は、データリコール追跡３９９が、疑わしいエンティティ４１５からアップロードされた情報と、疑わしいエンティティ４１５にダウンロードされた情報のすべてを追跡することを示す。これは、機密情報がマルウェアに転送される可能性があるというセキュリティリスクを軽減するために行われる。このセキュリティチェックは、正当な企業プロセスが模擬データ４００を受信するというロジスティックな問題も緩和する。模擬データが正当な（であると現時点ではわかっている）企業エンティティに送信された場合、すべての模擬データを呼び戻す「コールバック」が実行され、（元々リクエストされた）実データが、代わりに送信される。コールバックトリガーは、正当な企業エンティティが、データが偽ではないと確認されるまで、特定の情報に対する操作を差し控えるように実装されている。実データが仮想的混在環境内のマルウェアに転送された場合、内部のマルウェア３８５によって環境コンテナ全体が安全に処分される。環境コンテナが破壊

される前にこのマルウェアが所有していたことがわかっているデータに関する異常な活動については、アラートがシステム全体に発せられる。このコンセプトは、システム全体にわたる監視４０５で顕在化する。部分的な実データを受信したエンティティが（挙動パターンの分析で）マルウェアであると判明した場合、仮想環境（マルウェアを含む）は安全に処分され、タグ付き実データの異常な活動について企業全体のネットワークが監視される。このようにして、情報リークの可能性が防止される。模擬データのダウンロード４０７とアップロード４０８の追跡では、仮想コンテナ内の疑わしいエンティティ４１５との間で送信された模擬データが追跡される。アップロード安全度の通知４１０では、最初にセーフガードとして模擬データコレクション４００に書き込まれたデータは後で安全と見做され、疑わしいエンティティ４１５のアップロード４０２要求を充足するために実データ４１２に書き込む準備が整う。その後、アップロード中継４１１は、そのようにマークされた安全な情報を実データ４１２に渡す。正当な企業エンティティ（マルウェアではない）が模擬データ４００を受信した場合、企業エンティティは、模擬データ存在の程度を通知４１３される。実データ４１２は、模擬データを正確に置き換えるためにアップロードされる。データリコールトリガ４１４は、混合データ環境が活性化されたかもしれないことを示す、隠れた信号の有無をチェックする、正当なエンティティ（そして不注意にも、正当であると見せかけようとする悪意のあるエンティティ）上で実行されるソフトウェアのインストールである。データマネージャ４０１は、擬似データ４００（もしあれば）と混合すべき実データ４１２（もしあれば）の比率を計算する、エンティティ４１５とデータとの間の中間者インタフェースである。情報ストリームのアップロード４０２およびダウンロード３９８では、データリコールトリガ４１４がデータの逆戻りを考慮するために、個々のパケット／ファイルがマークされる（必要な場合）。

【０１１４】

図６４および図６５は、データリコールトリガ４１４の内部動作原理を示している。挙動分析４０３は、修正処置４１９の候補を決定するために、疑わしいエンティティ４１５のダウンロードおよびアップロードの挙動を追跡する。実システム４１７は、仮想環境の完全な外部に存在し、すべての考えられる機密データを含む、オリジナルの実データ４１２を含む。模擬データ４１８を置き換える実データは、実データが（実データ同期部３８６の前であっても）フィルタリングされずにデータリコール追跡３９９に提供される場所である。このようにして、実データパッチ４１６を作成して、模擬データを以前の疑わしいエンティティ４２２上の実データと置き換えることができる。仮想的に隔離された環境４０４に沈められているデータマネージャ４０１は、データリコール追跡３９９から実データパッチ４１６を受け取る。このパッチ４１６は、（今は無害であるとわかっている）以前の疑わしいエンティティ４２２を、正しく、本物で、正確な情報状態に変換するための置換命令を含んでいる。このようなパッチ４１６は、データリコールインターフェース４２７に転送され、その後、以前の疑わしいエンティティ４２２に転送される。ダウンロードデータ４２０は、企業が模擬データ環境４０４内でダウンロードしたデータである（よって、このデータは部分的または完全に偽である）。修復されたデータ４２１は、実データパッチ４１６が適用された後、模擬データが対応する実データと置き換えられた場所である。無害コード４０９が挙動分析４０３によって悪意を持っていると明らかにされると、修正処置４１９が実行される。そのようなアクション４１９は、以前の疑わしいエンティティ４２２の模擬データを、それが表す実データ４１２に置き換えることである。シークレットトークン４２４は、ＬＩＺＡＲＤによって生成され割り当てられるセキュリティ文字列である。シークレットトークン４２４は、疑わしいエンティティ４１５が正当で無害であることを仮想難読化システムに証明しない。その代わりに、本当に無害であるこのエンティティにその仕事を進めないようにする。なぜなら、このエンティティが部分的模擬データ環境３９１または完全模擬データ環境３９４の影響下にあることを知っているからである。このエンティティが正当なものである限り、偽の情報に基づいて活動し、現実世界の問題につながる従業員／ソフトウェアのなどロジスティックな問題（誤ったアドレス送信、誤った従業員の解雇など）はないはずである、データリコールトリガ４１４は、

正当な企業の機能およびエンティティにのみ存在する。デフォルトでは、正当なエンティティは、トークン４２４の存在について、組み込みサーバ環境４０４の合意済みの場所をチェックする。トークンが見当たらない場合４２９と４２５、これは、この正当なエンティティが間違って部分的模擬データ環境に配置されている可能性が高いシナリオを示している（それがマルウェアであるというリスク評価のため）。その後、遅延インタフェース４２６を有する遅延セッション４２８が起動される。トークンが見つかった場合４２６および４２４、これはサーバ環境が本物であることを示しており、したがって遅延セッションは無効化４２７される。遅延インタフェース４２６は、エンティティに直接プレインストールされたモジュールである。エンティティが模擬環境４０４にいることが示されると、遅延セッションが有効化される。遅延セッションは、このエンティティの処理を人為的に遅らせることで、挙動分析４０３にこのエンティティが無害か悪意かを判断するための時間を与えることを意味する。実際には、このような遅延は１つのアクションにつき数秒かかることが予想される。シークレットトークンは、マルウェアが存在することがほとんどない１００％実データシステムに秘密裏に埋め込まれているだけなので、実際のマルウェアにとっては、シークレットトークン（それ自体は常に変更と再生できる）のコピーを得ることは極めて困難である。シークレットトークンが見つからない場合のケースシナリオでは、遅延インタフェース４２６が関与する。これは、挙動分析４０３によって実データアクセスが再認可されるまで、エンティティが我慢強く振る舞うことを意味する。

【０１１５】

図６６は、極秘データを遮断し、実データと模擬データとを混合する、データ選択を示す。実データ４１２は、極秘データ４３１を遮断する実データ同期部３８６に提供される。フィルタの範囲は、静的コア３１５で定義されているシステムポリシー４３０によって異なる。このモジュール４３１は、機密情報が、疑わしいエンティティ４１５が存在する同一の仮想環境に決して到達しないことを保証している。データは、仮想環境４０４の生成４３４のときに一度選別される。生成４３３のための判断基準では、選別された実データは、どのような種類でどれだけの量の模擬データを生成すべきかの判断基準として使用される。模擬データジェネレータ３８７は、実データと区別できないように設計された偽データを作成する。たとえば、ひとまとまりの社会保障番号である。互換性の実施４３２により、生成された模擬データは実データとの互換性があることが確認され、重複があまりなく、欠落したデータ型の場所がないことが保証される。実データと偽データの両方の収集が、いかなる疑いも持たずにシームレスにマージできる。たとえば、偽の社会保障番号と本物の社会保障番号は重複しない（重複を避ける）。仮想環境ジェネレータ４３４は、模擬データの比率、利用可能なシステム機能、ネットワーク通信オプション、ストレージオプションなどの変数を含む、仮想環境４０４の構築を管理する。データ判断基準４３５は、実データと模擬（偽）データとの比率を調整するための変数である。マージされたデータ４３８では、データはデータ判断基準４３５にしたがってマージされる。マージ処理中に、機密度が低いとマークされた実データは、機密度が高いという印象を与える模擬データとマージされる。比率管理４３７は、所望の模擬データ比率に従うように、マージされる実データおよび模擬データの量を絶えず調整する。データは、疑わしいエンティティ４１５のデータリクエスト４４０にしたがってリアルタイムでマージされる。データは、リクエストされたデータ４３９に適切な模擬データ比で返される。

【０１１６】

図６７および図６８は、挙動分析の内部動作原理を示している。目標マップ４４１は、企業システム全体に目標を与えるシステムの目的の階層構造である。このような目標は、小規模なネットワーク、ＣＰＵ処理、およびストレージイベントの粒度に対してさえも割り当てられる。宣言された目標、活動の目標、およびコードベースの目標は、疑わしい実体４１５が行っていることが何であれ、本来のシステムの要求と比較される。活動監視４５３では、疑わしいエンティティのストレージ、ＣＰＵ処理、およびネットワーク活動が監視される。構文モジュール３５は、所望の機能に関してこのような活動４４３を解釈する。このような機能は、その後、目標モジュール３６による挙動において意図された目標に

変換される。たとえば、コードベースの目標４４６は、年間所得レポートを提出することだが、活動の目標４４７は、「給与が上位にある従業員の社会保障番号をすべて集める」かもしれない。この方法論は空港の税関部門に類似している。税関では特定の物品を申告しなければならないが、税関ではそれにもかかわらずバッグを検索する。コードベース４４２は、疑わしいエンティティ４１５のソースコード／プログラミング構造である。コンパイルされたクローズドソースプログラムであるためにソースコードを開示しないエンティティは、システムポリシー４３０によって、システムにアクセスすることをブロックすることができる。そのようなコードベース４４２は、挙動分析４０３のサブセットである構文モジュール３５に転送される。構文モジュール３５は、コーディングの構文を理解し、プログラミングコードおよびコードの活動を中間機能連携マップ４４４に還元することができる。

このような機能４４４は、コードベース４４２および活動４４３の機能を表し、不審なエンティティ４１５の認識された「意図」を生成する目標モジュール３６に転送される。目標モジュール３６は、コードベースの目標４４６および活動の目標４４７の出力を生成する。コードベース目的４４６には、ＬＩＺＡＲＤの構文的プログラミング能力によって引き出された、エンティティ４１５の既知の目的、機能、管轄範囲および権限が含まれている。活動の目標４４７には、ＬＩＺＡＲＤのストレージ、処理およびネットワーク活動の理解によって読み解かれた、エンティティ４１５の既知の目標、機能、管轄範囲および権限が含まれている。宣言された目標は、エンティティ自体によって宣言された、エンティティ４１５の想定される目的、機能、管轄範囲および権限である。要求された目標４４５には、エンタープライズシステムが必要とする期待される目的、機能、管轄範囲および権限が含まれている。これは、会社の要求を満たすために従業員を雇うことと似ている。これにより、ＬＩＺＡＲＤは、疑わしいエンティティ４１５に能力および／またはサービスがシステムによって必ずしも必要とされていない場合に、疑わしいエンティティ４１５をブロックすることができる。４つの目標４４５～４４８のすべてを、比較モジュール４４９において比較して、システムの目的３３６に対して良い結果をもたらすことにおいて、企業システム内でのエンティティ４１５の存在および挙動が合理的でＬＩＺＡＲＤによって理解されることを保証する。４つの目的４４５～４４８の間に不一致があれば、目標の相違４５０のシナリオが呼び出され、修正処置４１９につながる。修正処置は、潜在的に、疑わしいエンティティ４１５をマルウェア３８５または無害４０９としてマークすることができる。保証処置は、仮想コンテナを安全に処分したり、あるいは、実データ（模擬データのみ）や実際の企業ネットワークへアクセスしたりすることなく、マルウェア３８５を新しい仮想環境に慎重に移動することができる。

クリティカルシンキング・メモリ・パーセプション（ＣＴＭＰ）

【０１１７】

図６９は、ＣＴＭＰ２２のメインロジックを示している。ＣＴＭＰの第一の目標は、サードパーティによる意思決定を批判することである。ＣＴＭＰ２２は、複数のソース（たとえば、I^2ＧＥ、ＬＩＺＡＲＤ、信用プラットフォームなど）からの情報を相互参照し、パーセプションの期待と現実について学習する。ＣＴＭＰは、ある事柄についての客観的決定事項を形成する能力を見積り、低い内部確信度でなされた決定を表明することは差し控える。グローバルに展開されたエージェントや、信用プラットフォームからの情報など、到来するデータストリームはすべて処置可能なデータに変換される。主観的意見決定４５４は、選択パターンマッチングアルゴリズム（ＳＰＭＡ）５２６と呼ばれる入力アルゴリズムによって与えられるオリジナルの主観的決定を示している。ＳＰＭＡは通常、セキュリティ関連の保護システムであるが、辞書的客観性探索（ＬＯＭ）（推論アルゴリズム）や永続的慈善活動の方法（ＭＰＧ）（税法解釈アルゴリズムなど）の他のタイプのシステムを制限するものではない。入力システムメタデータ４５５は、ＳＰＭＡ５２６から与えられた、このアルゴリズムのメカニカルプロセスおよびそのような決定に至った経緯を記述している未処理メタデータを示している。事由処理４５６は、プロパティの属性を比較することにより行われる表明を論理的に理解するものである。事由処理のサブセットで

あるルール処理４５７では、導き出された結果ルールが、当面の問題のスコープを決定するための参照点として利用される。クリティカルルールスコープエクステンダー（ＣＲＳＥ）４５８は、パーセプションのクリティカルシンキングスコープを含むよう、パーセプションの既知のスコープを拡張する。妥当ルール４５９は、パーセプションのクリティカルシンキングスコープを利用することにより導き出された妥当ルールを示している。メモリウェブ４６０では、充足可能なルールを求めて、市場変数（市場実績３０および収益履歴３１）のログがスキャンされる。適用可能で充足可能なあらゆるルールが、投資割付を上書きする決定を生成するために実行される。ルール実行（ＲＥ）４６１では、メモリが乱雑フィールド６１３をスキャンすることにより、存在して充足可能であると確認されたルールが、該当する所望のクリティカルシンキング決定を生成するために実行される。このような規則を実行することで、必然的に明白な結果につながる。無秩序的に複雑なプロセスは、一貫性はないが生産性の高い結果につながり得る一方、ＲＥ４６１の論理的に複雑なプロセスは、一貫性のあるルールセットに依存する、常に同じ推測結果を導く。クリティカル決定出力４６２は、パーセプション観察者エミュレータ（ＰＯＥ）４７５およびルール実行（ＲＥ）４６１の双方が至った結論を比較することにより、ＣＴＭＰの出力全体を決定するための最終ロジックである。クリティカル決定４６３は、極力客観的であることを目指す事項についての意見である、最終決定である。ログ４６４は、入力アルゴリズム（ＭＰＧ）の主観的意見からの影響またはバイアスが一切ないクリティカル決定を独立して行うために使われる未処理情報である。未処理パーセプション生成（ＲＰ２）４６５は、ＳＰＭＡ５２６からメタデータログを受け取るモジュールである。そのようなログはパースされ、そのようなアルゴリズムのパーセプションを表すパーセプションが形成される。パーセプションは、複合パーセプションフォーマット（ＰＣＦ）に格納され、パーセプション観察者エミュレータ（ＰＯＥ）４７５によってエミュレートされる。適用済パーセプション観点４６６は、ＳＰＭＡ５２６によって既に適用され利用されたパーセプション視点を示している。自動化パーセプション発見メカニズム（ＡＰＤＭ）４６７は、パーセプションのスコープを拡張できるように混成パーセプション（適用済パーセプションの視点４６６によって与えられる入力にしたがって形成される）を生成する創作モジュール１８を活用するモジュールを示している。参照符号４６８は、コンピュータシステムが利用可能なパーセプションのスコープ全体を示している。クリティカルシンキング４６９は、ルールベースの思考の外殻範囲を示している。これにより、ＳＰＭＡ５２６にしたがって確立されたルールだけでなく、ＣＴＭＰ内から導出された新たな妥当ルール４５９をも明示する、ルール実行（ＲＥ）４６１に帰結する。

【０１１８】

図７０の自己批判的知識密度４７４を参照すると、これは、ＳＰＭＡ５２６が知っている技術知識を表す、入力未処理ログである。このモジュール４７４は、報告可能なログの限界を越えた、未知である可能性がある知識のスコープおよび型を推定する。このようにして、この結果生じるＣＴＭＰのクリティカルシンキング的な特徴によって、システムが直接知っている、または知らない、関与する知識のすべての可能なスコープを広げることができる。パーセプション観察者エミュレータ（ＰＯＥ）４７５は、観察者のエミュレーションを生成し、パーセプションポイントの候補すべてを、このような様々な観察者エミュレーションを使用してテスト／比較する。この入力は、そのパーセプションポイントの候補のすべてと、拡張データログである。出力は、このような拡張ログから、このような選択されたパーセプションの組み合わせと、最良で、最も該当する、最も注意深い観察者によって生成される、結果としてのセキュリティ上の判断である。意味付けの導出（ＩＤ）４７７を参照すると、このモジュールは、現時点で適用されたパーセプションの視点から意味付けされうる、パーセプションの視点のデータを導出する。上書き修正処置４７６を参照すると、これは、パーセプション観察者エミュレータ（ＰＯＥ）４７５により生成された、修正処置／表明への最終的な批判である。

【０１１９】

図７１は、ＣＴＭＰの依存構造を示している。リソース管理および割付（ＲＭＡ）４１９

を参照すると、調整可能ポリシーは、観察者エミュレーションを実行するために活用されるパーセプションの数を定める。選ばれたパーセプションの優先順位が、重み付けの降順で選択される。そして調整可能ポリシーは、パーセンテージ、固定値、あるいは、より複雑な選択アルゴリズムではなく、切り捨てを選択する方法を定めることができる。ストレージ検索（ＳＳ）４８０を参照すると、データ拡張ログから導出されたＣＶＦ（比較可能可変フォーマット）が、パーセプションストレージ（ＰＳ）４７８のデータベース検索における判定基準として使用される。メトリック処理（ＭＰ）４８９は、選択パターンマッチングアルゴリズム（ＳＰＭＡ）５２６の投資割付からの変数をリバースエンジニアリングし、このアルゴリズムの知性から、パーセプションを「救い出す」。パーセプション推論（ＰＤ）４９０は、この投資割付の回答の一部と、それに対応するシステムメタデータを使用して、この投資割付の回答の元のパーセプションを再現する。クリティカル決定出力（ＣＤＯ）４６２は、ＣＴＭＰ出力を決定するための最終ロジックを示している。メタデータカテゴリ化モジュール（ＭＣＭ）４８８を参照すると、従来の構文ベースの情報カテゴリ化によって、デバッグおよびアルゴリズム追跡が、個別のカテゴリに分割される。そして、このようなカテゴリは、市場／税法上のリスクおよび機会と相関関係を有する、個別の投資割付応答をまとめ上げて生成するために使用することができる。システムメタデータ分割（ＳＭＳ）４８７を参照すると、入力システムメタデータ４５５が、意味のある投資割付上の因果関係に分割される。データ入力ロジック４８３を参照すると、これは、すべての投資割付を、該当する市場／税法上のリスク、機会、およびそれらの対応する応答とともに、包括的に仕分けるものである。対象ナビゲータ４８１は、すべての適用可能な対象をスクロールする。対象データ投入部４８２は、その対象と関係のある、適切な投資リスクと割付を抽出する。それらに該当する重み付けに加え、パーセプションストレージ（ＰＳ）４７８のパーセプションが、そのインデックスとしての比較可能可変フォーマット（ＣＶＦ）とともに格納される。このことは、入力クエリ検索としてＣＶＦを受け取れるようにデータベースが最適化され、そして検索の結果は、パーセプションの取り合わせであることを意味している。

【０１２０】

図７２を参照すると、意味付けの導出（ＩＤ）４７７が、現時点で既知のパーセプションの視点から意味付けされうる、データのパーセプションの視点を導出する。自己批判的知識密度（ＳＣＫＤ）４９２を参照すると、入力された未処理ログが、既知の知識を表している。このモジュールは、報告可能なログの限界を越えた、未知である可能性がある知識のスコープおよび型を推定する。このようにして、この結果生じるＣＴＭＰのクリティカルシンキング的な特徴によって、システムが直接知っている、または知らない、関与する知識のすべての可能なスコープを広げることができる。メトリック合成４９３では、パーセプションの視点がメトリックのカテゴリに分割される。メトリック変換４９４では、個々のメトリックがパーセプションの視点全体に戻される。メトリック拡張（ＭＥ）４９５では、多数のさまざまなパーセプションの視点のメトリックが、個々のデータベースに、カテゴリ別に格納される。メトリックの上限は、それぞれのメトリックＤＢのピーク知識によって表される。メトリックは、増強され複雑性が高められると、戻されてパーセプションの視点に変換され、クリティカルシンキングのために活用される。比較可能可変フォーマットジェネレータ（ＣＶＦＧ）４９１では、情報ストリームが、比較可能可変フォーマット（ＣＶＦ）に変換される。

【０１２１】

図７３は、ＣＴＭＰの依存構造を示している。クリティカルルールスコープエクステンダー（ＣＲＳＥ）４５８では、ルールセットのクリティカルシンキングスコープを拡張するために、既知のパーセプションが活用される。パーセプションマッチング５０３では、ルール構文導出（ＲＳＤ）５０４から受信したパーセプションから、比較可能可変フォーマット（ＣＶＦ）が形成される。新たに形成されたＣＶＦは、パーセプションストレージ（ＰＳ）４７９内で類似したインデックスを有する、該当するパーセプションを検索するために使用される。一致する候補が、ルール構文生成（ＲＳＧ）５０５に戻される。メモリ

認識（ＭＲ）５０１では、入力データから乱雑フィールド６１３が形成される。既知のコンセプトを認識するために、フィールドスキャンが行われる。メモリコンセプトインデックス付け５００を参照すると、すべてのコンセプトが、個別に、インデックスとして知られる別々の部分に最適化される。これらのインデックスは、乱雑フィールド６１３と連携するために、文字スキャナにより使用される。ルール充足度パーサ（ＲＦＰ）４９８は、ルールの個々の部分を、認識のタグとともに受信する。各部分は、メモリ認識５０１によって、乱雑フィールド６１３内で見つかった、または見つからなかったとマークされ、そして、ＲＦＰは、どのルール全体、つまり、そのルールの全部分の合成が、乱雑フィールド６１３内でルール実行（ＲＥ）４６１に値するほど十分に認識されたのかを、論理的に推論することができる。ルール文法フォーマット分割（ＲＳＦＳ）４９９では、妥当ルールが分割され、型ごとにまとめられる。したがって、すべての処置、プロパティ、条件、およびオブジェクトが、別々に束ねられる。これによって、システムは、どの部分が乱雑フィールド６１３内で見つかっていて、どの部分が見つかっていないのかを判別することが可能となる。ルール構文導出５０４では、論理的な「白か黒か」ルールが、メトリックベースのパーセプションに変換される。多数のルールの複雑な配列が、さまざまな勾配の多数のメトリックにより表現される、単一で一様なパーセプションに変換される。ルール構文生成（ＲＳＧ）５０５は、パーセプション形式に格納されそのパーセプションの内部メトリック構成に関与している、以前に確認されたパーセプションを受信する。このような勾配ベースのメトリックの測定値は、元のパーセプションの入力／出力される情報のフローを列挙する、二値で論理的なルールセットに変換される。ルール文法フォーマット分割（ＲＳＦＳ）４９９の修正されたルールは、観察されているオブジェクトの現実に従うルールセットの正確な明示を表している。修正されたルールが分割され、型ごとにまとめられる。したがって、すべての処置、プロパティ、条件、およびオブジェクトが、別々に束ねられる。これによって、システムは、どの部分が乱雑フィールド６１３内で見つかっていて、どの部分が見つかっていないのかを判別することが可能となる。本質的論理的推論５０６は、論理的原則を用い、そうして誤謬を避けながら、どの種類のルールがパーセプションの範囲内でメトリックの勾配を正確に表しているかを推論する。例を挙げると、本質的論理的推論は（高周波などの）アナログサイン波を受け取りデジタル値に変換するようなものである。全体の傾向、位置、および結果は総じて同じものである。しかしながら、アナログ信号がデジタルに変換されている。メトリックコンテキスト分析５０７は、メトリックのパーセプションの範囲内で相互関係を分析する。あるメトリックは他のメトリックに様々な大小関係で依存する。この文脈化は、「デジタル」ルールセット形式の範囲内でルールが有するミラー化された相互関係を補足するために使用される。入力／出力分析５０８は、パーセプション（灰色）またはルール（白黒）それぞれの入力および出力の差分分析を行う。このモジュールの目的は、パーセプションまたはルールの入力および出力が変換（灰色から白黒、またはその逆）の後でも極力同様または同一であることを保証することである。判断基準計算５０９は、入力ルールの判断基準およびタスクを算出する。これは、ルールセットの背後にある「動機」であると解釈することができる。ルールは理由があって実装されるもので、その理由は示唆あるいは明確な定義によって理解される。したがって、「デジタル」なルールが実装された、意味付けられた理由を計算することによって、その同じ理由を、同様の入力／出力能力を求めるパーセプションの範囲内でメトリックの編成を正当化するために使うことができる。ルール形成分析５１０は、ルールの構成／編成全体、およびそれらがどのように相互作用しているかを分析する。ルール形成分析は、「アナログ」のパーセプションの範囲内でメトリックが有するルールセット形式の範囲内でルールが有するミラー化された相互関係を補足するために使用される。ルール構文形式変換（ＲＳＦＣ）５１１では、ルール構文形式（ＲＳＦ）５３８の構文に従うように、ルールが仕訳けられ、分割される。

【０１２２】

図７４は、ＣＴＭＰにおける知的情報を処理するための最終ロジックを示している。最終ロジックは、直感的／認知的モードおよび思考的／論理的モード（パーセプション観察者

エミュレータ（ＰＯＥ）４７５およびルール実行（ＲＥ）４６１に対応する）の双方から知的情報を受け取る。決定事項直接比較（ＤＤＣ）５１２では、直感的および思考的モード双方の決定事項が比較され、裏付けが確かめられる。主な相違点は、いかなるメタ・メタデータも比較されていないことであり、その理由は、いかなる形であれ両者が等しく一致する場合、メタ・メタデータはそれが何故かを理解するには余分なものだからである。最終出力制御（ＴＯＣ）５１３は、直感的モード５１４および思考的モード５１５双方の間のＣＴＭＰ出力を決定するための最後のロジックである。直感的決定５１４は、パーセプションを活用することを通じてクリティカルシンキングに携わる、ＣＴＭＰの２つの主要なセクションの一方である。パーセプション観察者エミュレータ（ＰＯＥ）４７５を参照。思考的決定５１５は、ルールを活用することを通じてクリティカルシンキングに携わる、ＣＴＭＰの２つの主要なセクションの他方である。ルール実行（ＲＥ）４６１を参照。パーセプション５１６は、内部形式５１８で定義された形式構文にしたがって、直感的決定１５８から受信したデータである。充足ルール５１７は、思考的決定５１５から受信したデータで、ルール実行（ＲＥ）４６１からの適用可能（充足可能）なルールセットの集合である。このようなデータが、内部形式５１８で定義されている形式構文に則って渡される。内部形式５１８を使用することで、両方の入力がＣＴＭＰ内部で使用される既知で一貫性のある形式で規格化されているとき、メタデータカテゴリ化モジュール（ＭＣＭ）４８８が、その入力の構文を認識可能である。

【０１２３】

図７５は、直感的／認知的および思考的／論理的の２つの主要な入力がＣＴＭＰ全体を表している単一の最終出力に同化していくことを示している。クリティカル決定＋メタ・メタデータ５２１は、内部形式５１８に定義された構文にしたがってパーセプション５１６と充足ルール５１７のいずれかを搬送するデジタルキャリアである。

【０１２４】

図７６は、オリジナルの選択パターンマッチングアルゴリズム（ＳＰＭＡ）５２６で行われる、知的思考のスコープを示している。入力変数５２４は、事由処理およびルール処理のために考慮されている初期の金融／税割付変数である。ＣＴＭＰは、入力変数を評価し、人工知能によるセカンドオピニオンとなろうと考えている。変数入力５２５は、セキュリティ上の決定を定義する入力変数を受信する。このような変数は、ＣＴＭＰが合理的な修正処置が何かを見分けるための判断基準を提供している。変数に加算、減算、もしくは変更がある場合、適切な変更が結果の修正処置に反映されなければならない。ＣＴＭＰのきわめて重要な目的は、入力変数の変化を正しく正確に反映する修正処置の、妥当で重要な変更を見分けることである。選択パターンマッチングアルゴリズム（ＳＰＭＡ）５２６、選択パターンマッチングアルゴリズムは、自身の判断基準にしたがって、最も適切な処置を見分けようとする。得られた出力形状５２７は、初期入力変数１６８を有するＳＰＭＡ５２６によって生成された結果である。ＳＰＭＡ１７０５２６の意思決定によって導出されたこのルールは「現行ルール」と見なされるが、必ずしも「妥当ルール」ではない。属性マージ５２８は、ＳＰＭＡ５２６から提供されたログ情報にしたがって、ＳＰＭＡ５２６による現時点での知識スコープを用いて事由処理４５６が行うものである。

【０１２５】

図７７は、パーセプションおよびルールを介してＣＴＭＰにより実行されるクリティカルシンキングアルゴリズムと並置される、従来のＳＰＭＡ５２６を示している。正しく理解されなかった処置５３１、これは選択パターンマッチングアルゴリズム（ＳＰＭＡ）５２６が完全に正確な修正処置を提供できなかったものである。この理由は、元々のＳＰＭＡ５２６のプログラミングまたはデータにおいて調べられていない、根底にある基本的な仮定のためである。この例では、入力変数として三次元オブジェクトを使用すること、および正しく適切な処置は、ＳＰＭＡ５２６が説明していない次元／ベクトルがあったことを示している。適切な処置５３２では、クリティカルシンキングが三番目の次元を考慮する。三番目の次元は、ＳＰＭＡ５２６がチェックのためのベクトルとして省略したものである。実行されたすべての追加パーセプションの視点をチェックするため、クリティカルシ

ンキング４６９によって三番目の次元が考慮される。妥当ルール５３３を参照すると、クリティカルルールスコープエクステンダー（ＣＲＳＥ）は、以前は考慮されなかったパーセプションの視点（たとえば、三番目の次元）を活用することにより、ルールセットの把握のスコープを拡張する。現行ルール５３４を参照すると、現時点での修正処置決定事項の派生ルールは、ＳＰＭＡ５２６が理解したこと、および（妥当ルールと比べて）その理解が欠落していること、を反映している。入力されたルールは選択パターンマッチングアルゴリズム（ＳＰＭＡ）５２６から導出されており、ＳＰＭＡがもたらすデフォルトの把握のスコープを記述している。このことは、金融割付の平板的なコンセプトにおける２次元しか把握していないＳＰＭＡ５２６によって示されている。

【０１２６】

図７８は、従来の現行ルールと比較して、重要な見識および／または変数を省略した妥当ルールが生成される様子を示している。乱雑フィールドパース（ＣＦＰ）５３５は、複数のログのフォーマットが、乱雑フィールド６１３として知られる、スキャン可能な単一の単位に合成される。既に確立された妥当ルール５３３を補足するために、メモリ認識（ＭＲ）５０１から追加ルール５３６が生成される。パーセプションのルール５３７を参照すると、該当しかつ定着したと見なされたパーセプションが、論理的ルールに変換されている。あるパーセプション（オリジナルのパーセプション形式）が、多くの「灰色の領域」を定義している多くの複合メトリック関係を有していた場合、「白黒」の論理的ルールはそのような「灰色の」領域を、複合度をｎ次だけ拡張することで包含する。ルール構文形式５３８は、効率的なストレージと変数の照会のために最適化されている格納フォーマットである。

【０１２７】

図７９～図８０は、パーセプションマッチング（ＰＭ）５０３のモジュールを示している。メトリック統計５３９に関して、パーセプションストレージ（ＰＳ）４７９から統計情報が与えられる。このような統計は、メトリックの定着傾向、内部メトリック関係、およびメトリックの成長率などを定義している。総合統計クエリの中には（全体メトリック定着度格付けのように）自動的に実行され格納されるものもある。それ以外の、より具体的なクエリ（メトリックＸとＹはどの程度関係があるか）は、ＰＳ４７９からリアルタイムにリクエストされる。メトリック関係保持５４０は、統合出力にプッシュできるよう、メトリック関係データを保持している。エラー管理５４１は、個々のメトリックのいずれかから生ずる構文エラーおよび／または論理的エラーをパースする。個々のメトリックは、以前は入力パーセプション５４４であった単一のユニットに合成されていたため、メトリック分割５４２は、個々のメトリックを分離する。入力パーセプション５４４は、視覚、嗅覚、触覚、聴覚からなるパーセプションの一つの構成例である。ノード比較アルゴリズム（ＮＣＡ）５４６は、２つ以上のＣＶＦのノード構成を受信する。ＣＶＦの各ノードはプロパティの大小を表している。個々のノードごとに、類似度比較が行われ、総合分散が計算される。これにより、正確な比較が効率的に計算されることが保証される。分散の数値が小さい場合は、それがノード固有であれ統合ウェイトであれ、一致度が高いことを表している。比較可能可変フォーマット（ＣＶＦ）５４７は、ＣＶＦが、パーセプションマッチング（ＰＭ）５０３への最終出力である、出力５５０として提出する様々な編成を示す視覚表現である。ノード比較アルゴリズム（ＮＣＡ）５４６において重複するノードはどれもマッチング結果として保留されるため、全体の結果はステージ５５０で提出される。

【０１２８】

図８１～図８５は、ルール構文導出／生成を示している。未処理パーセプション直感的思考（アナログ）５５１では、「アナログ」形式にしたがってパーセプションが処理される。未処理ルール論理的思考（デジタル）５５２では、デジタル形式にしたがってルールが処理される。金融割付決定事項に関係するアナログ形式５５３のパーセプションは、段差のない滑らかな曲線の勾配単位で格納されている。金融割付決定事項に関係するデジタル形式５５４の未処理ルールは、「あいまいな領域」のない目盛り単位で格納されている。

オリジナルのルール５５５は、データの内容に関して正しい規則５３３と同じある。相違点は、オリジナルのルール５５５が、ルール文法フォーマット分割（ＲＳＦＳ）４９９によって、メモリ認識５０１を介して乱雑フィールド６１３との相互参照を可能にする、より動的な形式に変換されていることである。認識されたルールセグメント５５６は、メモリ認識５０１によって認識されたオリジナルのルール５５５由来のルールである。このことは、オリジナルの妥当ルール５３３（処置、プロパティ、条件、目的など）を構成する個々のセグメントのどれが乱雑フィールド６１３で認識されたかを示し、潜在的に論理的に充足されたルールになる可能性があることを示している。セキュリティオーバーライド決定事項５５７は、修正処置が実行されることを可能にするルール実行（ＲＥ）４６１によって生成される最終結果である。このような修正処置は、クリティカル決定出力（ＣＤＯ）４６２で実行されるより大きな修正処置ロジックのサブセットである最終出力制御（ＴＯＣ）５１３にさらに提供される。未充足ルール５５８は、それらの論理的な依存性にしたがって乱雑フィールド６１３内で（ルール充足度パーサ４９８にしたがって）十分に認識されていないルールセットである。同様に、ＣＤＯ４６２によって分析された論理的な依存関係にしたがって、充足ルール５１７は乱雑フィールド６１３で十分に利用可能であると認識されている。サードパーティデータベースソリューション５５９は、バッファ、キャッシュ、ディスクストレージ、スレッド管理、メモリ管理、および他の典型的なメカニカルデータベース機能を管理するハードウェアインタフェースソフトウェアである。充足デバッガ５６０は、未充足ルールの理由を見つけようとする。その理由は、乱雑フィールド６１３が十分な内容ではなかった、あるいはそのルールセットが本質的に非論理的であるかのどちらかである。ルールセットが非論理的である場合、その理由は、ある程度の精度の範囲内で瞬時にチェックされる。しかしながら、乱雑フィールド６１３が希薄になる可能性を証明する際は、不十分な調査を行うという誤謬に陥らないために複数の調査を行う必要がある。

【０１２９】

図８６～図８７は、ルール文法フォーマット分割（ＲＳＦＳ）４９９モジュールの動作原理を示している。このモジュールでは、妥当ルール５０２が分割され、型ごとにまとめられる。したがって、すべての処置、プロパティ、条件、およびオブジェクトが、別々に束ねられる。これによって、システムは、どの部分が乱雑フィールド６１３内で見つかっていて、どの部分が見つかっていないのかを判別することが可能となる。処置５６１については、既に実行されているかもしれない処置を示す４つのルールセグメントのデータ型のうちの１つが実行され、起動のなどために考慮されている。プロパティ５６２については、何か他のものを記述する何らかのプロパティのような属性を示す４つのルールセグメントのデータ型のうちの１つであり、処置、条件、または目的である。条件５６３については、論理演算または演算子を示す４つのルールセグメントのデータ型のうちの１つ（たとえば、ｘおよびｙならばｚ、ｘまたはｚならばｙ、など）である。オブジェクト５６４については、処置５６１およびプロパティ５６２のような、それに適用される属性を有することができる標的を示す４つのルールセグメントデータタイプのうちの１つである。処理段階５６５では、それまでに収集された関係の導出の結果が出力として提出され、その後、プログラムは終了する。処理段階５６６は、一度につき１つのアイテムを、ルールセグメントを通じてイテレートする。処理段階５６７は、ルールセグメント（たとえば、処置５６１、目的５６４など）の間の個々の関係を解釈し記録する。こうして、各個別の関係が収集され、ステージ５６５で出力のために準備される。シーケンシャルスキャン５６８は、ＲＳＦ５３８の各ユニットを「［ＤＩＶＩＤＥ］」マーカで分割する。ＲＳＦ５３８からのＳＵＢＪＥＣＴ（対象）およびＧＬＵＥ（グルー）も分割され、パースされる。分割された出力５６９は、個々の対象および内部対象の関係がスキャナによって保持されるところである。それらは、ＲＳＦ５３８全体がシーケンシャルに走査されたときに出力のために一斉に送られる。分割ルールフォーマット５７０は、分割された出力５６９からの個々のルールセグメント（たとえば、処置５６１、目的５６４など）を含むための配信メカニズムである。分割ルールフォーマット５７０の使用は、情報伝達の２つの主要点にお

いて強調される。一つは、ルール文法フォーマット分割（ＲＳＦＳ）４９９（メモリ認識前段階と見なされる）からの出力として、そして、もう一つはメモリ認識（ＭＲ）５０１（メモリ認識後段階）からの出力として、である。

【０１３０】

図８８は、ルール充足度パーサ（ＲＦＰ）の動作原理を示している。ルール充足度パーサは、ルールの個々のセグメントを認識のタグとともに受信する。各セグメントは、メモリ認識（ＭＲ）５０１によって、乱雑フィールド６１３内で見つかった、または見つからなかったとマークされる。そして、ＲＦＰ４９８は、どのルール全体、つまり、そのルールの全部分の合成が、乱雑フィールド６１３内でルール実行（ＲＥ）４６１に値するほど十分に認識されたのかを、論理的に推論することができる。キュー管理（ＱＭ）５６１は、構文的関係再構築（ＳＲＲ）４９７モジュールを利用して、個々の部分を最も論理的な順序で分析する。バイナリのイエス／ノーフロー質問に答えることができ、適切な処置をとることができるように、ＱＭ５６１は、メモリ認識（ＭＲ）５０１の結果にアクセスすることができる。ＱＭは、すべてのルールセグメントを段階的にチェックし、単一のセグメントが乱雑フィールド６１３から欠落し、他のセグメントと適切な関係にない場合、ルールセットは未充足であるとフラグされる。すべてのチェック段階に合格すれば、ルールセットは充足とフラグが立てられる（５２２）。ＱＭステージ５７１は、ルールセグメント「目的Ｃ」が乱雑フィールド６１３内に見つかったかどうかをチェックする。ＱＭステージ５７２は、次の適切なセグメントがオリジナルの「目的Ｃ」に関連している一方、カオスフィールド６１３にも存在するかどうかを、メモリ認識（ＭＲ）５０１にしたがってチェックする。同様のロジックが、条件Ｂおよび処置ＡのＱＭステージ５７３および５７４にそれぞれ適用される。これらのセグメント表記（Ａ、Ｂ、Ｃなど）は、プログラムのコアロジックの一部ではないが、予想される典型的な使用法を表示する一貫した例を参照している。完全に再構築されたルールセット５７５を受信することは、このルールセットが充足可能であることがわかっていると仮定して、キュー管理５７６の充足ルールセット出力と、構文的関係再構築（ＳＲＲ）モジュール４９７によって与えられるルールセグメントの関連付けを必要とする。

【０１３１】

図８９～図９０は、未充足ルールの理由を見つけようとする充足デバッガ５６０を示している。その理由は、乱雑フィールド６１３が十分な内容ではなかった、あるいはそのルールセットが本質的に非論理的であるかのどちらかである。ルールセットが非論理的である場合、その理由は、ある程度の精度の範囲内で瞬時にチェックされる。しかしながら、乱雑フィールド６１３が希薄になる可能性を証明する、不十分な調査という誤謬を避けるために複数の調査を行う必要がある。フィールド希薄さ調査５７７は、乱雑フィールド６１３に十分に内容があるか、それともそこからルールセットの不定の構成を生じさせないかどうかを、具体的にチェックする。スキャン５７８は、乱雑フィールドの内部について、該当するルールパーツの存在の有無を確認する。調査ＤＢ５７９は、近い将来の参照のための調査結果を格納する。条件節５８０は、調査ＤＢ５７９が飽和／満杯になったかどうかをチェックする。これは、スキャンが正または負の結果をもたらすにもかかわらず、ルールパーツに対する可能なスキャンが実行されたことを意味している。すべての可能なスキャンが実行されている場合、結論５８１に結び付けられる。乱雑フィールド６１３全体の希薄さが、ルールセットが未充足と分類された理由である。すべての可能なスキャンが実行されていない場合、結論５８２に結びつけられる。すなわち、調査は不完全であり、乱雑フィールド６１３のより多くのセクタが、乱雑フィールド６１３の希薄さが、ルールが未充足となった原因であるかを確実に伝えるためにスキャンする必要がある。論理的不可能テスト５８３は、本質的に不可能な論理依存性がルールセット内に存在するか否かをチェックすることで、ルールセットが未充足と分類されるようにする。たとえば、オブジェクト５８４「独身男性」にはプロパティ５８５「結婚」が割り当てられており、これは本質的な矛盾につながる。このテスト５８３は、用語５８４および５８５の辞書的定義を決定する。内部ルール一貫性チェック５８８は、すべてのプロパティがそれらのオブジェ

クトの対応物と一致し関連しているかどうかをチェックする。ＲＳＦ５３８フォーマットの「独身男性」５８４の定義はオブジェクト５８６「男性」の部分定義に貢献し、「既婚」５８５の定義（ＲＳＦ５３８フォーマットも含む）はオブジェクト５８７の「二人」の部分定義に寄与する。チェック５８８の結論は、オブジェクト５８６「男性」がオブジェクト５８７「２人」を潜在的に包含している限り、定義５８６と５８７の両方に互換性があるということである。ルールの関連性の変換５８９では、公平な条件が変換され、比較テストが実行される。このような変換によって、第２の定義（「既婚」）は第１の定義（「独身男性」）の文脈の中で理解されることが可能になる。よって、このルールには、同じ男性が同時に現在既婚５９０でかつ現在未婚５９２であるという本質的な矛盾が含まれているという結論が導かれる。

【０１３２】

図９１は、ルール実行（ＲＥ）４６１を示しており、ルール実行では、メモリが乱雑フィールド６１３をスキャンすることにより、存在して充足可能であると確認されたルールが、該当する所望のクリティカルシンキング決定を生成するために実行される。ルールセットの変換を追跡するために使用される、市松模様の平面がある。平面上のオブジェクトは、任意のセキュリティ状況の複雑さを表しており、一方で「セキュリティの市松模様」に広がるそのようなオブジェクトの動きは、セキュリティルールセットの応答によって管理されるセキュリティ状況の進化を示す。ステージ１　５９３において、ＲＳＦ５３８の情報は、市松模様の平面上のすべての該当するオブジェクトの初期開始位置を定義し、動的に継続するセキュリティ状況の開始を定義する。これは、動的セキュリティポリシーを扱うルールの論理的な「位置」を示すため、象徴的に使用されている。ステージ２　５９４およびステージ６　５９８は、特定のセキュリティ状況の位置およびスコープを変更する、適用済みであるセキュリティルールを例示するオブジェクト変換を示している。たとえば、ステージ２および６におけるオブジェクトの変換は、暗号化批判ファイルを示すことができる。ステージ３　５９５は、市松模様上のオブジェクトの動きを示しており、セキュリティ応答戦略の一部として、機密ファイルがオフサイトの場所に実際に移動することに対応させることができる。ステージ４　５９６およびステージ５　５９７は、２つのオブジェクトを共通の第３のオブジェクトに併合するプロセスを示す。このルールの適用例は、効率的かつ安全に管理された情報の転送を容易にするために、２つの別個で隔離されたローカルエリアネットワークが統合されることである。ルール実行（ＲＥ）４６１が完了すると、妥当ルール５３３および現行ルール５３４の結果は異なる。これは、選択パターンマッチングアルゴリズム（ＳＰＭＡ）５２６から生成される批判性の低い結果ではなく、ＣＴＭＰが実行したクリティカルシンキングの利点を示している。すべての図形、色、および位置は、（実際のセキュリティオブジェクトよりは説明が簡単なため、）セキュリティ変数、発生、および応答を象徴的に表している。ＳＰＭＡは、ＣＴＭＰとは異なる最終的な形状の位置、ならびに、類似しているが異なっている（橙色対黄色）五角形の色の違いを生成している。このことは、すべての入力ログが処理のために通過する条件節ルールセット構成が複雑なために起こる。これは、様々なプレーヤー変数（高さ、力など）を用いてビリヤードの試合を開始すると、結果としてのボールの位置が全く異なる様子と似ている。ＣＴＭＰはまた、紫色の正方形を立方体に変換した。この立方体は（ＣＴＭＰの説明を通して）ＳＰＭＡ５２６や人間でさえも予想も考えもつかなかった次元やパーセプションを考慮する能力を表している。最終的なセキュリティオーバーライド決定事項５９９は、妥当ルール５３３にしたがって実行される。

【０１３３】

図９２および９３は、シーケンシャルメモリ編成を説明している。シーケンシャルメモリ編成は、アルファベットのような順番に並べられた情報の「チェーン」の読み書きにおいてより高い効率をもたらす、最適化された情報格納方法である。メモリアクセスポイント６００では、ノード６０１（ブロック）のそれぞれの幅は、記憶されたオブジェクト（ノード）への観察者の直接到達性を表している。シーケンシャルに記憶されたアルファベットの順番において、「Ａ」はこのシーケンスの最初のノードであることから最もアクセス

容易なメモリのポイントである。文字Ｅ、Ｈ、Ｌも、自身のサブシーケンス「ＥＦＧ」、「ＨＩＪＫ」、および「ＬＭＮＯＰ」の「先頭」であるため、より簡単に直接アクセスできる。到達性の範囲では、各文字は、観察者への直接メモリアクセスのポイントを表す。より広い到達性の範囲は、シーケンスノードごとにより多くの到達ポイントが存在し、かつ、その逆が真であることを示している。「順番に」のみ参照され、ランダムに選択されたノードからは参照されないシーケンス長くなるほど、到達性の範囲はより狭くなる（シーケンスサイズとの比較で）。これにより、シーケンシャル度合いの大きさに応じて、より効率的なメモリの想起が可能となる。ネストされたサブシーケンスレイヤ６０３では、強い不均一性を示すシーケンスは、相互接続している一連のより短いサブシーケンスで構成されている。アルファベットは、個々のサブシーケンス「ＡＢＣＤ」、「ＥＦＧ」、「ＨＩＪＫ」、「ＬＭＮＯＰ」はすべて、記憶されたシーケンスとして独立して存在するが、アルファベット全体を相互接続して形成している。この種類のメモリストレージおよび参照は、マスターシーケンスの特定のノードに時折または頻繁にアクセスする場合に、はるかに効率的である。このようにして、シーケンス全体の開始からスキャンすることを回避して、時間とリソースの効率を上げることができる。このことは、検索のたびに最初のページから本をスキャンするのではなく、章によって本をスキャンすることに似ている。極端に不均一な６０５スコープでは、すべてのノードにわたって一貫性のないアクセスポイントが存在する。これは、チェーンのように相互接続するネストされたサブシーケンスの重質な構成を有していることを意味する。非常に不均一なシーケンスとは、中程度にシーケンシャルであるが、複数のメモリアクセスポイント（ネストされたサブシーケンスレイヤ）を持つ必要があることを意味する。非常に不均一なシーケンス６０５の例はアルファベットであり、どの文字から始めるかによって列挙する困難さが変化する。極端に均一な６０７スコープでは、すべてのノードに一貫したアクセスポイントが存在する。これは、このスコープが、チェーンのように相互接続するネストされたサブシーケンスで構成されていないことを意味する。非常に均一なシーケンスは、それが極端にシーケンシャル（ノード全体にわたって常に一貫してアクセスポイントが皆無かそれに近い）である、または極端に非シーケンシャル（ノード全体にわたって一貫して多くのアクセスポイントがある）であることを意味する。極端に均一なスコープ６０７の例は果物の集合であり、それらを列挙する上では、特定も強調もされないシーケンスがかろうじて存在し、相互に連結されたサブシーケンスも存在しない。適度に均一な６０６スコープには最初は多くのアクセスノードが存在する。つまり、先頭からコンテンツを列挙するのに最も効率的である。しかし、メインコンテンツはさらに線形であり、これはネストされたサブシーケンス層が存在しないこと、および単一の大きなシーケンスが存在することを示している。適度に不均一な６０４スコープは、線形からはそれほど逸脱しておらず、よって全体的に一貫性のあるアクセスポイントである。これは、よりわずかでより定義の少ない、ネストされたサブシーケンスレイヤが存在すると同時に、一貫して可逆的なコレクションに準拠していることを示している。適度に不均一なスコープ６０４の動作を示す情報の一例としては、自動車製造業者のカタログが考えられる。スポーツカー、ハイブリッド、ＳＵＶのようなカテゴリが定義されている可能性があるが、別のカテゴリを指定しているにもかかわらずＳＵＶとスポーツカーを比較している可能性があるため、リストを列挙したり覚えたりする必要がない。

【０１３４】

図９４は、果実などの非シーケンシャルに関連する項目の情報ストレージを扱う非シーケンシャルメモリ編成を示している。果物のコレクションでは、どのように情報を読むべきかについて強いシーケンシャル順序を持つアルファベットとは対照的に、その順番で読むべきという高度に指定された順序はない。メモリ編成６０８は、一貫して均一なすべての果物のアクセスノードなノードを示し、非シーケンシャルな編成を表している。参照符号６０８の編成は、可逆性が、非シーケンシャルな配置と均一なスコープを示す様子を示している。この例では、果物のメモリが、ノードごとに比較的広いアクセスポイントによって示されるように、非シーケンシャルであることを示している。同様の均一性は、果物の

順序がシャッフルされるときに存在し、これは果物の可逆的な順序を示している。これに対して、アルファベットのようなシーケンシャルなシリーズは、規則的な列挙とは逆に、後ろ向きに列挙するのがはるかに難しい。一般的な果物のリストはこの現象を示さず、それがシーケンシャルリストの内部よりはより頻繁に、シーケンシャルリストの外部で参照されることを示している。核となる話題および関連性６０９では、この果実のリストにはシーケンシャル度合いがないため、同じ一連の果物が、異なる核（中心のオブジェクト）を除いて繰り返される。この核は、核となる話題が定義されていない場合とは対照的に、残りの果物がより容易にアクセスできるメモリの近隣として機能する、主たる話題を表している。ストロングネイバー６１０Ａでは、りんごが一般的な果実であるにもかかわらず、スペルが重なっているので、他の一般的な果物よりもパイナップルと強い関連性がある。したがって、それらはより多くのメモリに関連付けられていると考えられる。ウィークネイバー６１０Ｂでは、パイナップルは熱帯の果実であるため、オレンジやバナナ（一般的な果物）との関連性は低い。パイナップルは、熱帯であることが重複しているので、マンゴーとともに参照される可能性がより高くなる。グラフの点６１２は、果物のシリーズの非常に弱いシーケンシャル度合いが、ノード６０１のアクセスにおいて非常に強い均一性をもたらす様子を示している。

【０１３５】

図９５～図９７は、既知のコンセプトを認識するために乱雑フィールド６１３のスキャンが実行されるメモリ認識（ＭＲ）５０１を示している。乱雑フィールド６１３は、「ホワイトノイズ」の情報内に任意に潜んでいるコンセプトの「フィールド」である。乱雑フィールドは自発的にＣＴＭＰシステムに知らされ、「野生のもの」と考えられ、予測不能であると考えられる。メモリ認識の目的は、フィールドを効率的にスキャンして既知のコンセプトを認識することである。メモリコンセプト保持６１４では、認識可能なコンセプトが格納され、フィールド検査のためにインデックス付けおよび参照される準備が整う。この図示では、システムの理解を容易にするために、野菜の名称のスペルを簡略化した例を使用している。しかし、この例は、はるかに複雑なシナリオのアナロジーとして使用することができる。現実世界のセキュリティの例では、このことは、カメラフィードにおける、市民と兵士の認識と区別を含む。サイバーセキュリティの例では、記憶されている既知のトロイの木馬、バックドアを認識すること、およびそれらを、たくさんのセキュリティホワイトノイズ（ログ）で検出することができる。３文字スキャナ６１５では、乱雑フィールド６１３がスキャンされ、ターゲットに対応する３文字セグメントに対してチェックが行われる。たとえば、「ＰＬＡＮＴ」がターゲットであり、スキャナはフィールドに沿って３文字ずつ段階的に移動する。スキャナが進むたびに、セグメント「ＰＬＡ」、「ＬＡＮ」、および「ＡＮＴ」が、「ＰＬＡＮＴ」という単語のサブセットであるということでチェックされる。しかしながら、「ＬＡＮ」と「ＡＮＴ」という単語は、ターゲットとなることもある独立した言葉である。したがって、これら３文字セグメントの１つがフィールドに見つかった場合、それは、「ＬＡＮ」または「ＡＮＴ」の完全なターゲットが見つかったか、あるいは、「ＰＬＡＮＴ」のサブセットが見つかった可能性があることを含意している。同じ考えが、５文字スキャナ６１６に適用されるが、今度は、フィールド全体にわたってすべての進歩によってチェックされるセグメントは、単語「ＰＬＡＮＴ」全体である。「ＬＡＮ」や「ＡＮＴ」などのターゲットは省略される。これは、最低５文字のターゲットが、５文字のスキャナで機能するために必要となるためである。乱雑フィールド６１３は、様々なレベルのスキャン効率および有効性を提供するので、異なる比率（３、５またはそれ以上の文字スキャン）でスキャンするように分割される。スキャンの範囲が狭くなる（文字の量が少なくなる）につれて、精度が向上する（逆もまた同様である）。スキャナのフィールド領域が増加するにつれて、より大きい文字スキャナは、精度を犠牲にして認識を実行するので、より効率的になる（これは、ターゲットがどれだけ小さいかによって異なる）。メモリコンセプトのインデックス付け（ＭＣＩ）５００では、ステージ６１７は未処理のメモリコンセプトが残っていることに応答して、スキャナのサイズ（３、５またはそれ以上）を切り替える。ＭＣＩ５００は利用可能なスキャナの中で最

大のものから始め、ステージ６１７において徐々に減少し、より多くのコンピューティングリソースが発見され、より小さなメモリコンセプトターゲットの存在可能性をチェックすることができる。ステージ６１８は、ステージ６２０でそれらのインデックス（３または５などの適切な長さに適した、より小さいセグメント）を導出できるように、利用可能なメモリコンセプトを循環的に使用する。メモリコンセプトがコンセプトインデックスホールドアウト６２４にまだ存在しなかった場合、ステージ６１９は、処置のロジスティックフローに従ってメモリコンセプトを作成する。ステージ６２１は、ステージ６２０からの導出インデックスをホールドアウト６２４に割り当てる。ＭＣＩ５００のプログラムされた一通りの処理が継続するとき、ＭＣＩが未処理の文字スキャナを使い切った場合、ホールドアウト６２４が空であれば空（ヌル）の結果６２２を提出するか、空でないホールドアウト６２４を、モジュールの出力６２３として出力する。乱雑フィールド６１３のセクションは、符号６２５から６２８の範囲である。セクション６２５および６２６は５文字スキャナによって実行されるスキャンを表し、セクション６２７および６２８は３文字スキャンを表す。スキャン６２５は５文字の幅を持ち、一方で６文字のターゲット「ＴＯＭＡＴＯ」をチェックし、２つの５文字セグメントは以前にＭＣＩ５００でインデックス付けされていた「ＴＯＭＡＴ」と「ＯＭＡＴＯ」で一致した。これらのそれぞれは、６文字の単語のうち５文字の一致に対応し、さらに８３％に対応する。この割合／パーセンテージは、メモリコンセプト「ＴＯＭＡＴＯ」のために累積的に１６７％６３７で追加され、したがって、「ＴＯＭＡＴＯ」というコンセプトは、乱雑フィールド６１３において首尾よく発見された。スキャン６２６は、「ＥＧＧＰＬＡＮＴ」のメモリコンセプトターゲットを有し、２つの重要なセグメントは「ＧＧＰＬＡ」および「ＰＬＡＮＴ」である。「ＧＧＰＬＡ」は「ＥＧＧＰＬＡＮＴ」の本当の一致を指す一方で、セグメント「ＰＬＡＮＴ」は、「ＰＬＡＮＴ」がメモリコンセプトのターゲットであるため、誤検出の可能性をもたらす。システムが「ＰＬＡＮＴ」を乱雑フィールド６１３に存在するものとして認識するためには、「ＥＧＧＰＬＡＮＴ」がフィールド内の唯一の本物の認識可能なメモリコンセプトであると誤認として分類される。しかし、「ＧＧＰＬＡＮＴ」が６３％の一致に寄与し、「ＥＧＧＰＬＡＮＴ」のコンテキストで「ＰＬＡＮＴ」が６３％寄与し、ターゲット「ＰＬＡＮＴ」のコンテキストで「ＰＬＡＮＴ」が１００％寄与するので、システムのプログラミングは疑陽性のケースシナリオを迂回することができる。これらの一致が合計で加算されると、そのターゲット「ＥＧＧＰＬＡＮＴ」は１２５％（６３％＋６３％）の集計スコア６３８を受け取り、ターゲット「ＰＬＡＮＴ」は１００％６３９を得る。したがって、スキャナは、乱雑フィールド６１３の正しい解釈をうまく維持している。スキャン６２７は３文字の幅を持ち、セグメント「ＴＯＭ」を認識し、これは５０％６４０の合計一致につながる。これは、スキャン幅に差がある（５ではなく３）ために、スキャンのフィールド６２５に存在するのと同じターゲットであり、弱い確信度の一致（５０％対１６７％）が見つかった。したがって、ＭＣＩ５００の設計は、正確さと消費されたコンピューティングリソースとの間の正確なバランスをとるために、スキャン幅の複数の層を含んでいる。スキャン６２８はまた３文字の幅を組み込み、今回は２つの潜在的な偽陽性接線６３６を有している。フィールドの実際のコンセプトは「ＣＡＲＲＯＴ」だが、「ＣＡＲ」と「ＲＯＴ」のコンセプトはフィールド内に存在するものとみなされる。スキャナは、乱雑フィールド６１３に位置する正しいコンセプトがどれであるかを識別しなければならない。これは、近くの文字で行われた後続のスキャンでチェックされる。結局、スキャナは、他の位置付けされた指標の裏付けのために、このコンセプトを「ＣＡＲＲＯＴ」と認識し、「ＣＡＲ」または「ＲＯＴ」ではないと認識する。「ＣＡＲ」６４１の１００％複合マッチと「ＲＯＴ」６４３の１００％複合マッチの両方が、「ＣＡＲＲＯＴ」６４２の２００％複合マッチに対して敗退する。

【０１３６】

図９８～図９９は、フィールド解釈ロジック（ＦＩＬ）６４４および６４５を示しており、フィールド解釈ロジックは、文字幅の様々な複数のスキャナを管理するロジスティクスを実行する。汎用スコープスキャン６２９が、大型の文字スキャンからロジックを始める

。この種のスキャンは、フィールドの大規模なスコープを少ないリソースで精査する。ただし、小規模なスケールでの精度は損なわれる。より小型の文字スキャナはフィールド上のより詳細なスコープを任され、必要なときに精度を改善する。詳細スコープスキャン６３０は、重要なエリアが特定され、そこに「ズームイン」する必要のある場合に用いられる。全体的な相関関係は、スキャニングのために選択されたフィールド上のスコープが狭いほど、小型の（文字数の少ない）スキャナとなる。このことで、冗長で生産性のない場所では、高コストな高精度のスキャンは用いられないことが保証される。ＦＩＬのセクション６４５は、スキャナの結果への反応的ロジスティクスを示している。特定のスキャナが乱雑フィールド６１３でメモリコンセプトの追加の認識を受け取る場合、これはフィールドスコープ６３１（６１３のセクション）が高密度飽和のメモリコンセプトを含み、その特定のスコープをより狭い幅のスキャンで「ズームイン」する価値があることを示している。したがって、フィールドスコープが３０％６３２の５文字スキャナは、「増加した「追加の」認識」６３４とみなされた当初の結果であることに依存している、１０％６３３のフィールドスコープを持つ３文字スキャナを起動する。参照符号６３４の「追加」は、ＦＩＬセクション６４４で実行された当初の認識を補完するものであることを示している。

【０１３７】

図１００～図１０１は、自動化パーセプション発見メカニズム（ＡＰＤＭ）４６７を示している。観察者６４６は、デジタルな観察者または人間の観察者を表す一方で、同一のオブジェクトを複数のパーセプションで知覚することができる。観察可能なオブジェクトは、あり得るサイバーセキュリティのケースシナリオを示すために使用される。パーセプション視点６４７は、２次元でレンダリングされる観察可能なオブジェクトに関する限られたスコープの情報をもたらす。パーセプション視点Ｂ６４８は、第３の次元を含むので、より情報量多いスコープをもたらす。パーセプション視点Ｃ６４９の結果は、創造的な混成プロセスである創作１８が最新の並列処理能力によって活用されているため、自分達の限られた思考能力とっては未知である。クリティカルシンキングアルゴリズムは、視点ＡとＢのメトリックを混成し、新バージョン６５３を形成することにより、人間の理解力またはイテレーションの複雑度＋効力とＣＰＵ時間と電力との（停滞しない）指数関数的な関係を超えることができる形状とパーセプションを生成する可能性を有する。パーセプション視点６５０は、スコープ、種別、強度、および一貫性６５１を含む、しかしそれらに限定されない、複数のメトリックによって構成されている。これらのメトリクスは、全体的なパーセプションを構成する複数のパーセプションの側面を定義している。これらは、上記の例よりもスコープにおいて複雑になる可能性があるため、創作モジュールによって生成されるパーセプションの複雑なバリエーションが多数存在する可能性がある。パーセプションウェイト６５２は、パーセプション観察者エミュレータ（ＰＯＥ）４７５によってエミュレートされている間に、パーセプションがどの程度の相対的な影響を有するかを定義している。両方の入力パーセプションのこの重みは、新しくイテレートされたパーセプション６５３の重みを定義しつつ検討される。この新しくイテレートされたパーセプション６５３は、以前の世代のパーセプションから影響を受けた、ハイブリッド化されたメトリックを含む：Ａ＋Ｂ。このような新たなパーセプション視点は、潜在的に秘密のエクスプロイトを検出するためのセキュリティソフトウェアに対して有利な立場を提供する可能性がある。試行錯誤と知的選択の組合せによる混成のためにパーセプションの世代が選択される。あるパーセプション、特に新しくイテレートされたパーセプションがセキュリティ上の問題の洞察を提供する上で無用であると判明した場合、それは使用のためにそれほど重要視しないようにするすることができるが、それが有用な洞察を提供する場合には、あまり知られていないため、削除されることはほとんどない。したがって、計算機能力リソースとセキュリティ情報収集のトレードオフが経験される。

【０１３８】

図１０２は、選択パターンマッチングアルゴリズム（ＳＰＭＡ）５２６からメタデータログを受け取るモジュールである、未処理パーセプション生成（ＲＰ２）４６５を示してい

る。そのようなログはパースされ、そのようなアルゴリズムのパーセプションを表すパーセプションが形成される。パーセプションは、複合パーセプションフォーマット（ＰＣＦ）に格納され、パーセプション観察者エミュレータ（ＰＯＥ）によってエミュレートされる。システムメタデータ分離（ＳＭＳ）４８７は、セキュリティ応答／変数のペア６５４の出力を提供し、適切な修正処置がトリガ変数（対象、場所、行動分析など）と組み合わされたときに、セキュリティの因果関係を確立する。比較可能変数フォーマット５４７は、非グラフィカルな用語６５５で表される。これらのパーセプションコレクションの各々は、ＣＶＦ５４７を形成するための特定の重み付けされた影響を伴う様々なパーセプションを有する。

【０１３９】

図１０３は、比較可能可変フォーマットジェネレータ（ＣＶＦＧ）の論理フローを示している。ＣＶＦＧの入力は、データバッチ６５８であり、生成されたＣＶＦ５４７のノード構成によって表されなければならないデータを表している、データの任意の集合である。ステージ６５９は、データバッチ６５８によって定義された個々のユニットのそれぞれをシーケンシャルに使用する。データユニットは、ステージ６６０でノードフォーマットに変換され、最終のＣＶＦ５４７によって参照されるのと同じ構成の情報を有する。ノードはＣＶＦの基本単位であり、効率的で正確な比較評価が他のＣＶＦに対して実行されることを可能にする。ＣＶＦは、比較について最適化された性質（ノード）を持つことを除いて、不可逆なＭＤ５ハッシュサムと似ている。このように変換されたノードは、ステージ６６５でそれらの存在をチェックすると、ノードホールドアウト６６１に一時的に格納される。それらが見つからなければ、それらはステージ６６２で作成され、ステージ６６３で、発生および使用などの統計情報で更新される。ステージ６６４において、ホールドアウト６６１を有するすべてのノードが組み立てられ、ＣＶＦ５４７として、モジュールの出力としてプッシュされる。ジェネレータが実行された後にホールドアウト６６１が空であれば、空の結果が返される６１８。

【０１４０】

図１０４において、ノード比較アルゴリズム（ＮＣＡ）６６１は、未処理のＣＶＦ５４７から読み取られた２つのノード構成６６６および６６８を比較している。ＣＶＦの各ノードはプロパティの大小を表している。個々のノードごとに、類似度比較が行われ、総合分散が計算される。これにより、正確な比較が効率的に計算されることが保証される。分散の数値が小さい場合は、それがノード固有であれ統合ウェイトであれ、一致度が高いことを表している。実行されうる比較には２つのモード：部分一致モード（ＰＭＭ）と全部一致モード（ＷＭＭ）がある。ＰＭＭでは、１つのＣＶＦにアクティブノードがあり、それが比較候補に見つからない（ノードが休止状態である）の場合、この比較にはペナルティが課されない。モード適用例：木Ａを森Ａと比較すると、木Ａは森Ａ内に存在する最も近い一致木Ｂを見つけるＷＭＭでは、１つのＣＶＦにアクティブノードがあり、それが比較候補に見つからない（ノードが休止状態である）の場合、この比較にはペナルティが課される。モード適用例：木Ａと森Ａを比較するとき、木Ａと森Ａが直接比較され、重複と構造的類似性に大きなばらつきがあるため、一致するものは見つからない。

【０１４１】

図１０５～図１０６は、入力システムメタデータ４８４を、意味のあるセキュリティ上の因果関係に分割する、システムメタデータ分割（ＳＭＳ）４８７を示している。ＭＣＭ４８８からの出力として、ログのプログラミング要素がステージ６７２で個別に取り出される。ステージ６７３では、ＭＣＭからの個々のカテゴリを使用して、セキュリティ応答とセキュリティ変数（セキュリティログ）との間の関係のより詳細な構成を得る。このようなカテゴリ化６７４は、ステージ６６９、６７０、および６７１において同化される。対象スキャン／同化６６９により、カテゴリ化モジュールからの事前分類コンテナおよび未処理分析結果を使用して、システムメタデータからセキュリティ状況の対象／疑いが抽出される。対象は、セキュリティ応答／変数の関係を導出するための主な参照点として使用される。対象は、人、コンピュータ、実行可能コード、ネットワーク、または企業にさえ

含まれる可能性がある。そのようにパースされた対象６８２は、対象ストレージ６７９に格納される。リスクスキャン／同化６７０により、セキュリティ状況のリスク要因が、事前に作成された分類コンテナおよび分類モジュールからの未処理分析結果を使用して、システムメタデータから抽出される。リスクは、そのようなリスクを呈している、またはリスクにさらされているターゲットとなる対象に関連している。リスクは、潜在的な攻撃ポイント、攻撃の脆弱性のタイプなどとして定義できる。そのようなリスクは、対象インデックス６８３で関連する対象との関連付けを使用してリスクストレージ６８０に格納される。応答スキャン／同化６７１により、カテゴリ化モジュールからの事前に作成された分類コンテナおよび未処理分析結果を使用して、システムメタデータから、入力アルゴリズムによって生成されたセキュリティ状況の応答が抽出される。この応答は、そのような応答に値するとされるセキュリティ対象に関連付けられている。応答は、承認／ブロック／フラグ／検疫／難読化／シグナル模倣／報復ななどどの範囲に及ぶ可能性がある。そのような応答は、対象インデックス６８３で関連する対象への関連付けと共に応答ストレージ６８１に格納される。そのような格納された情報は、該当するリスクおよび応答を有するすべてのセキュリティ対象を包括的に仕分けるデータ入力ロジック（ＰＬ）４８３によって処理される。

【０１４２】

図１０７～図１０８は、メタデータカテゴリ化モジュール（ＭＣＭ）４８８を示している。フォーマット分割６８８において、メタデータは、認識されたフォーマットのルールおよび構文に従って分離され、分類される。そのようなメタデータは、認識可能なフォーマットにしたがって構成されていなければならず、そうでなければ、メタデータは処理のために拒絶される。ローカルフォーマットルールおよび構文６８９は、ＭＣＭモジュールが予めフォーマットされたメタデータストリームを認識できるようにするための定義を含んでいる。ローカルとは、メタデータ内の関連性および存在が理由で以前に選択された「フォーマットの」ことを意味する。デバッグ追跡４８５は、使用される変数、関数、メソッドおよびクラス、およびそれぞれの入力および出力変数の種別／内容を提供するコーディングレベルのトレースである。完全な関数呼び出しチェーン（他の関数を呼び出す関数）が提供される。アルゴリズム追跡４８６は、アルゴリズム分析結果と結合されたセキュリティデータを提供するソフトウェアレベルのトレースである。結果としてのセキュリティ決定（許可／ブロック）は、その決定（正当化）にどうやって到達したかの道筋と、各要素がそのセキュリティ決定を行うのに貢献した適切な重みと一緒に提供される。そのようなアルゴリズム追跡４８６は、ステージ６８６でのこれらのセキュリティ上の決定の正当化の各々を循環的に使用するＭＣＭのモードにつながる。そのような正当化は、（人間によって直接書かれたのではなく）コンピュータログ構文で特定のセキュリティ応答がどのように、そしてなぜ行われたのかを定義している。認識可能フォーマット６８７は、ＣＭＴＰと互換性がある、予め定められ、標準化された構文フォーマットである。したがって、入力システムメタデータ４８４からのフォーマット宣言が認識されない場合、モジュールの空の結果が返される６１８。ＣＩＭＰによって認識可能な標準化されたフォーマットでメタデータ４８４をコード化することは、ＳＰＭＡ５２６のプログラマの義務である。このようなフォーマットは、ＣＴＭＰ独自で専用のものである必要はない（ＪＳＯＮやＸＭＬなど）。変数ホールドアウト６８４は、処理中の変数を最終の統合出力としてまとめて提出６８５できるように、それらをカテゴリ別に保持している場所である。ステージ６７５は、デバッグ追跡４８５およびアルゴリズム追跡４８６である入力情報の２つの主要な分岐の間の比較チェックを行う。そのような比較は、なぜそのようなセキュリティ正当化が起こったのか、ＭＣＭの出力になる価値があるのかをよりよく理解するために、コーディングレベルでの正当化の発生を追跡している。ＣＴＭＰの潜在的な批判を全体としてさらに検証するためには、セキュリティ上の正当性を裏付ける推論を保証するために、このステップは予防的であり、決定はコーディングレベルでも十分に理解されている。同様に、リスクの証拠は、ステージ６７６でトレースデータのデバッグを用いて裏付けが確認される。ステージ６７７で、ＳＰＭＡによって呼び出されたあらゆる機能についてメタデ

ータがチェックされ、その後、そのような適用可能な機能が、使用される機能的目標および正当性が認識可能フォーマット６８７の仕様にしたがって定義されているかどうかがチェックされる。

【０１４３】

図１０９は、メトリック処理（ＭＰ）４８９を示しており、メトリック処理は、選択パターンマッチングアルゴリズム（ＳＰＭＡ）５２６のセキュリティ応答からの変数をリバースエンジニアリングし、このアルゴリズムの情報から、パーセプションを「救い出す」。セキュリティ応答Ｘ６９０は、ＳＰＭＡにより選ばれる結果としてのセキュリティ応答（たとえば、許可／ブロック／難読化）に寄与する一連のファクタを表している。図形の一つ一つが、選択パターンマッチングアルゴリズム（ＳＰＭＡ）からのセキュリティ応答を表している。初期ウェイトはＳＰＭＡによって決定され、したがって、その情報は活用されている。このような決定がその後モデルパーセプションに大量に参照される。パーセプション推論（ＰＤ）４９０は、このセキュリティ応答の一部と、これに対応するシステムメタデータを使用して、セキュリティ応答の元のパーセプションを再現する。多次元型シリーズ６９９のパーセプション解釈は、ＰＤがＳＰＭＡのセキュリティ応答を採用して、該当する入力システムメタデータ４８４に関連付けすることで、ＳＰＭＡが元々使用しているとおりの知的「デジタルパーセプション」のフルスコープを再生成する様子を表している。これによりＣＴＭＰは入力アルゴリズムの深い理解が得られ、複数の様々なアルゴリズムの情報を再利用および相互参照でき、したがって、人工知能の大きな金字塔が打ち立てられようとしている。このような図形は、ＳＰＭＡにより構築された複合ルール、挙動、および相関関係を象徴している。塗り潰し図形６９７、積み上げ量６９８、および多次元型６９９は、知的アルゴリズムの「考え方」をうまく捉えるデジタルパーセプションである。多次元型６９９のパーセプションは、３次元図形を表しており、これは会社従業員の社内メールを解釈したり、会社の機密情報のセキュリティ侵害を検知および／または予測を試みたりする、言語学習アルゴリズムの象徴的表現形式となり得る。多次元型が若干のバリエーションを有する単一の知的アルゴリズム（たとえば、バリエーション６９４Ｃが円形であるのに対し６９５Ｃ／６９６Ｃは長方形であり、知的アルゴリズムのわずかな差異を表している）のに対して、そのようなアルゴリズムによって表面上の意味が作成されていないように見えるかもしれない複数の初期セキュリティ応答が存在する可能性がある。表面上の意味６９４Ａは、６９６Ａよりも６９２Ａと共通しているように見える。これが直感に反しているにもかかわらず、６９２Ａは、多次元型６９９とは完全に異なる塗り潰し図形アルゴリズムによって実行されたセキュリティ応答である。パーセプション６９５Ｃおよび６９６Ｃが同一であるのに対して、それらのセキュリティ応答に対応する物６９５Ａおよび６９６Ｂには、わずかな差異がある。セキュリティ応答６９５Ａはより濃く、この多次元型パーセプションを側面６９５Ｂから表現しているのに対して、セキュリティ応答６９６Ａは、全く同じパーセプションではあるが、これを正面６９６Ｂから表現している。これらの差異は、異なるセキュリティ脅威／疑いに対して応答する、様々なセキュリティ応答が、リバースエンジニアリングされ、同一の知的アルゴリズムであると判明する様子を示している。多次元型６９９の３つのインスタンス（うち２つは同一物）すべてが単一のユニットへと合成され、その後、パーセプション視点Ｂ７０２としてＣＴＭＰの中で内部的に参照される。このパーセプション視点がＣＴＭＰの中で有する影響力のウェイトが、セキュリティ応答６９６Ａ、６９５Ａ、および６９６Ａが持つ影響力の初期ウェイトにしたがって計算される。積み上げ量パーセプション６９８によって、多次元型６９９のごとく３次元目の深さを受け取るのではなく、セキュリティ応答６９３Ａが整数倍量のセットの一部であることがわかる。これは、外部からの潜入を回避するために新しい会社従業員のセキュリティプロファイルを構築する、プロファイリングアルゴリズムの象徴的表現形式でありうる。ＣＴＭＰは最初セキュリティ応答６９３Ａとして表される単一のセキュリティプロファイルのみを受信するが、実際には（ＭＰ４８９がリバースエンジニアリングを実行した後に）パーセプションの積み上げ量６９８呼ばれる相互参照プロファイルの集合の一部である。そのような認識は、パーセプション視点Ａ７０１として

ＣＴＭＰ内で参照できる。セキュリティ応答６９１Ａおよび６９２Ａでは、不完全な形として象徴的に表されるセキュリティ応答がＭＰ４８９に提供される。ＰＤ４９０は、入力システムメタデータを活用して、このセキュリティレスポンスの起点となった知的アルゴリズムが、期待されるセキュリティ変数が存在しないことを見つけ出す。たとえば、これは、疑わしい動作の存在に気づくのではなく、通常の／期待された挙動がないことに気づくアルゴリズムである。これは、通常のやり方で自分の電子メールに署名しない会社の従業員かもしれない。これは、習慣を突然変更すること、またはこの従業員の電子メールアカウントが、本物の従業員のように電子メールに署名することに慣れていない悪意のある行為者によって攻略されたという徴候を意味する可能性がある。このようなアルゴリズムは、適切な重みの影響によりパーセプション視点Ｃ７００としてＣＴＭＰ内で参照されるデジタルパーセプション塗り潰し図形６９７となるようにリバースエンジニアリングされる。

【０１４４】

図１１０および１１１はパーセプション推論（ＰＤ）４９０の内部設計を示しており、これは、主にメトリック処理（ＭＰ）４８９により使用される。セキュリティ応答Ｘは根拠／理由付けの算出７０４への入力として転送される。このモジュールは、意図ＤＢ７０５に格納されている入出力削減（ＩＯＲ）モジュール７０６の意図の供給を活用することによって、ＳＰＭＡ５２６のセキュリティ応答の正当化を決定する。このようなモジュールＩＯＲは、関数の入出力関係を解釈して、関数の目的の正当性と意図を決定する。ＩＯＲモジュールは、メタデータにリストされたさまざまな関数呼び出しの分割された入出力を使用する。このようなメタデータ分割は、メタデータカテゴリ化モジュール（ＭＣＭ）４８８によって実行され、出力カテゴリは、コレクション６７２および６７４として発生する。ＪＲＣ７０４では、意図ＤＢ７０５に格納された機能の意図が、入力６９０として提供されたセキュリティ応答に対してチェックされる。機能の意図がＳＰＭＡのセキュリティ決定を裏付ける場合、それらは有効な根拠・メトリック変換ＪＭＣ７０３として提出される。このＪＭＣモジュールでは、検証されたセキュリティ応答の根拠が、パーセプションの性質を定義するメトリックに変換される。メトリックは人間の感覚に似ており、セキュリティ応答の根拠はこの感覚を使用する根拠を表している。人が道路を横切ると、視覚と聴覚の感覚（すなわちメトリック）が高まり、嗅覚と触覚の感覚は休止する。これらの感覚の集合は、強度のそれぞれの大きさとともに、「道路横断」パーセプションを表す。このアナロジーの根拠は、「道路上の車両は危険であり、あなたはそれらを見て聞くことができる」というものである。したがって、このパーセプション構成は合理的に正当化され、パーセプション視点Ｃ５４３の例が形成される。入出力関係は、一組の関数入力と、そのような関数によって提供された対応する出力として定義される。ＩＯＲ７０６は、関数の入出力関係および関数の「意図」が内部データベースを参照することによって事前に分析されているかどうかをまずチェックする。情報がこのデータベース内に見つかった場合、ステージ７０８で、現在の入出力データを捕捉するために情報が使用される。補足された（該当する場合）入出力データは、ステージ７１４で十分なレベルの意味のある分析を達成するほど十分に飽和しているかどうかをチェックされる。この量は専門用語で定量化され、最小レベルは既存のＣＴＭＰポリシーによって定義される。解析すべき入出力情報の量が不十分であれば、その特定の機能の分析はステージ７１１で中止され、ＩＯＲモジュール７０６は次の利用可能な機能に進む。分析するのに十分な量の情報がある場合、入出力関係は類似性７０９にしたがって分類される。たとえば、一つの入出力関係がある通貨を別の通貨に変換する（たとえば、ＵＳＤからＥＵＲ）ことが判明する一方で、別の入出力関係が、ある単位の単位を別の単位（たとえば、ポンドからキログラム）に変換することが判明する。双方の入出力関係は、トリガのコンセプトがカテゴリ化インデックスに関連付けられているため、データ変換に属するものとして分類される。たとえば、そのようなインデックスはＵＳＤ、ＥＵＲ、およびポンドを参照することができ、キログラムはデータ変換カテゴリを参照する。したがって、これらの単位が入出力関係で見つかると、ＩＯＲ７０６はそれらを適切に分類することができる。したがって、関数の意図は、通

貨と単位の変換関数である疑いがある。利用可能なすべての入出力関係を分類すると、カテゴリはステージ７１０で含まれる入出力関係の重みの量にしたがって格付けされ、最も人気があるものが最初に現れる。ステージ７１５で、入出力データのカテゴリが、機能の意図のパターンを確実に表示できるかどうかがチェックされる。これは、関数が実行する入出力変換の一貫性をチェックすることによって行われる。特定のカテゴリの情報が永続的かつ個別である場合（通貨をあるカテゴリに変換し、単位を第２のカテゴリに変換するなど）、これらのカテゴリは関数の「意図」となる。したがって、この機能は、通貨および単位を変換する意図を持つものとして説明される。ＩＯＲ７０６は、機能を目的にまとめることにより、ＣＴＭＰがコードに存在する機能の実際の目標を検証し、そのようなコードの実行によって損害が発生する前に悪意のある行動を先取りするために知的にスキャンすることができる。「意図」がＩＯＲ７０６によって十分な程度の信頼度で十分に理解されていれば、モジュールの出力７１２として提出される。「意図」カテゴリが互いに強く裏付けしておらず、機能の「意図」が確信を持って確立されていない場合、この機能の「意図」は未知と宣言され、ＩＯＲ７０６はステージ７１１で分析のために次の利用可能な機能に進む。

【０１４５】

図１１２～図１１５は、パーセプション観察者エミュレータ（ＰＯＥ）４７５を示している。このモジュールは、観察者のエミュレーションを生成し、パーセプションポイントの候補すべてを、このような様々な観察者エミュレーションを使用してテスト／比較する。入力は、そのパーセプションポイントの候補のすべてと、拡張データログであり、一方で、出力は、このような拡張データログから、このような選択されたパーセプションの組み合わせと、最良で、最も該当する、最も注意深い観察者によって生成される、結果としてのセキュリティ上の判断である。入力システムメタデータ４８４は、未処理パーセプション生成（ＲＰ２）４６５によって、比較可能可変フォーマットＣＶＦ５４７でパーセプションを生成するために使用される初期入力である。ストレージ検索（ＳＳ）４８０では、データ拡張ログから導出されたＣＶＦ（比較可能可変フォーマット）が、パーセプションストレージ（ＰＳ）４７８のデータベース検索における判定基準として使用される。ＰＳは、最も一致するＣＶＦを有するデータベースから利用可能なすべてのＣＶＦ５４７を提供する。それらの関連するパーセプション構成とウェイトは、結果７１６で成功した一致イベントに参照され、使用される。類似度の重複は、６０％一致７１９および３０％一致７２０として言及される。そのような結果は、ストレージ検索４８０によって計算される。結果７１６では、一致７１９および７２０が格納され、その後、ウェイト計算７１８で個々のパーセプションの格付けについて計算される。このような計算は、入力ＣＶＦと比較してデータベースＣＶＦの全体的な類似度（または一致）値をとり、その値を個々のパーセプションウェイトで乗算する。このようなウェイトは、メトリック処理（ＭＰ）４８９によって最初に決定されたように、ＣＶＦに既に格納され、関連付けられている。格付け７１７では、パーセプションは最終的なウェイトに応じて順序付けられる。そのような格付けは、セキュリティ状況を理解し、最終的にブロック７３０または許可７３１コマンドの出力を渡すために、最も関連性の高い（ウェイト計算７１８の重み付けされた）パーセプションを使用する選択プロセスの一部である。一度パーセプションが格付けされると、アプリケーション７２９に転送され、そこではデータ拡張ログ７２３がパーセプションに適用されて、ブロック／許可の推奨を生成する。ログ７２３は、オリジナルのセキュリティインシデントを伴うシステムの入力ログである。自己批判的知識密度（ＳＣＫＤ）４９２は、未知の知識の期待される上限スコープを定義するために、ログをタグ付けする。これは、パーセプションによって、未知のデータスコープでタグ付けされたデータを検討できることを意味する。これは、知っていることの程度と知らないことの程度の見積もりを考慮して、セキュリティインシデントの査定をより正確に実行できるということを意味する。データパース７２４は、オリジナルの選択パターンマッチングアルゴリズム（ＳＰＭＡ）５２６によって決定されたオリジナルの許可またはブロックの決定７２５を出力するために、データ拡張ログ７２３および入力システムメタデータ４８４の基本解釈を行う

。したがって、２つの潜在的なケースシナリオが存在し、ＳＰＭＡは、シナリオ７２７におけるセキュリティ関連インシデントをブロックする（たとえば、プログラムダウンロードを防止する）７３０を選択するか、またはシナリオ７２６においてそのようなインシデントを承認する７３１のいずれかを選択している。現時点では、ＣＴＭＰ２２はこれまでに、決定を批判する（サイバーセキュリティを含むがこれに限定されない）という、最も核心的かつ重要なタスクを実行する準備が整うところまで前進している。この批判は、パーセプションに応じてパーセプション観察者エミュレータ（ＰＯＥ）に１回、論理的に定義されたルールにしたがって１回、ルール実行（ＲＥ）で２回、ＣＴＭＰ内で２回発生する。ＰＯＥ内では、ＳＰＭＡからブロックコマンドを受信すると、７３２の上書きロジックが使用される。ＳＰＭＡから許可コマンドを受信すると、７３３の上書きロジックが使用される。ステージ７３２Ａにおいて、ブロック７３０のデフォルト処置が仮定され、ブロック－平均の値および許可－平均の値７３２Ｂは、ケースシナリオ７２７に格納されたブロック／許可の確信度の平均を見つけることによって計算される。ステージ７３２Ｃは、ケースシナリオ７２７の平均確信度が予め定義された（ポリシー別の）確信度の限界よりも大きいかどうかをチェックする。シナリオの確信度が低い場合、これは、ＣＴＭＰは情報／理解が不十分であるために批判を控えていることを示している。このような低い信頼度の状態が生じると、ＲＭＡフィードバックモジュール７２８は、より多くのパーセプションを含むセキュリティ状況を再評価しようと試みるために、ステージ７３２Ｄに関与する。このように追加的に考慮されるパーセプションは、確信度の限界を高める可能性がある。したがって、ＲＭＡフィードバックは、リソース管理ポリシーにしたがって再評価が許容されるかどうかを確認するために、リソース管理および割り当て（ＲＭＡ）４７９自体と通信する。そのような再評価が拒否された場合、アルゴリズムはその考えられる最高信頼度に達しており、このＰＯＥセッションでは最初の許可／ブロックの決定を上書きすることが永久に中断される。ステージ７３２Ｅは、ＲＭＡフィードバックモジュール７２８が、より多くのリソースを再割り当てするためにＲＭＡ４７９からの許可を受け、したがってより多くのパーセプションを計算に再割り当てする条件を示している。このような状態になると、ステップ７３２Ｆで上書きの試み（ＣＴＭＰの批評）が中止され、ケースシナリオ７２７の新たな評価が追加のパーセプション（したがってコンピュータリソース負荷の増加）とともに行われることが可能になる。ステージ７３２Ｇは、ステージ７３２Ｈでデフォルトブロックアクション７３０／７３２Ａを許可アクション７３１に変更するのに十分な許可平均が（ポリシーにしたがって）確実であることを示す。ケースシナリオ７２６で発生する許可ロジック７３３にも同じロジックが適用される。ステージ７３３Ａでは、デフォルト処置がＳＰＭＡ５２６によって要求されたとおり、許可に設定される。ブロック－平均の値および許可－平均の値７３３Ｂは、ケースシナリオ７２６に格納されたブロック／許可の確信度の平均を見つけることによって計算される。ステージ７３３Ｃは、ケースシナリオ７２６の平均確信度が予め定義された（ポリシー別の）確信度の限界よりも大きいかどうかをチェックする。このような低い信頼度の状態が生じると、ＲＭＡフィードバックモジュール７２８は、より多くのパーセプションを含むセキュリティ状況を再評価しようと試みるために、ステージ７３３Ｄに関与する。ステージ７３３Ｅは、ＲＭＡフィードバックモジュール７２８が、より多くのリソースを再割り当てするためにＲＭＡ４７９からの許可を受け、したがってより多くのパーセプションを計算に再割り当てする条件を示している。このような状態になると、ステップ７３３Ｆで上書きの試み（ＣＴＭＰの批評）が中止され、ケースシナリオ７２６の新たな評価が追加のパーセプション（したがってコンピュータリソース負荷の増加）とともに行われることが可能になる。ステージ７３３Ｇは、ステージ７３３Ｈでデフォルト許可の処置７３１／７３３Ａを許可の処置７３０に変更するのに十分な許可の平均が（ポリシーにしたがって）確実であることを示す。

【０１４６】

図１１６～図１１７は、現時点での既知のパーセプション観点から意味付けられうる、データのパーセプション観点を導出する、意味付けの導出（ＩＤ）４７７を示している。適

用済パーセプション観点４７０は、ＣＴＭＰストレージシステムに保存されている既知のパーセプションの範囲である。そのようなパーセプション４７０は、ＳＰＭＡ５２６によって適用され、使用され、パーセプションの集合７３４として集められ、メトリック合成４９３に転送される。このモジュール４９３は、パーセプション視点７３４のフォーマットを、意味付けの導出（ＩＤ）４７７によって認識されるフォーマットである、メトリックのカテゴリに変換する。メトリックの複合度７３６では、円の外側の境界は、個々のメトリックに関する既知の知識のピークを表す。したがって、円の外縁に向かうにつれて、メトリックの複雑さがより大きいことを表し、一方、中心はメトリックの複雑さがより小さいことを表す。中央の明るい灰色は、現在のひとまとまりの適用済パーセプション観点のメトリック合成を表し、外側の濃い灰色は、システムによって格納され、一般に知られているメトリックの複合度を表す。ＩＤ４７７のゴールは、関連するメトリックの複合度を増やし、それによってパーセプション観点を複合度と量において増大させることができるようになることである。現在のひとまとまりの適用済パーセプション観点からの既知のメトリックの複合度は、そのような詳細／複合度がまだ含まれていない場合、関連するメトリックＤＢ７３８に追加される。このようにして、システムは完結し、新たに格納されたメトリックの複合度は、将来ありうる、ひとまとまりのパーセプション観点の意味付けの導出おいて使用され得る。このような複合メトリック構成７３６が、メトリック拡張（ＭＥ）４９５への入力として渡され、そこでは多数のさまざまなパーセプションの視点のメトリックが、個々のデータベース７３８に、カテゴリ別に格納される。暗い灰色の表面積は、現在のひとまとまりの適用済パーセプション観点の全範囲と、既知の上限に応じて残されたスコープの量を表す。メトリックの上限は、それぞれのメトリックＤＢのピーク知識によって表される。したがって、（現在のひとまとまりのパーセプション観点によって導出された）現在のひとまとまりのメトリックは、それらのメトリックの既知の詳細／複合度により拡張される。拡張され複合度が高められると、メトリックはメトリックの複合度７３７として戻される。図解７３７に示すように、明るい灰色領域は、スコープ７３９、一貫性７４０、種別７４１、および強度７４２の、４つのメトリックセクタすべてにおいてより大きくなっている。これは、４つのメトリックセクタすべてにおいて、そのパーセプションがより詳細かつ複雑になっていることを示している。この拡張されたメトリックの複合度７３７は、メトリック変換４９４の入力として渡され、メトリック変換４９４は、個々のパーセプション観点から全体のパーセプション観点７３５に戻す。したがって、最終出力は、オリジナルの入力適用済パーセプション観点４７０の拡張バージョンである、意味付けられたパーセプション観点として組み立てられる。

【０１４７】

図１１８～図１２０は自己批判的知識密度（ＳＣＫＤ）４９２を示しており、これは、報告可能なログの限界を越えた、未知である可能性がある知識のスコープおよび型を推定する。このようにして、この結果生じるＣＴＭＰ２２のクリティカルシンキング的な特徴によって、システムが直接知っている、または知らない、関与する知識のすべての可能なスコープを広げることができる。以下は、ＳＣＫＤ４９２の意図された機能と能力を実証するためのユースケースの例である。

１）このシステムは、核物理学のための強力な参照範囲を構築している。

２）このシステムは、原子核物理学と量子物理学が、複合度と種別においてカテゴリ的かつ系統的に類似しているという類推を行っている。

３）しかしながら、このシステムは、量子物理学については、核物理学に比べて参照可能な知識がはるかに少ない。

４）したがって、システムは、潜在的に達成可能な量子物理学知識の上限を核物理学の類推を用いて定義している。

５）システムは、量子物理学的に未知の知識の範囲が大きいと判断している。

既知データカテゴリ化（ＫＤＣ）７４３は、確認された（既知の）情報を入力７４６からカテゴリ的に分割して、適切なＤＢアナロジークエリを実行することができるようにする。そのような情報は、カテゴリＡ、Ｂ、およびＣ７５０に分割され、その後、別々のカテ

ゴリは、個別に、比較可能可変フォーマットジェネレータ（ＣＶＦＧ）４９１に入力を提供する。次に、ＣＶＦＧは、ＣＶＦ５４７フォーマットのカテゴリ情報を出力し、これは、ストレージ検索（ＳＳ）４８０によって既知データスコープＤＢ７４７において類似性をチェックするために使用される。ＤＢ７４７では、既知のデータの上限がデータカテゴリにしたがって定義される。同様の種別と構造のデータを比較することで、知識の範囲の確信度を評価する。ＳＳ４８０がシナリオ７４８で知識を類推するための結果を見つけることができなかった場合、将来の類推ができるように現在のデータが格納される。このユースケースの例によれば、これは核物理学の範囲を定義することを可能にするインシデントである。その後、量子物理学が将来参照されるとき、現在の核物理学の知識スコープの格納で量子物理学の知識スコープを類推することができる。シナリオ７４９は、ＳＳ４８０の結果にしたがって既知のデータの該当するスコープが各カテゴリにタグ付けされている結果の発見状況を説明している。その後、カテゴリ毎の未知の情報のタグ付けされたスコープは、未知データ合成器（ＵＤＣ）７４４でオリジナルのデータの同じストリーム（入力７４６）に再構築される。出力７４５では、オリジナルの入力データが返されており、未知データのスコープ定義と結合される。図１１９では、既知データカテゴリ化（ＫＤＣ）モジュール７４３がより詳細に示されている。既知データ７５２は主な入力であり、エラーログからの個々のエントリなどのデータの定義されたスコープを表す情報ブロック７５５を含む。ステージ７５６は、ユースケースの通りに、核物理の情報としてラベル付けされているブロック内の認識可能な定義をチェックする。カテゴリホールドアウト７５０のブロックの情報ラベルに適合するカテゴリが存在する場合、既存のカテゴリは、処理された情報ブロック７５５を補足することによって、ステージ７４８で詳細情報とともに強化される。そのようなカテゴリが存在しない場合、ステップ７４９で作成され、情報のブロック７５５がそれに応じて正しく格納されることができる。基本ロジック７５９は、すべてが処理されるまでブロックを順番に循環的に使用する。それらのブロックのすべてが処理された後で、最小限の量（ポリシーによって定義される）もカテゴリホールドアウト７５０に提出されなかった場合、ＫＤＣ７４３はモジュールの出力を空の結果６１８として提出する。十分な量の処理済みブロックがある場合、カテゴリホールドアウト７５０は中間アルゴリズム７５１（主にＳＣＫＤ４９２）に提出される。未知データ合成器（ＵＤＣ）７４４は、未知データポイント７５７でタグ付けされた既知データを中間アルゴリズム７５１から受信する。このようなデータは、最初にカテゴリホールドアウト７５０に格納され、そこから基本ロジック７６０が、データのすべてのユニットを順番に、循環的に使用する。ステージ７５４は、ホールドアウト７５０からの定義されたカテゴリが、別個のカテゴリを一致する情報ストリームに再構築する方法を記述しているリジナルのメタデータを含むかどうかをチェックする。そのようなメタデータは、元々はＫＤＣ７４３から入力された既知データ７５２で見つかった。なぜなら、その段階では、このデータがまだカテゴリに分割されておらず、すべてのデータを保持している、当初の単一の一致する構造が存在していたためである。ステージ７５４がこのメタデータをそれらの対応するデータと再度関連付けした後、タグ付けされたブロックは、ブロック組換ホールドアウト７５３に転送される。ステージ７５４でこのデータと一致するメタデータが見つからない場合、ホールドアウト７５３は必然的に空のままであり、モジュールの空の結果６１８が返される。メタデータの一致に成功すると、ホールドアウト７５３が満たされ、ＵＤＣ７４４のモジュールの出力は、既知データ＋タグ付けされた未知データ７５７である。モジュールの出力のブロック７５５は、ＫＤＣ７４３の既知データ７５２に記載されているオリジナルの情報ブロックを表している。五角形７５８は、既知データ７５５のすべてのブロックと結合されている未知データのスコープ定義を表している。

辞書的客観性探索（ＬＯＭ）

【０１４８】

図１２１は、辞書的客観性探索（ＬＯＭ）のメインロジックを示している。ＬＯＭは、さまざまな質問や表明に対する客観的な回答に可能な限り近づけようとする。ＬＯＭは、ＬＯＭの立場に反してそれら質問や表明の申し立てを認める、あるいは改善するために、人

間である対象８００とかかわり合う。申し立てを認める、あるいは改善することはＬＯＭの中核的態度である。というのは、まさに最初に知識を得るところである、人間が持っている知識から学ぶことができるように、間違っていたことを認めることができなければならないからである。ＬＯＭは極度にデータベース偏重（ＣＰＵ、ＲＡＭ、ディスクはすべて重要なプレーヤーである）であり、単一の（しかし、冗長性とバックアップのために複製される）マスターインスタンスに集中化されている、知識保持中枢（ＣＫＲ）８０６から便宜を受けている。サードパーティ製のアプリケーションは、そのような集中マスターインスタンスに接続する有償または無料のＡＰＩを通じて便宜を得る。ＬＯＭの活動は、メインのＬＯＭビジュアルインタフェースに質問または表明８０１を入力する、人間である対象８００から開始される。このような質問／表明８０１Ａは、知識保持中枢（ＣＫＲ）８０６を活用して質問／表明の理解および回答／応答においてなくてはならない、欠落した詳細情報を解読する初期クエリ推論（ＩＱＲ）８０２に、処理のために転送される。［．．．］その後、質問／表明８０１は、補足的なクエリデータとともに調査の明確化（ＳＣ）８０３Ａに転送される。調査の明確化は、人間である対象８００とかかわることで補足的な情報を得て、質問／表明８０１Ａを客観的かつすべての必要なコンテキストで分析できるようにする。こうして、明確化された質問／表明８０１Ｂが形成される。これは、人間である対象８００によって提起されたオリジナルの未処理の質問／表明８０１を受け取り、ＳＣ８０３Ａを介して人間である対象８００から学習した詳細情報を補足する。表明の構築（ＡＣ）８０８Ａは、（８０１Ｂのような）表明または質問の形式で命題を受け取り、その命題に関連するコンセプトの出力を提供する。回答の提示８０９は、ＬＯＭ（具体的にはＡＣ８０８）によって引き出された結論を、人間である対象８００と合理的訴求（ＲＡ）８１１の両方に提示するためのインタフェースである。このようなインタフェースは、人間８００には理解のために視覚的に提示され、ＲＡ８１１には純粋にデジタルな構文フォーマットで提示される。階層的マッピング（ＨＭ）８０７Ａは、関連するコンセプトをマップして、質問／表明の一貫性において、裏付けまたは競合を発見する。階層的マッピングは次に、話題に一定の立場をとっていることの利点とリスクを計算する。知識保持中枢８０６は、ＬＯＭのために知識を参照するためのメインデータベースである。強力な議論が構築されるように、クエリの効率と論理的な分類とコンセプトの分離に最適化されており、人間である対象８００の批判には負かされる。知識検証（ＫＶ）８０５Ａは、クエリ能力およびＣＫＲ８０６への吸収のために論理的に分割される必要がある、高い確信度および事前批判された知識を受け取る。応答の受け入れ８１０は、ＬＯＭの応答を受け入れるか、批判とともに訴求するかのいずれかを行う、人間である対象８００に与えられた選択肢である。応答が受け入れられた場合、それはＫＶ８０５Ａによって処理され、確認された（高い確信度の）知識としてＣＫＲ８０６に格納できる。人間である対象８００が応答を受け入れなければ、人間８００によって与えられた訴求の理由をチェックして批判する合理的訴求（ＲＡ）８１１Ａに転送される。ＲＡ８１１Ａは、それが自己批判であろうと人間の応答に対する批判であろうと、表明を批判することができる（応答の受け入れ８１０の「ＮＯ」の応答から）。

【０１４９】

図１２２～図１２４は、管理された人工知能的サービスプロバイダ（ＭＡＩＳＰ）を示している。ＭＡＩＳＰは、知識保持中枢（ＣＫＲ）８０６のマスターインスタンスとともに、ＬＯＭのインターネットクラウドインスタンスを実行している。ＭＡＩＳＰ８０４Ａは、ＬＯＭをフロントエンドサービス８６１Ａ、バックエンドサービス８６１Ｂ、サードパーティアプリケーションの依存関係８０４Ｃ、情報源８０４Ｂ、およびＭＮＳＰ９のクラウドに接続する。フロントエンドサービス８６１Ａには、人工知能的パーソナルアシスタント（たとえば、ＡｐｐｌｅのＳｉｒｉ、ＭｉｃｒｏｓｏｆｔのＣｏｒｔａｎａ、ＡｍａｚｏｎのＡｌｅｘａ、ＧｏｏｇｌｅのＡｓｓｉｓｔａｎｔ）、通信アプリケーションおよびプロトコル（たとえば、Ｓｋｙｐｅ、ＷｈａｔｓＡｐｐ）、ホームオートメーション（たとえば、冷蔵庫、ガレージ、ドア、サーモスタット）、医療用途（たとえば、医師のセカンドオピニオン、病歴）がある。バックエンドサービス８６１Ｂには、オンラインショ

ッピング（たとえば、Ａｍａｚｏｎ．ｃｏｍ）、オンライン交通機関（たとえば、Ｕｂｅｒ）、処方箋注文（たとえば、ＣＶＳ）がなどある。そのようなフロントエンドサービス８６１Ａおよびバックエンドサービス８６１Ｂは、情報の転送およびプロトコルの標準化を可能にする、文書化されたＡＰＩインフラストラクチャ８０４Ｆを介してＬＯＭと相互作用する。ＬＯＭは、自動化された調査機構（ＡＲＭ）８０５Ｂを介して外部情報源８０４Ｂから知識を取り出す。

【０１５０】

図１２５～図１２８は、モジュール同士が相互に依存している様子を表すＬＯＭの依存構造を示している。言語学的構築（ＬＣ）８１２Ａは、人間である対象８００および類似したモジュールからの未処理の質問／表明の入力を解釈し、ＬＯＭシステム全体で理解できる言語構文の論理的な分割を生成する。コンセプト発見（ＣＤ）８１３Ａは、明確化された質問／表明８０４内の関心ポイントを受け取り、ＣＫＲ８０６を活用することによって関連するコンセプトを導出する。コンセプトの優先順位付け（ＣＰ）８１４Ａは、該当するコンセプトを受け取り、それらを特定性および一般性を表す論理的な複数の層に整理する。最上位層には最も一般的なコンセプトが割り当てられ、より下位の層にはより特定のコンセプトが割り当てられる。応答分割ロジック（ＲＳＬ）８１５Ａは、ＬＣ８１２Ａを活用することで人間の応答を理解し、適切かつ有効な応答を、最初の明確化リクエストと関連づけ、そうすることでＳＣ８０３Ａの目的を達成する。ＬＣ８１２Ａは、出力フェーズで再活用され、オリジナルの質問／表明８０１を修正し、ＳＣ８０３によって受信された補足的情報を含むようにする。ヒューマンインターフェースモジュール（ＨＩＭ）８１６Ａは、初期クエリ推論（ＩＱＲ）８０２Ａによって特定された知識のギャップに対処するために、明確かつ論理的に分割したプロンプトを、人間である対象８００に提供する。コンテキスト構築（ＣＣ）８１７Ａは、表明の構築（ＡＣ）８０８Ａのメタデータと、人間である対象８００からの潜在的な証拠を使用して、クリティカルシンキングのためにＣＴＭＰに未処理の事実を提供する。決定事項比較（ＤＣ）８１８Ａは、事前批判された決定事項と批判された後の決定事項との間の重複を判断する。コンセプト互換性検出（ＣＣＤ）８１９Ａは、オリジナルの質問／表明８０１からのコンセプト的な派生事項を比較して、論理的な互換性の結果を確認する。そのようなコンセプトは、状況、存在状態、傾向をなど表すことができる。利益／リスク計算（ＢＲＣ）８２０Ａは、ＣＣＤ８１９Ａからの互換性の結果を受け取り、コンセプト構成に暗に含まれた変数の傾斜を包含する一様な決定を形成するために、利益とリスクを重み付けする。コンセプト連携（ＣＩ）８２１Ａは、ＡＣ８０８Ａのコンセプトに関連する属性を、調査の明確化（ＳＣ）８０３Ａを介して、人間である対象８００から収集された情報の一部に割り当てる。

【０１５１】

図１２９および図１３０は、初期クエリ推論（ＩＱＲ）８０２Ａの内部ロジックを示す。言語構成（ＬＣ）８１２Ａは、ＩＱＲ８０２のサブセットとして機能し、人間である対象８００からオリジナルの質問／表明８０１を受信する。質問／表明８０１は言語的に分離されているため、ＩＱＲ８０２Ａは一度に個々の語句を処理する。助動詞「Ｓｈｏｕｌｄ」８２２は、時間次元８２２に関する明快さの欠如を引き起こす。よって、「毎日？」や「毎週？」のなど、明確にするために聞き返す質問が作成される。主語「私」８２３は、対象が誰であるかに関する明確さの欠如を呼び起こし、したがって、後続の質問が形成され、対象８００に提示される。動詞「食べる」８２４は必ずしも不明確ではないが、明瞭性に欠けている他の分析ポイントを補うことができる。ＩＱＲ８０２は、ＣＫＲ８０６のＤＢを活用することで、ステージ８２４で健康と金銭のコンセプトと食べ物のコンセプトを結びつける。このことは、クエリ「主語を問う質問」８２３に通知することで、「男性か女性か？」、「糖尿病？」、「運動？」、「購買力？」などの、より適切で関連性の高い後続の質問がされるようになる。名詞「ファーストフード」８２５は、その言葉をどのように解釈すべきか、という観点から、明確さの欠如を呼び起こす。この名詞は、技術的意味８２７で「非常に早く提供される食べ物」であると解釈されるか、「安くて、注文した場所で手早く作られる、フライされた塩味のような食べ物」という、より口語的な理解

８２６で解釈される。サラダバーは、技術的には、事前に作られてすぐに食べられるような、食べ物を得るための迅速な手段である。しかしこの技術的定義は、「ファーストフード」のより一般的に理解される口語的な理解にしっかり従っている。ＣＫＲ８０６を参照することで、ＩＱＲ８０２は、「ファーストフード」という用語の曖昧性を考慮しながら、可能な選択肢の候補を考慮する。「ハンバーガーショップ？」や「サラダバー？」のような曖昧な選択肢は、ヒューマンインターフェースモジュール（ＨＩＭ）８１６を介して、人間である対象８００に転送できる。しかしながら、質問８０１の一般的な文脈が口語的意味８２６への参照を表すことを理解できるほど、ＣＫＲ８０６に十分な情報があるかもしれない。ファーストフードと健康に関わるレベルの論争があることを次第に学ぶと、ＣＫＲ８０６はこのような一般的な文脈を表現することが可能となる。したがって、質問８０１がこの論争を参照している可能性が高い。よって、人間である対象８００を利用してさらなる明確化を目指すためにＨＩＭ８１６を呼び出す必要はない。したがって、ＩＱＲ８０２は、定義の意味における明確だが微妙なニュアンスを解読しようとする。質問８２８は、ＬＯＭ全体に対して、人間である対象８００が陳述を表明するのではなく、質問をしていることを表している。

【０１５２】

図１３１は、ＩＱＲ８０２からの入力を受け取る、調査の明確化（ＳＣ）８０３を示している。そのような入力には、達成されるべきオリジナルの質問／表明８０１に対する客観的な回答のために、人間の被験者８００が対応する必要のある、一連のリクエストされた明確化事項８３０が含まれる。よって、リクエストされた明確化事項８３０は、ヒューマンインターフェースモジュール（ＨＩＭ）８１６Ｂに転送される。そのような明確化事項に対してなされる対応はどれも、応答分割ロジック（ＲＳＬ）８１５Ａに転送され、その後、対応と明確化リクエストを相関させる。リクエストされた明確化事項８３０と並行して、明確化の言語学的連携８２９が言語学的構築（ＬＣ）８１２Ａに提供される。そのような連携８２９には、リクエストされた明確化事項８３０と言語構造との内部関係が含まれる。これにより、ＲＳＬ８１５Ａは、ＬＣ８１２ＡがＨＩＭ８１６を介して学習された情報が組み込まれた、明確化された質問８０４を出力できるように、オリジナルの質問／表明８０１を修正することができる。

［００］図１３２は、調査の明確化（ＳＣ）８０３によって作成された、明確化された質問／表明８０４を受け取った表明の構築（ＡＣ）８０８を示している。次にＬＣ８１２Ａは、この問題を関心ポイント８３４（キーコンセプト）に分解し、コンセプト発見（ＣＤ）８１３に渡す。次にＣＤは、ＣＫＲ８０６を活用することによって関連するコンセプト８３２を導出する。すると、コンセプトの優先順位付け（ＣＰ）８１４Ａは、コンセプト８３２を、特異性および一般性を表す論理的な複数の層に整理することができる。最上位層には最も一般的なコンセプトが割り当てられ、より下位の層にはより特定のコンセプトが割り当てられる。このような整理は、ＣＫＲ８０６から提供されたデータを用いて容易になった。最上位層は、モジュールの入力として階層的マッピング（ＨＭ）８０７に転送される。情報の並列転送において、ＨＭ８０７は関心ポイント８３４を受信し、この関心ポイントは、その依存モジュールであるコンセプト連携（ＣＩ）８２１によって処理される。ＣＩは、ＣＫＲ８０６で利用可能なインデックス付けされた情報にアクセスすることによって、そのような関心ポイント８３４に属性を割り当てる。ＨＭ８０７が内部プロセスを完了すると、その最終出力は、導出されたコンセプトの互換性がテストされ、ある立場の利益／リスクが重み付けされて返された後、ＡＣ８０８に返される。このことは、ＡＣ８０８およびＨＭ８０７が完結しており、アナリストがコンセプトの複合度を完全に飽和させるまで、そしてＣＫＲ８０６が知識の限界によりボトルネックになるまで（のどちらか早い方）、モジュールの出力を互いに送信し続けるため、モジュールの出力のフィードバックループ８３３と呼ばれる。

【０１５３】

図１３３および図１３４は、階層的マッピング（ＨＭ）８０７がどのように動作するかの内部的詳細を示している。ＡＣ８０８は、ＨＭ８０７に２種類の入力を並行して提供する

。一つはコンセプトの関心ポイント８３４と呼ばれ、もう一つは優先順位付けされたコンセプト８３７（最も一般的なもの）の最上位層である。コンセプト連携（ＣＩ）８２１は、両方の入力を使用して、図１２８にあるように、コンテキスト化された結論を関心ポイント８３４に関連付ける。次に、ＣＩ８２１は、２つのコンセプト同士の互換性／競合レベルを識別する、コンセプト互換性検出（ＣＣＤ）８１９への入力を提供する。これにより、ＨＭ８０７は、人間である対象８００の表明および／または命題と、知識保持中枢（ＣＫＲ）８０６でインデックス付けされた確信度の高い知識との間の一致または不一致の全体的な理解が認められる。このような互換性／競合データは、問題について全体論的な統一された立場を取ることに関する、これらの互換性と競合を利益とリスクに変換するモジュールである、利益／リスク計算（ＢＲＣ）８２０に転送される。たとえば、（人間である対象８００が設定した基準にしたがって）ユースケースごとに３つの主要な立場が浮かび上がる。つまり、ファーストフードは概して推奨されない、ファーストフードは容認できるがそれを強調はしない、ファーストフードは概して推奨されている、の３つである。そのような立場は、リスク／利益ファクタとともに、モジュールの出力８３６としてＡＣ８０８に転送される。これは、ＡＣ８０８がＨＭ８０７によって提唱された表明の拡張を容易にしようとするため、情報のフローが完結する、ＬＯＭ内のいくつかのポイントの一つである。情報フローのループを含むシステムは、知性の傾向が、質問／表明の主観的性質として徐々に補足される、徐々に構築された客観的応答、を表している。一つのアナロジーは、ミツバチは花の蜜を求めるものだが、意図せずその花の花粉を他の花々にまき散らす様子である。この花の受粉により、より多くの花が生み出され、長い目で見れば、それがより多くのミツバチを引き寄せる。これは、ＬＯＭ内で発生し、システムが話題に対する立場についての強い確信を持つに至るまで、表明と成熟したコンセプトを徐々に「受粉」する、相互接続された情報エコシステムに類似している。ＨＭ８０７のサブセットとしての、コンセプト連携（ＣＩ）の内部動作が、図１２８に示されている。ＣＩ８２１は、関心ポイント８３４を受け取り、優先順位付けられたコンセプトの最上位層８３７にしたがって、それぞれの関心ポイント解釈する。この例の、優先順位付けられたコンセプトの最上位層の２つは、「健康」と「予算的制約」である。したがって、ＣＩが関心ポイントを解釈しようとすると、これらの話題のレンズを通過することになる。関心ポイント「糖尿病」８３８は、「予算的制約」８３７に関する「高額な医療」と、「健康」８３７に関する「より脆弱な健康」／「糖不耐症」の表明につながる。関心ポイント「男性」８３９は、「仕事中毒」のなどように、より多くの特異性が必要であることをシステムが発見しているので、「だいだいは時間に追われている」と表明する。時間と金銭との相関関係にシステムが気づいているので、時間の問題は、「予算的制約」に逆につながっている。関心ポイント「中産階級」８４０は、「予算的制約」に関して「より高品質な食品を買う余裕がある」と表明する。関心ポイント「バーガーキング」８４１は、「予算的制約」８３７、に関して「安い」そして「節約」を表明し、「健康」に関しては、「高糖度」と「揚げ物」を表明している。このような表明は、ＣＫＲ８０６に格納された、確立され確信できる知識を参照することによって行われる。

【０１５４】

図１３５および図１３６は、それが自己批判であろうと、人間の応答に対する批判であろうと、表明を批判した、合理的訴求（ＲＡ）８１１の内部の詳細を示している。ＬＣ８１２Ａは、ＲＡ８１１の中核サブコンポーネントとして機能し、２つの潜在的な情報源からの入力を受け取る。一つの情報源は、人間である対象８００がステージ８４２でＬＯＭによって表明された意見を拒絶する場合である。もう一つの情報源は、回答の提示８４３で、ＡＣ８０８によって構築された批判を、ＬＯＭの内部自己批判のためにデジタルで送信する。ＬＣ８Ｉ２Ａが、言語テキストをシステムの残りの部分が理解可能な構文に変換した後、それはＲＳのコアロジック８４４によって処理される。このようなコアロジックが高い確信度の結果８４６を返すと、この結果はＣＫＲ８０６への適切な吸収のために知識検証（ＫＶ）８０５に渡される。コアロジックが低い信頼度の結果８４５を返すと、その結果はＡＣ８０８に渡され、自己批評のサイクル（完結したＬＯＭの別の要素）を継続す

る。コアロジック８４４は、（人工知能の使用に最適な構文を代わりに使用して）言語要素のない事前批判された決定８４７としてＬＣ８１２Ａからの入力を受け取る。そのような決定８４７は、それが入力される「主観的意見」８４８のセクタとしてＣＴＭＰ２２に直接転送される。決定８４７はまた、ＡＣ８０８からのメタデータおよび人間である対象８００からの見込みのある証拠を使用して、未処理の事実（たとえば、システムログ）をＣＴＭＰ２２に、入力する「客観的事実」として与える、コンテキスト構築（ＣＣ）８１７に転送される。ＣＴＭＰ２２が２つの必須入力を受け取ると、このような情報は「客観的意見」８５０に到達する最良の試みを出力するために処理される。このような意見８５０は、ＲＡ８１１内で、批判された後の決定８５１として取り扱われる。事前批判された決定８４７と批判された後の決定８５１の両方が、両方の決定８４７と８５１の間の重複のスコープを決定する決定事項比較（ＤＣ）８１８に転送される。不服申し立ては、次に、真実であると認められる８５２か、この訴求が無効である理由を説明するために、対照的要素が改善される。このような査定は、この訴求が人工知能または人間から来ているかの考慮も偏見もなしに、行われる。シナリオを認める８５２のか改善する８５２のかとは無関係に、高い確信度の結果８４６はＫＶ８０５に渡され、低い確信度８４５の結果はさらなる分析のためにＡＣ８０８に渡される。

【０１５５】

図１３７～図１３８は、ＬＯＭのデータを元にした情報が格納されマージされる場所である、知識保持中枢（ＣＫＲ）の内部詳細を示している。情報の単位は、単位知識フォーマット（ＵＫＦ）に格納される。単位知識フォーマット（ＵＫＦ）には、次の３つの種類がある。ＵＫＦ１　８５５Ａ、ＵＫＦ２　８５５Ｂ、ＵＫＦ３　８５５Ｃである．ＵＫＦ２　８５５Ｂは、ターゲットとなった情報がルール構文形式（ＲＳＦ）５３８に格納されるメインフォーマットであり、値８６５Ｈとして強調されている。インデックス８５６Ｄは、デジタルストレージ、および大量のデータコレクションのリソース効率のよい参照を可能にする互換／不服申し立ての参照点の処理である。このメインの情報ブロックは、ＵＫＦ１　８５５Ａと呼ばれるインデックス８５６Ａを介した別の知識単位への参照であるタイムスタンプ８５６Ｃを参照している。このようなユニットは、ＵＫＦ２　８５５Ｂと同じタイムスタンプ８５６Ｃセクションを保持していないが、値８５６ＨセクタのＲＳＦ５３８フォーマットにタイムスタンプに関する多数の情報を格納している。ルール構文形式（ＲＳＦ）５３８は、参照ルールの追跡を維持するための構文的標準のセットである。ＲＳＦ５３８内の複数のルールの単位を利用して、単一の目的または処置を記述することができる。ＲＳＦは、ＣＴＭＰの内部で直接、頻繁に使用される。ＵＫＦ１　８５５Ａには、ソース属性８５６Ｂのセクタが含まれている。これは、ＵＫＦ３　８５５Ｃインスタンスのインデックス８５６Ｇへの参照である。このような単位ＵＫＦ３　８５５Ｃは、タイムスタンプのセクションを持つが、ソース属性のセクションを持たないＵＫＦ１　８５５Ａとは逆である。これは、ＵＫＦ３　８５５Ｃがソース属性８５６Ｅと８５６Ｂの内容をＲＳＦ５３８の値８５６Ｈのセクタに格納しているためである。ソース属性は、要求された情報源を追跡する複合データの集合である。このような情報源には、ＫＣＡ８１６Ｄで処理されたような、裏付けと否定的な要因による信頼性と真正性のステータスが与えられている。したがって、ＵＫＦクラスタ８５４Ｆは、管轄区域的に分割された情報を定義するためにリンクされたＵＫＦの変種の連鎖で構成されている（時間とソースは動的に定義されている）。要約すれば：ＵＫＦ２　８５５Ｂには、メインのターゲットされた情報が含まれている。ＵＫＦ１　８５５Ａにはタイムスタンプ情報が含まれているため、無限回帰を避けるためにタイムスタンプフィールドそのものは省略されている。ＵＫＦ３　８５５Ｃにはソース属性情報が含まれているため、無限回帰を避けるためにソースフィールドそのものは省略されている。すべてのＵＫＦ２　８５５Ｂには少なくとも１つのＵＫＦ１　８５５Ａと１つのＵＫＦ３　８５５Ｃが添付されていなければならない。さもなければ、クラスタ（シーケンス）は不完全とみなされ、そこにある情報は、ＬＯＭシステム全体の汎用ロジック８５９では処理できない。中央のＵＫＦ２　８５５Ｂ（中心的なターゲットされた情報を持つ）とそれに対応するＵＫＦ１　８５５ＡおよびＵＫＦ３　８５５Ｃの

間には、リンクされた橋の役割を果たすＵＫＦ２　８５５Ｂユニットがある。一連のＵＫＦクラスタ８５４Ｄは、ＫＣＡ８１６Ｄによって処理され、導出された表明８５４Ｂを形成する。同様に、一連のＵＫＦクラスタ８５４ＥはＫＣＡ８１６Ｄによって処理され、導出された表明８５４Ｃを形成する。知識裏付け分析（ＫＣＡ）８１６Ｄは、ＵＫＦのクラスタ化された情報を、意見のあるスタンスに関する証拠を裏付けるために比較する。このアルゴリズムは、帰属元の信頼度、および否定的な証拠（そのような主張がなされた場合）をなど考慮する。よって、ＫＣＡ８１６Ｄの処理が完了した後、ＣＫＲ８０６は、話題についての結論となる、独断的な立場を出力することができる。偽であると判断された情報であっても、将来、真実か嘘かを区別するのに役立つ可能性がある、ＣＫＲ８０６は情報を削除しない。したがって、ＣＫＲ８０６は、ＣＫＲ８０６の無制限に成長するデータセットを処理しスケーリングすることができる、高度なストレージ容量サービス８５４Ｇから実行される。

【０１５６】

図１３９は、ＬＯＭの全体的な見積もりと意思決定能力を拡張するために、ＣＫＲ８０６に新しい知識を絶え間なく提供しようとする、自動化された調査機構（ＡＲＭ）８０５Ｂを示している。ユーザ活動８５７Ａで表されるように、ユーザがＬＯＭと対話するとき（利用可能なフロントエンドを介して）、コンセプトは質問／表明に対する回答／応答に関連して直接的または間接的にもたらされる。ユーザ活動８５７Ａは、リクエストされたがまだ利用不可能なコンセプトのリスト８５７Ｂに示されるように、ＣＫＲ８０６が、それに関する情報がほとんど全くないコンセプトを最終的に生み出すことが期待される。コンセプトのソートおよび優先順位付け（ＣＳＰ）８２１Ｂでは、コンセプトの定義は、３つの独立したソースから受信され、情報リクエスト（ＩＲ）８１２Ｂのリソース（帯域幅など）に優先順位付けをするために集約される。そのようなモジュールＩＲ８１２Ｂは、具体的に定義された情報を得るために、該当するソースにアクセスする。このような情報は、コンセプトの種別によって定義される。このような情報源は、パブリックニュースソース８５７Ｃ（ロイター、ニューヨークタイムズ、ワシントンポストのなど公開ニュース記事）、パブリックデータアーカイブ８５７Ｄ（ウィキペディア、クオーラのなど情報収集コレクション）、ソーシャルメディア８５７Ｅ（フェイスブック、ツイッターフィードなど）。そのような情報源によって提供されたデータは、それらをリクエストしたコンセプトの定義にしたがって情報アグリゲータ（ＩＡ）８２１Ｂで受信され、解析される。検索時刻、検索元のなど、該当するメタデータが保持される。その後、情報は相互参照分析（ＣＲＡ）８１４Ｂに送られ、そこでは、受信された情報がＣＫＲ８０６からの既存の知識と比較され、それを考慮して構築される。これにより、ＣＫＲ８０６が現在何を知っていて何を知らないかにしたがって、新しく来た情報を評価し、検証することが可能になる。文体計量学的スキャニング（ＳＳ）８０８Ｂは、ＣＲＡ８１４Ｂが文体計量学的シグネチャを考慮して、ＣＫＲ８０６からの既存の知識を用いて新しい情報を吸収することを可能にする、補助モジュールである。欠落した依存コンセプト８５７Ｆは、当初のターゲットコンセプトを理解するための基盤として理解されることが論理的に要求されるコンセプトである。（たとえば、トラックがどのように動くかを理解するためには、まずディーゼルエンジンの動作について調査し、理解しなければならない）。このような欠落したコンセプトは、処理のためにＣＳＰ８２１Ｂに転送される。アクティブコンセプト８５７Ｇのリストは、ＣＫＲ８０６で最もアクティブなものとして格付けされた、人気のある話題である。このようなコンセプト８５７Ｇは、クリエイティブコンセプトジェネレータ（ＣＣＧ）８２０Ｂに転送され、（創作モジュール１８を介して）クリエイティブにマッチングされ、新しい潜在的コンセプトを生成する。このメカニズムは、これらの混合物のうちの１つがＩＲ８１２Ｂに接続されたソース８５７Ｃ、８５７Ｄ、８５７Ｅからの新しい範囲の情報をもたらす可能性に依存している。

文体計量学の使用例：

新しい外部データ８５８Ａは、既知のＣＮＮリポーターから来たとマークされる。しかし、軍事シンクタンクの署名と非常に強い文体計量学的一致が見つかる。したがって、その

コンテンツはＣＫＲ８０６の中で主として軍事シンクタンクに帰属し、ＣＮＮからのものであると「主張している」と注記した。これにより、さらに、ＬＯＭロジックを後で実行するため（たとえば、今後、ＣＮＮから来たコンテンツであるとの主張を怪しむ）のパターンマッチングおよび共謀検知が可能となる。表明の裏付け、競合、偏見の評価は、その後、このコンテンツがシンクタンクのものであり、ＣＮＮのものではないかのように、査定される。

【０１５７】

図１４０は、（システムがまださらされていない）新しい外来コンテンツの文体計量学的シグネチャ８５８Ｃを分析する文体計量学的スキャニング（ＳＳ）８０８を示している。文体計量学は、あるライターやジャンルと他のものとの間の文学スタイルのバリエーションを統計分析するものである。これは、データ／表明のソースの期待を追跡する上でＣＫＲ８０６に役立ち、ＬＯＭが裏付け表明を検出するのにさらに役立つ。シグネチャ結論（ＳＣ）８１９Ｂの新外部データ８５８Ａのコンテンツソース帰属は、文体計量学的シグネチャ８５８Ｃの重要な一致の影響を受ける。文体計量学的一致が強いほど、文体計量学によるソース属性が強くなる。シグネチャ照会（ＳＱ）８０７Ｂでは、文体計量学的シグネチャ８５８Ｃは、ＳＩ８１３Ｂからのすべての既知のシグネチャと照合される。重要な傾斜のあらゆる一致が記録される。シグネチャインデックス（ＳＩ）８１３Ｂは、ＣＫＲ８０６から検索されたすべての既知の文体計量学的シグネチャ８５８Ｃのリストを表している。サードパーティの文体計量学アルゴリズム８５８Ｂに代表されるように、ＬＯＭは正当に選択された高度かつ有効なアルゴリズム、文体計量学アルゴリズムに依存する。

【０１５８】

図１４１は、表明または質問の形式で命題を受け取り、その命題に関連するコンセプトの出力を提供する、仮定上書きシステム（ＡＯＳ）８１５Ｂを示している。コンセプト定義マッチング（ＣＤＭ）８０３Ｂは、人間である対象８００によって提供される、任意のハードコーティングされた仮定８５８Ｄが、依存性解釈（ＤＩ）８１６Ｂモジュールに対して照会される場所である。すべてのそのようなコンセプトは、違反の懸念のために倫理的・守秘的・合法的（ＥＰＬ）８１１Ｂによってチェックされる。依存性解釈（ＤＩ）８１６Ｂモジュールでは、要求されたデータの所与の応答を満たす知識ベースの依存関係すべてがアクセスされる。このようにして、客観的な意見に基づく、情報の完全な「木」が検索される。要求されたデータ８５８Ｅは、ＬＯＭシステム全体にわたる汎用ロジック８５９が要求したデータである。特定のクエリは、正確にマークされた情報のセットを探す。条件付きクエリは、特定の条件に一致する、すべての情報をリクエストする。

【０１５９】

図１４２は、知的情報および構成管理（I^2CM）８０４Ｅならびに管理コンソール８０４Ｄを示している。アグリゲーション８６０Ａを参照すると、多数のプラットフォームから情報ストリームがマージされ、タグ付けされつつ、汎用のレベル判定基準を使用して、不必要で冗長な情報が遮断されている。脅威のジレンマ管理８６０Ｂは、コンセプト上のデータの危険性が俯瞰図から知覚される場所である。このような脅威は、グラフィカルに表現するために、管理コンソールに渡される。脅威の仕組みに関連する、計算された測定値が、最終的に多数のプラットフォームからマージされているので、より多くの情報を得た状態で、脅威を管理する上での判断が自動的に実行される。自動化制御８６０Ｃは、ＭＮＳＰ９、信用プラットフォーム８６０Ｑ、サードパーティサービス８６０Ｒの管理に関する制御を行うことにアルゴリズムがアクセスすることを表している。管理フィードバック制御８６０Ｄは、ポリシー作成、科学捜査、脅威の調査をなど容易にするために使用できる、すべてのＭＮＳＰ９クラウド、信用プラットフォーム（ＴＰ）８６０Ｑ、追加のサードパーティサービス８６０Ｒに基づくサービスの、ハイレベルな制御を提供している。このような管理制御８６０Ｄは最終的に、カスタマイズ可能な適切な画像と効率的なプレゼンテーションとともに、管理コンソール（ＭＣ）８０４Ｄ上に明示される。これによって、必要に応じて拡大して詳細を見ることのできる単一のインタフェースから直接、システム（ＭＮＳＰ、ＴＰ、３ＰＩ）全体が効率的に制御・操作可能になっている。手動制御

８６０Ｅは、ＭＮＳＰ９、信用プラットフォーム８６０Ｑ、サードパーティサービス８６０Ｒの管理に関する制御を行うことに人間がアクセスするためにある。知的文脈化８６０Ｆステージでは、残ったデータはこの時点では一群の島々のように見え、それぞれの島は、コンセプト上のデータの危険性である。コンセプト分析の熟達のために、各プラットフォーム間で相互関係が結ばれる。脅威パターンを読み解くため、（ＬＩＺＡＲＤとは対照的に、I^2ＧＥ２１から）履歴データがアクセスされ、ＣＴＭＰ２２が、クリティカルシンキング分析のために使用される。設定および導入サービス８６０Ｇは、新たな企業の資産（コンピュータ、ノートパソコン、携帯電話）を、正しいコンセプト上のデータの設定と通信設定で導入するためのインタフェースである。あるデバイスが追加され設定が行われた後、セキュリティ設定と通信設定は、管理フィードバック制御８６０Ｄを仲立ちにして、管理コンソール（ＭＣ）８０４Ｄを通じて微調整される。設定および導入サービスは、新たな顧客／クライアントのユーザアカウントの導入も管理している。この導入は、ハードウェアとユーザアカウント、インタフェースのカスタマイズ、顧客／クライアント変数（たとえば、ビジネスタイプ、製品タイプなど）のリストとの関連付けを含んでもよい。管轄範囲による分割８６０Ｈでは、タグ付けされた情報の集積が、ＭＣ８０４Ｄのユーザに該当する管轄範囲にしたがって、排他的に分割される。脅威による分割８６０Ｉによって、情報が個々の脅威（たとえば、コンセプト上のデータの危険性）にしたがって整理される。あらゆる型のデータは、ある脅威と関係付けられて多少の情報が追加されるか、あるいは削除される。ダイレクトマネジメント８６０Ｊは、ＭＣ８０４Ｄのユーザが手動制御８６０Ｅを介して管理フィードバック制御８６０Ｄに接続するためのインタフェースである。カテゴリおよび管轄範囲８６０Ｈでは、管理コンソールＭＣ８０４Ｄのユーザは、自分の管轄範囲および情報カテゴリアクセス権のスコープを定義したログイン認証情報を使用する。すべてのデータベクタの候補８６０Ｌは、移動中のデータ、休止中のデータ、および使用中のデータですべてである。カスタマイズ可能な画像８６０Ｍは、企業のさまざまな部署（経理、金融、人事、ＩＴ、法務、セキュリティ／総括監察官、プライバシー／情報公開、労働組合など）および当事者（それぞれの部署のスタッフ、管理職、幹部）、ならびにサードパーティパートナー、法執行機関のなどためのものである。コンセプト上データの全側面に関する統合ビュー８６０Ｎは、周辺、企業、データセンター、クラウド、リムーバブルメディア、モバイル機器をなど表している。統合単一ビュー８６０Ｏは、監視、ログ採取、報告、イベントの関係付け、アラート処理、ポリシー／ルールセット生成、修正処置、アルゴリズム調整、サービスプロビジョニング（新規顧客／変更）、信用プラットフォームの利用、ならびに、サードパーティサービス（サードパーティサービスプロバイダおよびサードパーティサービスベンダをからのレポートおよびアラート／ログをなど受信することを含む）など、すべての機能の候補に関する、単一のビューである。コンセプト上のデータのチーム８６０Ｐは、多数のシステムの活動および状況を全体にわたってモニターする、資格を有する専門家のチームである。知的情報処理およびＡＩによる判断が行われていることから、経験年数の少ない人員を少人数だけ雇うことができ、コストを下げることが可能である。このチームの第一の目的は、大量の分析ポイントを処理しつつ、システムが所望の判断基準にしたがって発達し向上していることを検証することにおいて、万一の時に頼りになるものとなることである。

【０１６０】

図１４３は、多数の潜在的なエンドポイントおよびフロントエンドを介して個々人の個人情報が格納される場所である、個人情報プロファイル（ＰＩＰ）８０２Ｃを示している。個々人の情報は、非常に安全であり、ＣＫＲ８０６からは隔離されているが、ＬＯＭシステム全体にわたる汎用ロジック８５９では、高度にパーソナライズされた意思決定を行うために使用可能である。個人認証および暗号化（ＰＡＥ）８０３Ｃを実装することで、着信データリクエストは、まず個人情報が正しいユーザによってアクセスされることを保証するために、このリクエスト自体を認証する必要がある。人工知能アプリケーションに関する個人情報は暗号化され、ＵＫＦフォーマットのパーソナルＵＫＦクラスタプール８１５Ｃに格納される。情報匿名化プロセス（ＩＡＰ）８１６Ｃでは、情報は、個人を特定可

能な情報が取り除かれた後、ＣＫＲ８０６に補充される。このような個人情報がデータストリームから取り除かれた後であっても、ＩＡＰ８１６Ｃは、個人の身元を知るために（科学捜査の詳細な調査ように）リバースエンジニアリングできるかもしれない過剰な量の並列データが提供されることを防止しようとする。相互参照分析（ＣＲＡ）８１４Ｂでは、受信した情報は、ＣＫＲ８０６からの既存の知識と比較され、それを考慮して構築される。これにより、ＣＫＲ８０６が現在何を知っていて何を知らないかにしたがって、新しく来た情報を評価し、検証することが可能になる。どのようなデータリクエスト情報も、常にＣＫＲ８０６からアクセスされる。データリクエストに個人的判断基準がある場合、個人データと一般データのマージ（ＰＧＤＭ）８１３Ｃを介してＰＩＰ８０２Ｃが参照され、ＰＩＰ８０２ＣがメインのＣＫＲ８０６の知識を基盤として構築される。

【０１６１】

図１４４は、日常生活でのルーチンや単発の出来事のためのタスクを自動化する一体化プラットフォーム上で、様々なインターネット対応の機器およびサービスを接続する、生活の管理と自動化（ＬＡＡ）８１２Ｄを示している。積極的意思決定（ＡＤＭ）８１３Ｄは、ＬＡＡ８１２Ｄの中枢ロジックであり、フロントエンドサービス８６１Ａ、バックエンドサービス８６１Ｂ、ＩｏＴデバイス８６２Ａの可用性と機能性を考慮し、ＦＡＲＭ８１４Ｄに従って利用可能な支出ルールと金額を考慮している。資金充当ルールと管理（ＦＡＲＭ）８１４Ｄでは、人間がこのモジュールに対する判断基準、制限、およびスコープを手作業で定義して、ＡＤＭ８１３Ｄの活動の管轄範囲がどこまでかということについて、ＡＤＭ８１３Ｄに知らせる。人間である対象８００は、暗号通貨での資金（たとえば、Ｂｉｔｃｏｉｎ）をデジタルウォレット８６１Ｃに手作業で預け、それにより、ＬＡＡ８１２Ｄが費やすことができる金額の上限を示す。ＩｏＴ連携モジュール（ＩＩＭ）８１５Ｄは、どのＩｏＴデバイス８６２Ａが人間に利用可能であるかについてのデータベースを維持管理する。ＩｏＴデバイス８６２Ａの安全な制御８６２Ｃを可能にするために、認証キーおよび認証メカニズムがこのデータベースに格納される。製品のメーカー／開発者８６１Ｆは、プログラム可能なＡＰＩ（アプリケーション・プログラミング・インタフェース）のエンドポイントを、ＩｏＴ製品連携プログラミング８６１Ｅとして、ＬＡＡ８１２Ｄに提供する。このようなエンドポイントは、特にＩｏＴ連携モジュール（ＩＩＭ）８１５Ｄによって使用される。データフィード８６２Ｂは、知的で自動化された動作が実行できるように、ＩｏＴ対応デバイス８６２ＡがＬＡＡ８１２Ｄに情報を送信するときを表す。例：温度を報告するサーモスタット、ミルクのストックを報告する冷蔵庫。デバイス制御８６２Ｃは、ＩｏＴ対応デバイス８６２Ａが、実行すべき動作について、ＬＡＡ８１２Ｄから命令を受信するときを表す。例：エアコンの電源を入れる、宅配便のために門を開く、など。フロントエンドサービス８６１Ａのカテゴリには、以下のものがあり得る

・人工知能パーソナルアシスタント
・通信アプリケーションおよびプロトコル
・ホームオートメーション
・医療インタフェース
・配送追跡サービス

バックエンドサービス８６１Ｂの例としては、以下のものがある

・Ａｍａｚｏｎのオンライン注文
・Ｕｂｅｒ／交通手段
・処方箋

ＬＡＡ８１２Ｄの機能性を例示する、全体的なユースケースの例は次のとおりである。ＩｏＴ対応の冷蔵庫が、牛乳がなくなりそうであることを検出する。ＬＯＭは感情的知性を介して、高脂肪牛乳を飲まないと対象者の気分がよりマイナスになる傾向があると分析する。対象者の生活の状況についてのリスクと利益を評価したＬＯＭは、オンラインデリバリーサービス（たとえば、アマゾン）から高脂肪牛乳を注文する。ＬＯＭは追跡番号により牛乳の出荷を追跡していて、家の正面玄関を開け、家の敷地内まで配送できるようにする。配達人が去ると、ＬＯＭはゲートを閉める。配達人が悪意のある行為者である場合

にはセキュリティ的に用心深くなる。その後、巧妙な機能を備えた車輪付きの簡易なロボットが牛乳を取って冷蔵庫に入れ、冷やして傷まないようにする。

【０１６２】

図１４５は、ユーザからの、個人を識別可能なデータのリクエストをモニターすることで、非倫理的および／または違法な物質の有無をチェックする挙動監視（ＢＭ）８１９Ｃを示す。メタデータ集約（ＭＤＡ）８１２Ｃでは、ユーザ関連データが外部サービスから集約され、ユーザのデジタル上の身元（たとえば、ＩＰアドレス、ＭＡＣアドレスなど）を明らかにすることができる。このような情報は、帰納８２０Ｃ／演繹８２１Ｃ、最終的にはＰＣＤ８０７Ｃに転送され、そこでは洗練された分析がＭＮＳＰ９からの裏付けファクタを用いて実行される。例：フロントエンドとしてショッピングポータルａｍａｚｏｎ．ｃｏｍと接続するユーザは、セキュリティの目的で、自身のＩＰアドレスをＬＯＭの挙動監視（ＢＭ）８１９Ｃに転送する。ＰＩＰ８０２Ｃが宛先である、認証済みのユーザからのすべての情報は、情報トラッキング（ＩＴ）８１８Ｃを通過し、挙動ブラックリスト８６４Ａに照らしてチェックされる。例：ユーザが、硫黄の化学的組成について質問する。ブラックリスト８６３Ｂからの要素と（部分的または完全に）一致する情報が、ＩＴ８１８Ｃから帰納８２０Ｃおよび演繹８２１Ｃに転送される。未然犯罪検知（ＰＣＤ）８０７Ｃでは、未然犯罪の結論を出すために、演繹的情報および帰納的情報がマージされ分析される。相当な量の裏付けが検出された場合、このユーザについての犯罪に関する情報と既知の身元が、法執行機関当局に転送される。ＰＣＤ８０７Ｃは、挙動ブラックリスト８６４Ａを直接参照するＣＴＭＰ２２を利用することで、帰納８２０Ｃおよび演繹８２１Ｃによって生成された立場を検証する。ブラックリスト管理機関（ＢＭＡ）８１７Ｄは、ＭＮＳＰ９のクラウドサービスフレームワーク内で稼働する。ＢＭＡ８１７Ｄは、犯罪を防止し犯罪者を捕えるために、ユーザの監視を必要とする危険なコンセプトを定義する挙動ブラックリスト８６４Ａを発行、維持管理する。ＢＭＡ８６４Ｂまた、機密資料がＬＯＭによるクエリ結果として提出されることが決してないように、その機密資料にフラグを立てるＥＰＬ（倫理的・守秘的・合法的）のブラックリスト８６４Ｂを発行、維持管理する。そのような機密資料には、漏洩した文書、個人情報（たとえば、社会保障番号、パスポート番号など）が含まれている可能性がある。ＢＭＡ８６４Ｂは、倫理、プライバシー、および法律に関連する準拠法およびポリシー（たとえば、サイバーセキュリティポリシー、受入れ可能使用方針、ＨＩＰＡＡ（米国における医療保険の相互運用性と説明責任に関する法令）、ＰＩＩ（個人情報）など）を解釈する。このブラックリストは、通常、トリガコンセプトから構成されており、トリガコンセプトとは、ユーザがそのようなコンセプトに過度に関わっている場合に、そのユーザを疑わしいとみなすものである。このブラックリストはまた、指名手配リストのように、特定の個人および／または組織をターゲットにすることもできる。将来の犯罪予防は、裏付けファクタがＭＮＳＰ９で検証された状態で、ＢＭ８１９Ｃ内で行われる。法執行機関当局８６４Ｃは、ＭＮＳＰ９クラウドを介してＢＭＡ８１７Ｄに接続することで、ブラックリストに掲載されたコンセプトに関する入力を提供し、ＢＭ８１９ＣのＰＣＤ８０７Ｃの犯罪検出結果からの入力を受け取ることができる。挙動監視情報裏付け８６４Ｄは、ＭＮＳＰ９がＢＭ８１９Ｃに挙動監視情報を提出して裏付けを行うことを可能にする。倫理的・守秘的・合法的（ＥＰＬ）８１１Ｂは、ＭＮＳＰからのカスタマイズされたブラックリストを受信し、ＡＯＳ８１５Ｂを使用することで、非倫理的、プライバシーに抵触する、および／または違法な内容を含むいかなる表明もブロックする。

【０１６３】

図１４６は、ＭＮＳＰからのカスタマイズされたブラックリストを受信し、ＡＯＳ８１５Ｂを使用することで、非倫理的、プライバシーに抵触する、および／または違法な内容を含むいかなる表明もブロックする、倫理的・守秘的・合法的（ＥＰＬ）８１１Ｂを示している。ＭＮＳＰ９は、トロイの木馬、ウイルスなどによるハッキングの試みのような、従来からあるセキュリティ脅威に対処するために使用する。ＬＯＭのＢＭモジュール８１９ＣおよびＥＰＬモジュール８１１Ｂは、倫理、プライバシーおよび法的な影響を判断する

ために、帰納８２０Ｃおよび演繹８２１Ｃによりコンセプトデータに関するコンテキストを分析する。

【０１６４】

図１４７は、ＬＩＺＡＲＤアルゴリズムの概要を示している。ダイナミックシェル（ＤＳ）８６５Ａは、イテレーションを通じた変化を最も受けやすい、ＬＩＺＡＲＤのレイヤである。自身の目的を達成するために大きな計算量を必要とするモジュールは、通常、ダイナミックシェルに属する。というのも、これらのモジュールは、プログラマのチームが扱える計算量のレベルを凌駕することが考えられるからである。構文モジュール（ＳＭ）８６５Ｂが、コンピュータコードを読み書きするためのフレームワークを提供している。書き込みでは、構文モジュールは、ＰＭ（目標モジュール）から複合フォーマットの目標を受信し、コードを任意のコードの構文で書き込み、それによって、ヘルパ機能がこの任意のコードを（所望の言語に依存して）実際の実行可能コードへと翻訳できる。読み込みでは、構文モジュールは、ＰＭ８６５Ｅが、このようなコードの機能性の目標を導出できるよう、このコードの構文解釈を提供する。ＬＩＺＡＲＤが行った判断の確信度が低い場合、ＬＩＺＡＲＤは、今後のＬＩＺＡＲＤのバージョンを改善するために、該当するデータをデータ返送中継（ＤＲＲ）８６５Ｃ経由でＡＣＴ８６６に中継する。ＬＩＺＡＲＤ自身は、意志決定のためのデータに直接は依存していないが、進化する脅威に関するデータが、ＬＩＺＡＲＤの将来のバージョンが行うかもしれない演繹的な決定に、間接的に寄与できる。疑似コンセプト脅威（ＡＣＴ）８６６は、イテレーションプロセスを実行可能にするために、シミュレートされたコンセプト上のデータの危険性を伴う仮想テスト環境を生成する。ＡＣＴ８６６の疑似的な進化は、悪意のあるコンセプト形態の自然な進化の先を行くほど十分に行われる。イテレーションモジュール（ＩＭ）８６５Ｄは、ＳＣ８６５Ｆを使用することで、「決定されたゴール」に定義された目標およびＤＲＲ８６５Ｃからのデータにしたがって、ＤＳ８６５Ａのコードベースを構文的に変更する。この改変バージョンのＬＩＺＡＲＤは、ＡＣＴ８６６によって、多数のさまざまなコンセプト上のデータの危険性のシナリオのもとで（並行して）ストレステストを受ける。最も成功したバージョンが、実稼働バージョンとして採用される。目標モジュール（ＰＭ）８６５Ｅは、ＳＭ８６５Ｂを用いることでコードから目標を導出し、このような目標を、自身の「複合目標フォーマット」に出力する。この目標は、ＳＭ８６５Ｂによって解釈されたままのコードブロックの、意図された機能性を十分に記述している（たとえこのコードが、データ内に密かに埋め込まれていても）。静的コア（ＳＣ）８６５Ｆは、自動化されたイテレーションによる変化を最も受けにくく、その代わりに人間のプログラマによって直接変更される、ＬＩＺＡＲＤのレイヤである。特に、最も内側の濃い色の四角形は、自動化されたイテレーションの影響を全く受けない。この最も内側のレイヤは、ＬＩＺＡＲＤの方向と全体的な能力を差配する、樹木の根のようなものである。

【０１６５】

図１４８は、さまざまな危険に適応するにつれて、静的ルール群が成熟する様子を説明する、（I^2ＧＥ２１のサブセットである）反復型知的成長を示している。連続する世代のルールセットが作成され、これらルールセットの進化は、「パーソナリティ」トレイトの定義を通じて行われる。このようなルールセットは、入力されたコンセプトデータフィードを処理し、最も望ましい通知および修正処置を行うために使用される。進化系統８６７Ａは、一貫した「パーソナリティ」を有する複数の世代の連鎖の全体である。ＣＰＵ時間が進むにつれ、世代は次第に動的になる。初期の静的ルールセットは通用しなくなり、場合によっては消去されたり上書きされたりする。例：進化系統Ａは、厳密で予防的なトレイトを有し、このトレイトは、寛容さまたは許容範囲がほとんどない仮定を有する。コンセプト挙動８６７Ｂは、コンセプトデータアナリストの挙動が処理され、それらから進化系統８６７Ａが学習できるように格納される場所である。例：系統Ａは、特定の状況と「日和見的」パーソナリティ型に一致したコンセプト上のデータの危険性に対する多数の反応を見つけた。すると、系統Ａはそのような挙動を模倣するルールを生成する。人間８６７Ｃは、進化の連鎖を開始するために初期ルールセットを生成する、コンセプトデータア

ナリストを表している。例：闇市場でプルトニウムを購入することに関わるコンセプトは、すべてブロックするという規則が定義されている。系統パーソナリティ８６７Ｄは、コンセプト上のデータの危険トリガに対して働くべき反応的性質を定義する、変数の集合である。

【０１６６】

図１４９～図１５０は、並行する複数の進化系統８６７Ａが発達し選択される手法である、（Ｉ^{2}ＧＥ２１のサブセットである）反復的進化を示している。イテレートされた世代が、同じＡＣＴ８６６に適応し、最良のパーソナリティトレイトを有する系統が、最終的にはこのコンセプト脅威に対して最も良く耐えることになる。ＣＰＵ時間８６８Ａは、時間に対するＣＰＵパワーの計測値であり、ＣＰＵサイクル数／秒で計測される。１個の進化系統のための処理負荷量を、時間だけで測定するのは十分ではなく、コア数および各ＣＰＵのパワーが考慮されなくてはならない。例：ペンティアムＩＩＩでは千年かかる要求の処理が、ハスウェルプロセッサでは３０分で済むかもしれない。仮想的隔離８６８Ｂを使用することにより、すべての進化系統は、仮想的に隔離されており、それぞれのバージョンが、それら自身のパーソナリティの判定基準からのみに基づいていることを保証している。例：系統Ｂは、系統Ｃが困難なコンセプトデータ問題を解決したことを全く知らず、自分自身のパーソナリティトレイトおよび学習データに依存してソリューションを求めなければならない。いくつかの系統は、コンセプトデータの危険を認識できないという不定状態に達しているので、破棄される８６８Ｃことがある。最も可能性が高い結論としては、パーソナリティを変更して新たな系統を生成しなければならないというものである。例：系統Ｄは、１００ＣＰＵ時間８６８Ａ単位の間、コンセプト上のデータの危険を認識できなかった。したがって、この系統全体を破棄した。監視／連携システム８６８Ｄは、ＡＣＴ８６６のシステムからコンセプト上のデータの危険トリガを投入し、コンセプト挙動クラウド（すべてが固有のパーソナリティトレイトに従っている）から、関連するコンセプト上のデータの危険の応答を中継するプラットフォームである。例：この監視システムが、世代１２を組み上げるのに必要なコンセプト上のデータの危険の応答を、系統Ｂに提供した。疑似コンセプト脅威（ＡＣＴ）８６６は、安定したコンセプト上のデータの危険の環境を提供する、隔離されたシステムである。疑似コンセプト脅威は、システムにコンセプトデータの応答およびトレイトの種々の候補を認識させる練習および訓練をさせるためのコンセプト認識訓練を、アナリストに提供する。例：ＡＣＴは、人間にとって危険であると認識される、一連の複雑なコンセプトを提供した。それは、「家庭用原料を使ってサリンガスを化学的に合成する」といったものである。実コンセプト脅威（ＲＣＴ）８６９Ａは、コンセプトシナリオ８６９Ｃに、実際のデータログから実際の脅威を提供する。人間８６７Ｃは監視／連携システム８６８Ｄに直接命令８６９Ｂを与える。例：手動で系統を中止させる、系統パーソナリティのマスター変数を変更する、相など互参照モジュール８６９Ｄは、コンセプト上の危険８６９Ｃと、コンセプトアナリスト８６７Ｃによる応答８６９Ｅとの間を分析的につなげるものである。意味のある処置を抽出した後、相互参照モジュールはこの処置をトレイトタグ付けモジュール８６９Ｆに送る。コンセプト上の危険８６９Ｃは、実際の危険８６９Ａまたは訓練８６６のいずれかから起こる可能性がある。トレイトタグ付けモジュール８６９Ｆは、パーソナリティ型にしたがってすべての挙動を区分する。例：このコンセプトデータアナリスト８６７Ｃが、自殺の方法について過度に言及しているメールに危険であるとのフラグを立てた８６９Ｅ場合、トレイトタグ付けモジュールは、このアナリストが、過去の複数のイベントにおいて挙動が共通しているが、自称用心深い人物でもあるので。この行為に対して予防的パーソナリティであるというフラグを立てる。トレイト連携モジュール８６９Ｇは、種々のパーソナリティ間の相関を分析する。この情報は、コンセプト挙動８６７Ｂを渡され、その後、監視／連携システム８６８Ｄおよび各系統自身に渡される。例：非寛容パーソナリティおよび現実的パーソナリティは、使用される状況に共通するところが多く、同一のイベントに対しては、同様の反応を返す。しかし、厳格パーソナリティおよび楽観的パーソナリティは、同じイベントに同様の応答をすることはほとんどない。

【０１６７】
図１５１～図１５４は、従前の入力形状から新しいハイブリッド形状を生成する知的アルゴリズムである、創作モジュール１８を示している。創作モジュール１８は、多数のアルゴリズムにサービスを行うプラグインモジュールとして使用される。参照符号８７０Ａでは、２つの親形状（前形状）がインテリジェントセレクタに送られ、ハイブリッド形状８７０Ｂが生成される。これらの親形状は、データの抽象的な構造を表すことができる。例：形状Ａは、コンセプトＤＢによって導出される危険なコンセプトの平均的なモデルを表している。形状Ｂは、危険なコンセプトに対してどのように反応したかに関するコンセプトトリガルールセットによりリリースされた、新たな情報を表している。形状Ｂにある情報によって、生成されたハイブリッド形状は、形状Ａが表しているものより危険なコンセプトとすることができる。インテリジェントセレクタ８７０Ｂのアルゴリズムは、新たな特徴を選択し、ハイブリッド形状にマージする。例：形状Ａは、コンセプトＤＢによって導出されるコンセプト上のデータの危険の平均的なモデルを表している。形状Ｂは、従前のコンセプト上の危険に対してどのように反応したかに関するコンセプトルールセットによりリリースされた、新たな情報を表している。形状Ｂにある情報によって、生成されたハイブリッド形状は、形状Ａが表しているものより優れたコンセプト上の危険のトリガとすることができる。モード８７０Ｃは、創作モジュール１８が使用されているアルゴリズムの型を定義している。このように、インテリジェントセレクタ８７０Ｂは、使用されているアプリケーションに応じて、どの部分がマージするのに適切かを知っている。例：モードがＡＣＴ８６６と設定されているので、インテリジェントセレクタ８７０Ｂは、予期された入力データが危険ＤＢの表現形式（形状Ａ）のものであり、また、コンセプト上の危険のトリガ（形状Ｂ）に対するルールセットの反応を詳細に記述している、新しくリリースされた情報のものであることを知っている。属性モード８７０Ｃは、効果的なハイブリッド形状を生成するためには、新しいデータを古いデータにどのようにマージするのが最良なのかに関する、詳細な方法を定義している。形状がどのようにマージされるべきかに関する、汎用のカスタマイゼーションを提供する静的判断基準８７０Ｄが、コンセプトデータアナリストによって与えられている。このようなデータは、格付けの優先順位付け、所望のデータ比、および、どのモード８７０Ｃが選択されているかに応じて行われるマージを差配するデータを含み得る。例：このモード８７０ＣがＡＣＴ８６６として選択されたとすると、ある危険トリガが失敗した場合、それによって得られる結果は、このようなトリガの構成を大幅に変化させるため、危険トリガＤＢに多大な影響を与えるべきである。もし変更後においてもこのトリガが失敗し続ける場合は、このトリガを完全に放棄する。入力された双方の形状に対して、未処理データ比較８７１Ｂが、コンセプトデータアナリスト８６７Ｃによって与えられた静的判断基準８７０Ｄに応じて実行される。生データ比較が実行された結果、静的判断基準８７０Ｄにより、これらの形状の大部分が互換可能であることがわかった。唯一の相違点は、形状Ａが、静的基準によって「外来」であるとフラグを立てられた応答を含んでいることであった。このことは、危険トリガＤＢの表現形式である形状Ｂが、形状Ａに見つかったある異常を包含／表現していないことを意味する。変更重要度格付け８７１Ｃは、与えられた静的判断基準８７０Ｄにしたがって、どの変更が重要あるいは重要でないのかを格付けする。例：形状Ｂで表現されない異常が形状Ａで見つかったので、この異常が極めて重要であることを静的判断基準８７０Ｄは認識している。よって、このことが結果的に、ハイブリッド形状ＡＢを生成するためにマージプロセスにおいてなされる重立った変更になる。マージモジュール８７１Ｄでは、残すべきものと、異なっていると判明したものが、静的判断基準８７０Ｄと、使用されているモード８７０Ｃに基づき、ハイブリッド形状に再構成される。このようなバリエーションは、データの比分布８７２Ａ、あるデータの重要性、そのデータが互いにどのように噛み合い／関連するかを含みうる。例：異常の構成についての、格付けされた重要性が受信される。適切な調整がなされた後、静的判断基準８７０Ｄによって導かれたプロセスが、この異常への反応が、このデータの他の箇所と互換性がないかどうかを判別する。そして、マージプロセスが、この異常の解決策がこのような既存のデータと効果的に調和するように

、既存のデータを変更する。静的判断基準８７０Ｄによって設定された比８７２Ａに応じて、共通している情報の量が選別される。この比８７２Ａが大きく設定されている場合は、大量の形状データがそのままハイブリッド形状にマージされる。この比８７２Ａが小さく設定されている場合は、ハイブリッド形状の大半が過去のバージョンとは大きく異なるように構築される。優先順位８７２Ｂは、形状の中の同じ箇所である特徴を定義することで、データセット同士が競合している場所であり、優先順位付けプロセスが起動し、目立たせる特徴と、共通しているために隠す特徴を選び出す。ただ一つのトレイトだけが、ある場所（長方形でハイライトされている）を占有できる場合は、優先順位付けプロセスが、どの特徴を継承するかを選ぶために起動される。スタイル８７２Ｃは、共通する点をマージするやり方を定義する。大体の場合、ある特定のマージが発生する状況は多岐に亘っている。このため、静的判断基準８７０Ｄとモード８７０Ｃによって、このモジュールが、ある一方を他方にマージすることを優先させるように指揮されている。大体の場合、特徴間には共通する形状があり、したがって、マージされたトレイトを有する形状が生成できる。例：三角形と円形が入力形状として与えられたとき、「パックマン」の形が生成される。

【０１６８】

図１５５～図１５５は、パーソナルアシスタントとして使用されているＬＯＭを示している。ＬＯＭは、ある個人の生活でパーソナライズされたポートフォリオを管理するように構成することができる。ある個人がジレンマまたは命題に遭遇したときに、ＬＯＭが意味のある適切なアドバイスを提供することができるように、ＬＯＭが毎日のルーチンに関する個人情報を登録することに、積極的に同意することができる。このことは、仕事の状況、食習慣、買物の決定などに及ぶ可能性がある。ＬＯＭは最初の質問８７４Ｂを受け取り、ＬＯＭの内部審議プロセス８７４Ａを介して結論８７４Ｃに至る。ＥＰＬ８１１Ｂは、ＬＯＭによって生成された応答の倫理的、法的、およびプライバシーに基づくコンプライアンスを検証するために使用される。ＬＯＭをよりパーソナルにするために、ＬＯＭがデータを受信して制御できるインターネット対応デバイスに接続するＬＡＡモジュール８１２Ｄに接続できる（たとえば、家に近づくとエアコンがオンになる）。ＰＩＰ８０２Ｃでは、ＬＯＭはユーザから個人情報を受け取り、またそのユーザは、その情報を安全に追跡することに同意することがある。このようにして、ＬＯＭはより個人的に、正確な将来の応答を提供することができる。文脈化８７４Ｄでは、ＬＯＭは申し立てを構成する際に欠落しているリンクを推論することができる。ＬＯＭはその高度なロジックにより、オリジナルの表明によって提起されたジレンマを解決するために、この状況に関するある変数をまず知るか仮定するかしなければならないということを解読した。

【０１６９】

図１５７は、調査ツールとして使用されるＬＯＭを示している。あるユーザは、投資ツールとしてＬＯＭを使用している。表明８７５Ｂは客観的かつ人間の感情を排した方法で提供される。よって、ＬＯＭは、この問題について洗練された意見を出すために、具体的で関連性のないユースケースについての追加的な詳細情報８７５Ｄを要求しない。したがって、個人情報なしで結論８７５Ｃに到達する。ＥＰＬ８１１Ｂは、ＬＯＭによって生成された応答の倫理的、法的、およびプライバシーに基づくコンプライアンスを検証するために使用され、ＢＭ８１９Ｃは、ユーザに代わり違法／不道徳な活動を行う共謀をモニターするのに使用される。

【０１７０】

図１５８および図１５９は、提示された理論８７６Ｂの利点と欠点を調査するＬＯＭを示している。ビットコインは、ブロックチェーンと呼ばれる公開台帳の暗号化の所有権を検証する、ピアツーピアの分散型ネットワークである。発生するビットコイントランザクションのすべては、ネットワークによって１０分ごとにマイニングされるブロックに記録される。ビットコインコアのクライアントに現時点でハードコーディングされた制限は１ＭＢであり、このことは、１０分ごとに（データの形で表現される）１ＭＢ分のトランザクションしか存在しないことを意味している。最近では、資産としてのビットコインの人気

が上がっていることによって、ブロックサイズの制限が、システムへのストレス、支払いの確認時間の長時間化、マイナーの手数料の値上がりを引き起こしている。文脈化８７６Ｄでは、ＬＯＭは申し立てを構成する際に欠落しているリンクを推論することができる。ＬＯＭはその高度なロジックにより、オリジナルの表明によって提起されたジレンマを解決するために、誰がブロックサイズの上限を引き上げるだろうかをまず知るか仮定するかしなければならないということを解読した。したがって、結論８７６ＣはＬＯＭによって到達する。ＥＰＬ８１１Ｂは、ＬＯＭによって生成された応答の倫理的、法的、およびプライバシーに基づくコンプライアンスを検証するために使用され、ＢＭ８１９Ｃは、ユーザに代わり違法／不道徳な活動を行う共謀をモニターするのに使用される。

【０１７１】

図１６０および図１６１は、外交戦争ゲームでのポリシー決定を行うＬＯＭを示している。隔離され安全なＬＯＭのインスタンスは、軍に承認されたハードウェアおよび施設で利用できる。これによって、ＬＯＭは、個人知能プロファイル（ＰＩＰ）のローカルインスタンス内の軍特有の（かつ機密でさえある）情報にアクセスしながら、知識保持中枢（ＣＫＲ）８０６の一般知識にアクセス可能となる。軍関係者は、ＬＯＭの高度なインテリジェンス能力のために、複雑な戦争ゲームを実行することができ、その一方で一般的な知識や特有の知識にアクセスすることが可能である。戦争ゲームの初期シナリオは、表明８７７Ｂとハードコードされた仮定８７７Ｅで提案される。この戦争ゲームのシナリオが複雑であるため、ＬＯＭは、高度で詳細なリクエスト８８７Ｄで応答する。洗練された対応を実現するために、ＬＯＭは、５０，０００人の軍隊という詳細なプロファイルといった、ハイレベルな情報を受け取らなければならないと判断することがある。このような情報転送は、数テラバイトのデータの大きさとなることがあり、洗練された結論に到達するために、何日もの間、複数の並列処理を必要とする。すべての情報は、標準化され自動化されたフォーマットおよびプロトコル（たとえば、１回のコンピュータインターフェースアクションで２時間にわたって５０，０００シートのＥｘｃｅｌシートをインポートする）により転送される。ＢＭ８１９ＣおよびＥＰＬ８１１Ｂによって、この情報の機密的性質によるこのような予防的特徴を無効にするために、秘密取扱許可が有効になる。戦争ゲームのシミュレーションでの課題は、ＢＭ８１９ＣとＥＰＬ８１１Ｂによってフラグが立てられるかもしれない話題が含まれる。ＥＰＬは、実生活と金銭の消費に最終的な影響を与えるシミュレーションに、別の方法で役に立ったかもしれない情報をブロックするかもしれない。ＢＭ８１９Ｃはこの話題にフラグを立てて、それをＭＮＳＰ９の当局に報告していたかもしれない。したがって、適切に資格を与えられた軍事チャネル／組織は、ＰＩＰ８０２Ｃを介してＬＯＭのセッションを認証することで、そのような機密の話題を、中断したり、邪魔されたり、当局に報告されたりすることなく、ＬＯＭを介して処理することを可能にすることができる。軍隊の数や場所などの、このような情報は機密扱いにされているかもしれないため、認証されたセッションは、ＢＭ８１９ＣとＥＰＬ８１１Ｃを完全にブロックするオーバーライドを可能する。そのようにすると、このような機密情報が、ＬＯＭを離れてＭＮＳＰ９などの外部プラットフォームや関係者に流れることはなくなる。ＰＩＰ８０２Ｃでは、この戦争ゲームを実行している、許可された軍関係者は、アップグレードされた／専門化された暗号化および情報隔離を備えた、ＬＯＭのカスタマイズされたインスタンスを使用している。これには、機密軍事情報が決してパブリックのクラウドストレージに入らず、軍に認可された施設内に残ることを保証する、オンサイトのストレージソリューションが含まれることがある。したがって、このような安全に保持された情報は、ＬＯＭの内部審議８７７Ａに、提案された戦争ゲームをシミュレートすることを可能にしている。

【０１７２】

図１６２～図１６３は、ある人物に関する特定可能な詳細情報を明らかにするといった調査ジャーナリズムのタスクを実行するＬＯＭを示している。このユースケースの例は、ナカモトサトシという仮名で知られているビットコインの考案者を取り巻く謎を追っている。ビットコインコミュニティは、多くの雑誌や調査ジャーナリストとともに、その正体を

明らかにする努力をしてきた。しかし、ＬＯＭは、調査への取り組みを、自動化された徹底的な方法で最大化することがでる。ＬＯＭは、最初のクエリに正確に応答できると分からなければならない、ジャーナリズム特有の難問の、特定の側面に向き合うことがある。よって、ＬＯＭはカスタム情報リクエストをＡＲＭ８０５Ｂに送ることで、ＣＫＲ８０６に情報を吸収させることができる。文脈化８７９Ｄでは、質問８７８Ｂは客観的かつ人間の感情を排した方法で提供されるため、ＬＯＭは、この問題について洗練された意見を出すために、具体的で関連性のないユースケースについての追加的な詳細情報を要求しない。ＬＯＭは、知らないとか、確信がないということを「恥ずかしく」感じることがない。というのも、ＬＯＭは、「残酷なまでに正直になる」という「パーソナリティ」を有しているからである。したがって、補助結論８７８Ｅのように、サトシの本当の正体を明らかにするために必要な証拠には、避けがたい穴があることを理解することができる。ＡＲＭ８０５Ｂが、間違いなくサトシのものである知られているすべての電子メールとチャットログを取り出すと、文体計量学８０８Ｂが実行され、サトシの本当の正体が裏付けされ、定義される。したがって、調査ジャーナリズムのタスクに関してＬＯＭが知っていることのすべてが、結論８７９Ｃとして提示される。

【０１７３】

図１６４～図１６５は、歴史的検証を実行するＬＯＭを示している。ＬＯＭは、ひとつながりの語り手の裏付けによって、歴史的文書の真正性を検証することができる。「Ｈａｄｉｔｈ（ハディース）」（アラビア語では文字通り「ニュース」）と呼ばれる歴史的文書は、伝達されたニュースを裏付ける人々の裏付けにより、その元祖に正当に帰属することが証明される。ハディース文献は、もともとアラビア語の口語的な文脈の範囲内で保存され理解されるため、言語学的構築モジュール８１２Ａは、サードパーティの翻訳アルゴリズムを参照することで、母国語で直接この文献を理解している。文脈化８７９Ｄでは、質問８７９Ｂは客観的かつ人間の感情を排した方法で提供されるため、ＬＯＭは、この問題について洗練された意見を出すために、具体的で関連性のないユースケースについての追加的な詳細情報を要求しない。ＫＣＡ８１６Ｄでは、ひとつながりの語り手によって検証されたものとして、引用（ハディース）の正当性に関する証拠を裏付けるために、ＵＫＦのクラスタ化された情報が比較される。このアルゴリズムは、そのような主張がなされたとき、帰属されたソース（たとえば、疑われたハディースの語り手）の信頼性、証拠の否定などを考慮に入れる。ＬＯＭは、ハディースの認証プロセスを容易にするＡＲＭによって取り出されたデータから、ＣＫＲ８０６内で長い時間を掛けてコンセプトを構築する。「ハディースとは何か？」、「ハディースにはどういうバリエーションがあるのか？」、「最善の認証方法は何？」といった自己へ問いかける質問がなされる。そこでは、ＣＫＲ８０６が持ち前の高度な推論を通じて強力な定義の基礎を構築し、ＬＯＭが出力する結論８７９Ｃを正当化することができる。クラスタ構築８７９Ｃでは、ＣＫＲ８０６は、ＵＫＦクラスタと呼ばれる情報の基本単位「積み重ねる」ことによって、コンセプト的な結論に達する。これらのクラスタは、帰属元、疑いのある情報生成の時間などターゲットの情報に関する広範なメタデータを包含している。

デジタル指向言語ＬＡＱＩＴ

【０１７４】

図１６６は、ＬＡＱＩＴのコンセプトを紹介している。ＬＡＱＩＴは、信頼でき対象となる関係者のネットワーク内部から、情報を転送するための、効率的で安全な方法である。ＬＡＱＩＴは、読みやすさ重視とセキュリティ重視とを切り替えることができる、さまざまなモードを提供する。線形、原子、および量子の各モードが、さまざまな機能とアプリケーションを提供する、情報転送の異なる個別のモードである。ＬＡＱＩＴは、安全な情報伝達おける究極の形態である。というのも、ＬＡＱＩＴの最も弱い部分は、頭の中のプライバシーだからである。効率的に簡単に記憶できる鍵は、受信者の頭の中にのみ格納されており、メッセージはその鍵の構成に応じてリアルタイムで（人間の記憶を利用して）解読されるので、相手方のリスクは実質的に除去される。鍵は一度転送してメモリに保存する必要があるだけなので、携帯電話の電源を切った状態で、一時的に暗号化された電子

メールになどより自分で鍵を運ぶなど、単発の記憶イベントに対してより精巧なプライバシー対策を採用できる。すべてのセキュリティ上の責任は、鍵を秘密にしておくことにある。暗記が簡単であるため、セキュリティ上の全責任の大半は軽減される。ブロック９００Ａは、ＬＡＱＩＴの論理的に構造化された構文内で繰り返された、再帰的な、赤、オレンジ、青、緑、および紫の、同じ一貫したカラーシーケンスを示している。ブロック９００Ｂは、英語のアルファベットで翻訳を行うために、再帰的に使用されるカラーシーケンスを、さらに示している。アルファベットの「ベース」レイヤを構築するとき、このカラーシーケンスは、紫のチャネル上では、短縮された不均一なウェイトで使用される。紫のチャンネル内で構文定義のために残されているスペースは、将来の潜在的な使用および拡張のために予約されている。ステージ９０１は、複雑なアルゴリズムが、そのログイベントおよびステータスレポートを、ＬＡＱＩＴを使って報告することを表している。このシナリオでは、好みで暗号化を無効にしているが、暗号化を選択することもできる。ステージＡ１９０２Ａは、ステータスレポート／ログレポートの自動生成を表している。ステージＡ２９０３Ａは、ステータスレポート／ログレポートを、可搬なテキストベースのＬＡＱＩＴ構文へと変換することを表している。ステージＡ３９０４Ａは、デジタル的に暗号化されたチャネル（たとえば、ＶＰＮ１２）や暗号化されていないチャネル（たとえば、素のＨＴＴＰ）を通じて転送することができる、構文的には安全でない情報の転送を表している。暗号化されたチャネルが望ましいが、必須ではない。ステージＡ４９０５Ａは、可搬なテキストベースの構文を、非常に読みやすいＬＡＱＩＴの可視構文（たとえば、線形モード）へ変換することを表している。ステージ９１１は、ターゲットの受信者を人間として表している。ＬＡＱＩＴは、非コンピュータ／非ＡＩの情報の受信者のために設計され、意図され、最適化されているためである。ステージ９０６は、機密情報の送信者が人間であることを示している。このような人間は、情報機関や内部通報制度を代表していることがある。このような送信者９０６は、ＬＡＱＩＴの暗号化鍵を、このような鍵９３９を永続ストレージには何の痕跡も残さずに転送するために設計された、安全で一時的な暗号化トンネル経由で、人間の受信者９１１に直接開示する。人の受信者９１１は、鍵９３９をメモリに保存し、ハッキングの可能性を排除するため、この鍵がデジタルシステム上に有していたあらゆるストレージの痕跡を除去することが理想的である。このことは、鍵の９３９が人間の記憶に対して最適化されていて、比較的短い図形のシーケンスに基づいているため、可能である。ステージＢ１９０２Ｂは、受信者９１１に提出するために、送信者９０６によって入力された局所的に安全でないテキストを表している。ステージＢ２９０３Ｂは、このようなテキスト９０２Ｂを、可搬な暗号化されたテキストベースのＬＡＱＩＴ構文へ変換することを表している。ステージＢ３９０４Ｂは、デジタル的に暗号化されたチャネル（たとえば、ＶＰＮ）や暗号化されていないチャネル（たとえば、素のＨＴＴＰ）を通じて転送することができる、構文的に安全な情報の転送を表している。ステージＢ４９０５Ｂは、視覚的に暗号化されたＬＡＱＩＴ構文（たとえば、暗号化レベル８の原子モード）へのデータ変換を表しており、後で人間の受信者９１１に提示される。

【０１７５】

図１６７は、位置、形状、色、および音などの情報チャネルの使用を通じて情報を転送する際の有効性を比較するために、使用可能な言語の主なタイプ（すなわち情報転送モード）のすべてを示している。最も効果的、効率的、かつ使用可能な言語は、ほとんどのチャネルを効果的に組み込んで活用できる言語である。インクリメンタル認識効果（ＩＲＥ）９０７は、情報転送のチャネルである。これは、情報が完全に伝達される前に、情報の単位の完全な形が認識できる効果を特徴とする。このことは、主語が完了する前に単語やフレーズを終了することに似ている。ＬＡＱＩＴは、単語から単語への遷移を表示することによって、この予測可能インデックスの効果を組み込んでいる。熟練したＬＡＱＩＴの読み手にとっては、ブロックがある位置へと動いているがまだ到着していない間に、表示されようとしている単語を形成し始めることができる。近似認識効果（ＰＲＥ）９０８は、情報転送のチャネルである。これは、壊れているか、混ざっているか、あるいは変更されているかのいずれかであっても、情報の単位の完全な形が認識できる効果を特徴とする。

このことは、「ｃｈａｒａｃｔｅｒ」と「ｃｈｒａｃａｅｔｒ」というスペルの英単語で説明できる。このユニットの外側の境界は定義されている（最初と最後の文字）が、この入り交じった文字同士が近いことで、単語はまだ全体として定義されている。書かれた英語９１２では、典型的な英語のテキストは、文字の位置、文字の形、および、ＩＲＥ９０７で説明したような一緒になっている個々の文字ではなく、単語全体の認識を組み合わせている。会話９１３では、平均的な口頭の会話は、単語の位置（それらの単語が発せられる順序）、ピッチの頻度を表す形状、および可聴強調を組み合わせている。モールス符号９１５は、変化する音の２進的位置で構成されている。情報の受信者の予測認識は、ＩＲＥ９０７は可能にするが、モールス符号は情報を漸進的に流すため、隣接的ではない。手信号９１５では、手の動きの位置およびフォーメーション（形状）が情報を決定する。手信号は、飛行機に合図を送ることから、トラックを止めることまでさまざまである。予言能力は皆無かそれに近い。したがって、ＩＲＥ９０７もＰＲＥ９０８もない。ＬＡＱＩＴ９１６は、競合する言語９１２～９１５と比較して、情報チャネルを最も活用することができる。このことは、より少ない時間とより少ないメディア（たとえば、画面上のスペース）でより多くの情報を転送できることを意味する。このように容量的な余裕を設けることで、強力な暗号化など複雑な機能を効果的に組み込むことができる。ＬＡＱＩＴの音暗号化９０９により、ＬＡＱＩＴは音の情報チャネルを活用することで、情報をさらに暗号化することができる。したがって、素の通信では不可能であることだが、音声を介して情報を転送することが可能であると考えられる。

【０１７６】

図１６８～１６９は、単純さ、使いやすさ、高い情報密度、および暗号化の欠如によって特徴付けられる、ＬＡＱＩＴの線形モードを示している。ブロック９１７は、線形モードの「基本レンダリング」バージョンを示している。ポイント９１８は、それが暗号化されていないことを表わしている。線形モードでは、原子モードでの暗号化の基盤となる図形難読化９４１の、効率的なスペース割り当てはできない。その代わりに、線形モードは、高密度に情報を転送することと、提示画面を効率的に使用するために、最適化されている。単語セパレータ９１９では、この図形の色は単語に続く文字を表し、単語と次の単語との間の区切りとして機能する。これは、原子プロシージャの原子核と同じ構文である。疑問符、感嘆符、終止符、コンマを表す色コードが、すべて適用可能である。単一ビューゾーン９２０は、基本レンダリング９１７が、高度レンダリング９１８と比較して、より大きな文字、したがってより少ない情報をともなう、小さなビューゾーンを組み込む様子を示している。高度レンダリングは、その二重ビューゾーン９２２によって特徴付けられる。高度レンダリングでは、ＬＡＱＩＴリーダーがスピードの面で追いつくことができると予想されるため、ピクセルあたりより多くのアクティブ文字がある。したがって、提示速度と情報密度との間にはトレードオフのジレンマがある。陰影カバー９２１は、観察者の主なフォーカスがビューゾーン上にあるように、入って来る文字および外に出て行く文字を曇らせる。このようにカバーしているにもかかわらず、入ってくる単語を予測し、出て行く単語を検証しチェックする能力を観察者に与えるために、陰影カバーは部分的に透明である。これは、インクリメンタル認識効果（ＩＲＥ）９０７とも呼ばれる。高密度情報転送９２３は、各文字がより小さく、より多くの文字が同じ広さのスペースに提示されるので、ピクセル当たりでより多くの情報が伝達される様子を示している。

【０１７７】

図１７０～図１７１は、広範囲の暗号化レベルが可能な原子モードの性質を示している。ベース９２４の主なキャラクタ参照は、どの文字が定義されているかについて一般原理を指定する。ベースが赤い場合は、アルファベット参照９００Ｂにしたがって、その文字が文字Ａ～Ｆの間（両端含む）にあることを示している。ベースだけで（キッカー９２５なしに）単語を読み取ることが可能である。というのも、単語のスペルを推測するのに、帰納法が使えるのである。暗号化を可能にするため、合計で５つの可能な形状に存在可能である。キッカー９２５は、ベースと同じ色の範囲で存在し、特定の文字を正確に定義する。キッカーがないと、ある定義、たとえば赤いベースが文字Ａであるという定義も、自分

自身で、キッカーなしに表す。暗号化を可能にするため、キッカーが、合計で５つの可能な形状に存在することが可能である。読み取り方向９２６では、情報伝達の読み取りは、軌道輪１の頂上にある正方形から始まる。読み取りは時計回りに実行される。軌道輪が完結すると、次の軌道輪（輪２）の頂上にある正方形からリーダーが続ける。入口／出口ポータル９２７は、キャラクタ（そのベース）の生成と破壊のポイントである。該当する軌道に属する、新しいキャラクタが、ポータルから現れ、時計回りにその位置にスライドする。原子核９２８は、その単語に続くキャラクタを定義する。典型的には、このキャラクタスペースであり、この単語が提示された後は文章が続くことを示す。疑問符、感嘆符、終止符、コンマを表す色コードが、すべて適用可能である。また、３つの軌道輪のすべてがそれらの最大容量まで満たされているため、同じ単語が新しい情報状態で継続されるかどうかを示している。ある軌道輪９２９がいっぱいになると、その文字は次の（より大きな）軌道輪にオーバーフローする。軌道輪１の限界は７であり、輪２は１５であり、環３は２０である。これにより、原子内で最大４２文字（偽物可能性含む）が可能になる。４２文字の制限に達すると、この単語は４２のセグメントに分割され、核は次の情報状態が現在の単語の続きであることを示すことになる。ワードナビゲーション９３０では、各ブロックは、画面の左側に単語全体（あるいは、複数の単語を分子モードで）を表している。ある単語が表示されると、それぞれのブロックが外側に右の方に移動し、その単語が完成するとブロックは後退する。ナビゲーションブロックの色／形は、この単語の最初の文字のベースと同じ色／形である。センテンスナビゲーション９３１では、各ブロックは単語のクラスタを表している。クラスタとは、単語ナビゲーションペインに収まる最大量の単語である。センテンスナビゲーションブロックがそのままである場合、あるいはたくさんのうちの最後の一つである場合、それは最大容量よりも小さな単語のクラスタを表す可能性が高い。原子状態生成９３２は、インクリメンタル認識効果（ＩＲＥ）９０７を誘発する遷移である。このような遷移により、ベース９２４は入口／出口ポータル９２７から現われし、それらのキッカー９２５は隠され、時計回りに移動してそれらの位置を占める。この遷移の間、ＬＡＱＩＴの熟練した読み手は、ＩＲＥ９０７によりキッカー９２５が明らかになる前に、部分または全体の単語を予測することができる。これは、ほとんどの検索エンジンのオートコンプリート機能に似ており、最初のひとまとまりの情報でシーケンスの残りシーケンスを推定する。原子状態拡張９３３は、近似認識効果（ＰＲＥ）９０８を誘発する遷移である。ベース９２４がその位置に達すると、それらのベースは情報状態提示の「拡張」シーケンスにおいて外側に移動する。これにより、キッカー９２５が明らかになり、情報状態の特定の定義を提示することができる。ＬＡＱＩＴの熟練した読み手は、単語を漸進的に構築するために個々の文字を少しずつにスクロールする必要はない。むしろ構造全体を全体として見て、ＰＲＥ９０８によって単語の意味をすぐに認識することになる。原子状態破壊９３４は、インクリメンタル認識効果（ＩＲＥ）９０７を誘発する遷移である。この段階で、キッカー９２５を再び覆うために、ベース９２４は後退している（拡張シーケンス９３３を逆転して）。ベースは時計回りにスライドして入口／出口ポータルに達している。情報状態の高速レンダリングにおいて、ＬＡＱＩＴの熟練した読み手は、破壊遷移を利用して単語の認識を完了することができることになる。これは、拡張された原子状態（キッカーが現れること）を見る機会が非常に少ない（１秒の数分の１）場合に役に立つ。

【０１７８】

図１７２～図１７４は、原子モードの暗号化機能の概要を示している。ＬＡＱＩＴは情報を効率的かつ高密度に転送する手段を提供するため、暗号化の実装をまかなうのに、十分な情報帯域幅がある。この構文的暗号化は、意図された情報受信者が、記憶した鍵でリアルタイムに情報を解読することを必要とする点で、従来のサイバーセキュリティ暗号化とは異なる。これにより、移動中のデータ、休止中のデータ、および使用中のデータが悪意のある、認証されていない者達によって読み取られ理解されるリスクが軽減される。暗号化の複雑さは、９つの標準化レベル９４０に変化し、これは、可読性とセキュリティ強度の間のトレードオフである。図形難読化９４１（レベル１～９）では、標準の四角形が５

つの視覚的に区別できる図形に置き換えられる。構文内の図形の分散は、原子プロファイルの戦略的ポイントにダッド（偽物）文字を挿入することを可能にする。ダッド文字はメッセージの本当の意図された意味を難読化させる。文字が真であるか偽かを解読することは、安全かつ一時的に転送された解読鍵によって行われる。文字がキーと互換性がある場合、それは単語の計算で頼りにされる。キーと非互換である場合、その計算内で無視される。リダイレクトボンド９４２（レベル４～９）では、ボンドが２つの文字を結合し、読み込みの流れを変更する。典型的な時計回りの読み込みパターンから始まり、合法／非偽の文字を打ち上げ（始まって）着地する（終わる）ボンドに遭遇すると、読み込みパターンを変更して着地文字を再開する。放射性元素９４３（レベル７～９）では、文字が偽物であるか否かの評価を覆すことができるいくつかの要素は「音を立てる」ことができる。図形９３５は、暗号化に利用可能な図形を示している：三角形、円形、正方形、五角形、および台形。中心要素９３６は、単語の直後に来るキャラクタを定義する、軌道の中心要素を示している。このような要素は、終止符を示す赤、カンマを示すオレンジ、スペースを示す青、疑問符を示す緑、感嘆符を示すピンクである。暗号化の例９３７は、暗号化レベル１～９に適用可能な図形難読化９４１を示している。中心要素９３６は軌道の中心に示され、ダッド文字９３８は図形難読化９４１による暗号化の主な手段である。左のダッドには、円-四角形のシーケンスがある。右のダッドには四角形-三角形のシーケンスがある。これらのシーケンスの双方が暗号化キー９３９に存在しないため、リーダーは、それらをダッドとして認識することができる。したがって、情報状態の意味を計算するときにそれらをスキップすることができる。

【０１７９】

図１７５～図１７６は、リダイレクトボンド９４２のメカニズムを示している。暗号化の例９４４は、リダイレクトボンド９４２と９４５を示している。これらは、リダイレクトボンドに関する「関与ルール」であり、

１）ボンドに達したときは、デフォルトでそのボンドに従うので、時計回りの挙動は放棄される。

２）経路をたどるとき：打ち上げ文字、つまりその文字から経路が始まる文字、がシーケンスの一部として数えられる。

３）経路をたどるとき：着地文字、つまりその文字で経路が終わる文字、がシーケンスの一部として数えられる。

４）経路は一度しか追跡できない。

５）文字の特定のインスタンス、一度しか数えられない。

６）打ち上げと着地の両方の文字がダッドでない場合にのみ、経路をたどらなければならない。リダイレクトボンド９４５では、ボンドは「打ち上げ」文字から始まり、「着地」文字で終わる。どちらの文字も、ダッドであってもなくてもかまわない。それらのいずれもがダッドでない場合、ボンドは読み取り方向および位置を変更する。片方または両方がダッドである場合、ボンド全体を無視しなければならない。さもなければ、メッセージが正しく解読されない。個々のボンドには読み取られる正しい方向があるが、その順序は明示的には記述されてなく、情報の状態の現在の読み取り位置とダッドの構成によって誘導されなければならない。ダッド文字９４６は、これらの２つのダッド文字が解読をより複雑にし、よってブルートフォース攻撃に耐性があるようにする様子を示している。これは、図形難読化とリリダイレクトボンドの組み合わせが、ブルートフォース攻撃者にとって、指数関数的に難しいタスクにつながるからである。ボンドキー定義９４７：情報状態の読み取りの際にボンドに従わなければならない場合、それは、暗号鍵で具体的に定義されているかどうかによって異なる。あり得る定義は、単結合、二重結合および三重結合である。誤ってリダイレクトボンドを読み取る（ボンドキー９４７を知らないために）という潜在的なケースシナリオは、正しくない解釈９４９に示されている。このような正しくない解釈９４９は、メッセージ「ＲＤＴＮＢＡＩＢ」につながるが、正しい解釈９４８の本当のメッセージは「ＲＡＢＢＩＴ」である。図形難読化９４１の複雑さを活用して指数関数的に安全なメッセージを作成するため、リダイレクションボンド９４５を間違って解釈

する複数の可能性がある。正しい解釈９４８に示すように、本当の正しいメッセージを解釈する正しい方法は一つだけである。

【０１８０】

図１７７～図１７８は、放射性元素９４３のメカニズムを示している。暗号化の例９５０は、放射性元素９４３および９５１を示している。これらは、放射性元素に関する「関与ルール」であり、

１）情報状態の拡張フェーズ中に、放射性元素が不安定または振動していると認識される。

２）放射性元素は、放射能活性または休止状態のいずれかであり得る。

３）活性な放射性元素は、ダッドであるというその状態が反転されたということを示している。たとえば、図形の構成が、それがダッドであることを示す場合、それは疑陽性であり、実際にはダッドしてカウントされず、実際の文字としてカウントされる。図形の構成が、それが本物であることを示している場合、それは疑陽性であり、実際の文字ではなく、ダッドとしてカウントされる。

４）休止状態の放射性元素は、ダッドであるか実際の文字であるかというその状態が、影響を受けていないことを示している。

５）一群の放射性元素は、軌道輪内部の連続した放射能の存在によって定義される。放射性元素が（特定の軌道環内で）互いに隣接している場合、それらはクラスタを形成する。放射性元素の近隣が非放射性である場合、これはクラスタの上限である。

６）キーは、どのクラスタが活性・休止状態であるかを定義する。たとえば、キーがダブルクラスタを意味する場合、すべてのダブルクラスタは放射性であり、すべてのシングルクラスタおよびトリプルクラスタは休止状態である。放射性元素９５０は、情報提示の拡大フェーズで激しく揺れた場合に、文字（または要素）が放射性であるとみなされる様子を示している。暗号化レベルの分類のために、放射性元素を含む原子は常に原子間結合を有する。放射性元素は、それらがダッドであるか否かについての文字の分類を変更するため、セキュリティの難読化が指数関数的に増加する。ダブルクラスタ９５２は、あるシーケンス内かつ同じ軌道内に２つの放射性元素があるので、クラスタ（ダブル）としてカウントされる様子を示している。それらを活性あるいは休止状態として扱うかどうかは、暗号化キー９５４によって定義される。シングルクラスタ９５３では、両方の隣接ノードが非放射性であるため、クラスタのスコープが定義される。キーは二重クラスタを有効と指定しているため、この要素９５３は、それがそもそも放射性でない場合に処理される。ダブルクラスタのキー定義９５４では、キーはダブルクラスタを活性と定義するため、他のすべてのサイズのクラスタは、メッセージを復号化している間、休止状態であるとみなされる。正しくない解釈９５６は、インタプリタがダブルクラスタ９５２を逆順シーケンス（偽陽性）として扱わなかった様子を示している。このことは、ステップ９５６Ａにおいて、ダッドでないにもかかわらず、それが解読プロセスに文字を逆に解釈するように指示する（鍵９５４によって検証された）活性の放射性クラスタに属しているため、正しい答えがそれを無視することを意味している。図形難読化９４１、リダイレクトボンド９４２、および放射性元素９４３が同時に使用されている間、キーを知らない人は、実用的な意味でブルートフォース攻撃を使用してすべての潜在的な組み合わせを推測することができない。正しくない解釈９５６は、鍵９５４のないインタプリタが、正しい解釈９５５にしたがって守られることを想定されていないリダイレクションボンド９５６Ｂを誤解する可能性があることを示している。これは、「ＲＡＢＢＩＴ」ではなく「ＲＡＤＩＴ」という、まったくことなるメッセージの結果につながっている。メッセージを正しく解読する手段の詳細は、「正しい解釈９５５」に示されている。

【０１８１】

図１７９は、暗号化およびストリーミング９５９が可能な分子モードを示している。秘密辞書攻撃抵抗９５７では、メッセージの誤った解読は、「赤いニシン」という別のメッセージにつながる。これは、常習犯に、本当のメッセージの隠れ蓑として機能する偽のメッセージを受け取っている間に、メッセージを正常に復号化したという誤った印象を与える

ことになる。分子９５８ごとに複数のアクティブワードを用い、単語は分子プロシージャの間に並行して提示される。これは表面積比当たりの情報を増加させるが、一貫した移行速度でより熟練した読み手を必要とする。ナビゲーションという言葉は、現在アクティブな４つの単語があることを示している。しかし、リダイレクトボンドの難読化のために、メッセージの単語は、分子内の複数の原子にまたがって部分的に、そして全体として存在する。バイナリおよびストリーミングモード９５９はストリーミングモードを示し、典型的な原子構成では読み取りモードはバイナリである。バイナリモードは、中心要素が単語に続くキャラクタ（たとえば、疑問符、感嘆符、終止符、スペースなど）を定義することを示している。分子モードもまたバイナリである。ただし、ストリーミングモードに準拠した暗号化が有効になっている場合を除く。ストリーミングモードは、軌道内で疑問符などの特殊文字を参照する。これは、暗号化された分子内で複数の原子にまたがって単語が存在するため、特定の中心要素が特定の単語に対して排他的に存在できないために行われる。分子ボンド９６０では、分子情報状態は排他的な暗号化機能ではなく、暗号化難読化の触媒となり得る。暗号化の３つのモード（図形難読化、リダイレクションボンド、および放射性要素）は、分子寄りの環境に置かれると、セキュリティ強度が急激に増加する。読み取り方向キー９６１は、デフォルトの読み取り方向が行１の左から右へ、次に行２の左から右へというのに対して、読み取り方向は暗号鍵によって取って代わられることを示している。これにより、意図されたメッセージの難読化が増加、メッセージのプライバシー／セキュリティが向上する。リダイレクトボンドは最も優先度が高く、キーに定義されている方向にも優先する（ボンドがダッドでない限り）。

ベース接続協調攻撃統合ノード（ＢＣＨＡＩＮ）を伴った普遍的ＢＣＨＡＩＮ全接続（ＵＢＥＣ）のサマリ

【０１８２】

図１８０は、ＢＣＨＡＩＮ対応アプリケーション１００３を含み、実行するＢＣＨＡＩＮノード１００１を示している。通信ゲートウェイ（ＣＧ）１０００は、ＢＣＨＡＩＮノード１００１が、そのハードウェアインタフェースと対話し、その後、他のＢＣＨＡＩＮノード１００１との通信に至るための、主要なアルゴリズムである。ノード統計調査（ＮＳＳ）１００６は、リモートノードの挙動パターンを解釈する。ノードエスケープインデックス１００６Ａは、隣接ノードが知覚ノード近傍を回避する可能性を追跡する。高いエスケープ指数は、取り組むために洗練された戦略を必要とする、より無秩序な環境を示す。
事例：高速道路にある自動車のスマートフォンは、高いノードエスケープインデックスを示す。スターバックスにある冷蔵庫は、非常に低いノードエスケープ指数を示す。
ノード飽和指数１００６Ｂは、知覚ノードの検出範囲内にあるノードの量を追跡する。高い飽和指数は、多数のノードを有する混雑したエリアを示す。これは、需要と供給のトレードオフがあるため、パフォーマンスに肯定的および否定的な影響を及ぼす可能性があるが、高密度のノードエリアはより安定／予測可能で、したがって無秩序さが少ないと予想される。
事例：ニューヨーク市の中心にあるスターバックスは、ノード飽和インデックスが高い。砂漠の真ん中のテントは、ノード飽和インデックスが非常に低い。
ノード一貫性インデックス１００６Ｃは、知覚ノードによって解釈された、ノードサービスの品質を追跡する。高いノード一貫性インデックスは、周囲の隣接ノードがより多くの可用性稼働時間およびパフォーマンスの一貫性を有する傾向があることを示す。２つの目的で用いられるノードは、一貫性インデックスが低くなる傾向がある一方で、ＢＣＨＡＩＮネットワーク専用のノードは、高い値を示す。
事例：企業の従業員のコンピュータなど、２つの目的を持つノードは、勤務時間中には利用可能なリソースが少なく、昼休みや従業員の不在中は利用できるリソースが多いため、一貫性インデックスは低くなる。
ノードオーバーラップインデックス１００６Ｄは、知覚ノードによって解釈される、ノード同士の互いの重複の量を、互いに追跡する。オーバーラップインデックスと飽和インデックスとの間は相関がある傾向があるが、オーバーラップインデックスは隣接インデック

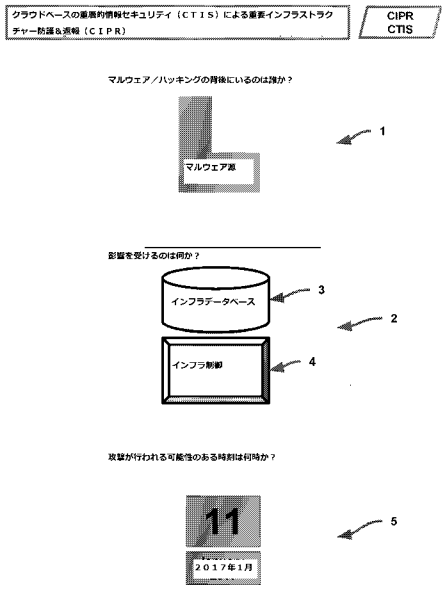
ス同士の共通オーバーラップ量を示し、飽和インデックスは物理的傾向のみを扱うという点で区別できる。したがって、各デバイス上の広い無線範囲を有する高い飽和指数は、高い重複指数につながる。
事例：デバイスは、新しいＢＣＨＡＩＮ最適化マイクロチップ（ＢＯＭ）がインストールされたＢＣＨＡＩＮネットワークの特定のセクタへの侵入を開始する。デバイスは高度なビームフォーミング技術を備えた高利得指向性アンテナを備えている。したがって、それらのセクタでは、オーバーラップした通信構造を有するノードが理由で、オーバーラップインデックスが増加する。
【０１８３】
図１８１は、ＢＣＨＡＩＮプロトコルのコアロジック１０１０を示している。カスタムチェーン認識モジュール（ＣＲＭ）１０２２は、ノードによって過去に登録されたカスタムチェーン（ＡｐｐｃｈａｉｎｓまたはＭｉｃｒｏｃｈａｉｎｓである可能性がある）と接続する。したがって、このノードは、そのような機能に対する読み取り、書き込み、および／または管理能力に対する暗号化アクセス権を有する。このモジュールは、Ｍｅｔａｃｈａｉｎまたは ＭｉｃｒｏｃｈａｉｎのＭｅｔａｃｈａｉｎエミュレータの、Ａｐｐｃｈａｉｎのセクションでアップデートが検出されたとき、ＢＣＨＡＩＮプロトコルの残りの部分を通知する。コンテンツクレームデリバリ（ＣＣＤ）１０２６は、検証されたＣＣＲ１０１８を受信し、その後、リクエストを満たすために、該当するＣＣＦ１０２４を送信する。
【０１８４】
図１８２は、創作モジュール１８を使用して、最適化ストラテジー選択アルゴリズム（ＯＳＳＡ）を介してシステムが好む複雑なストラテジーを混成することによって、新しいストラテジー配置１０５４を動的に生成する、ストラテジー生成モジュール（ＳＣＭ）１０４６を管理する、動的ストラテジー適応（ＤＳＡ）１００８を示している。新しいストラテジーは、フィールド乱雑解釈（ＦＣＩ）１０４８によって提供される入力にしたがって変化する。
【０１８５】
図１８３は、ＵＢＥＣプラットフォームインタフェース（ＵＰＩ）の下でグラフィカルユーザインタフェース（ＧＵＩ）によって管理される様々な経済人格１０５８、１０６０、１０６２、および１０６４を有する、暗号化デジタル経済交流（ＣＤＥＥ）１０５６を示している。人格Ａ１０５８では、ノードリソースは、消費するものと一致するものだけが消費される（もしあれば）。人格Ａは、情報伝達量が軽度から中程度である、カジュアルで質素な消費者にとって理想的である。ＶｏＩＰコール（たとえば、Ｓｋｙｐｅ）や優先情報転送などのライブストリームは極力抑えられる。人格Ｂ１０６０は、利益マージンがＸより大きい限り、可能な限り多くのリソースを消費する。（余分な作業単位は、暗号通貨、法定紙幣、貴金属などの代替通貨で取引できる）。人格Ｂは、とりわけ利潤動機のためにＢＣＨＡＩＮネットワークのインフラに貢献するように設定されたノードにとって理想的である。したがって、このようなノードは、典型的には、バッテリ駆動の装置ではなく、商用電源で稼働する永続的なインフラ設備であり、強力なコンピュータ内部構造（無線機能、ＣＰＵ強度、ハードディスクサイズなど）、たとえば固定式アプライアンスをなど有する。人格Ｃ１０６２は、より少ないノードリソースを消費しながらコンテンツを消費できるように、取引通貨（暗号化、法定紙幣、貴金属など）を通じて作業単位を支払う。人格Ｃは、情報伝達の大量消費者、またはＢＣＨＡＩＮネットワークから利益を引き出すことを望んでいるが、デバイスのリソースが枯渇する（たとえば、スマートフォンがバッテリを急速に使い切ってポケットの中で温かくなっている）ことを望んでいない人にとって理想的である。人格Ｄ１０６４では、ノードのリソースは、コンテンツの消費であろうと、金銭的な補償であろうと、極力多くのものを期待してなんら制限なしに消費する。人格Ｄは、ＢＣＨＡＩＮネットワークの強みに最大の関心を持つ人によって選ばれる。（たとえば、ＢＣＨＡＩＮネットワークのコア開発者は、コンテンツを消費したり、収益を上げたりするためではなく、ただネットワークを強化するためだけに、ノードを購入し、

インストールすることができる。仕事現状の解釈（ＣＷＳＩ）１０６６は、Ｍｅｔａｃｈａｉｎのインフラ経済セクションを参照することで、仕事量クレジットに関してこのノードの現在の黒字または赤字を判断する。経済的に考慮された労働賦課（ＥＣＷＩ）１０６８は、選択された経済人格を、現行の作業剰余／赤字とともに考慮し、現在より多くの作業が行われなければならないかどうかを評価する。

【０１８６】

図１８４は、互いを知的に成長させることができる、３つの異なるアルゴリズムの三者関係である、象徴的再帰的知性向上（ＳＲＩＡ）を示している。ＬＩＺＡＲＤ１６は、コードの目的を理解することによって、アルゴリズムのソースコードを改善することができる。I^2ＧＥ２１は、世代の仮想プログラムのバージョンをエミュレートすることができ、このため、最も強力なプログラムバージョンを選択できる。ＢＣＨＡＩＮネットワークは、分散型の方法で複雑なデータ偏重のプログラムを実行できる、無秩序に接続されたノードの巨大なネットワークである。

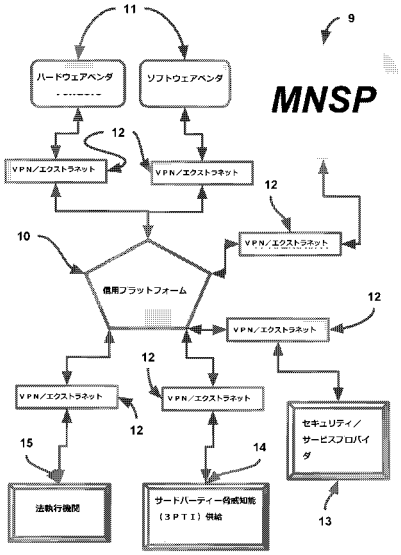
【図１】



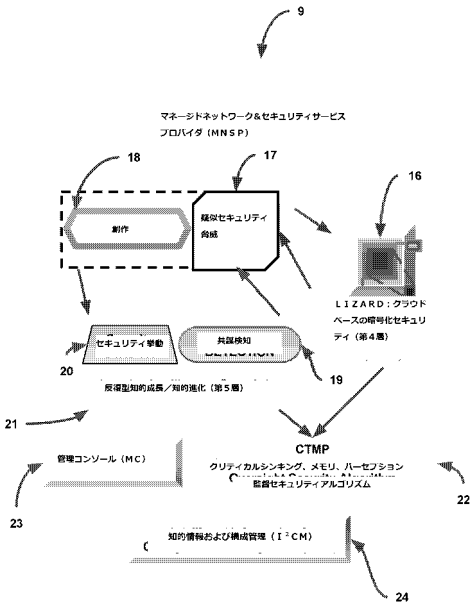
【図２】



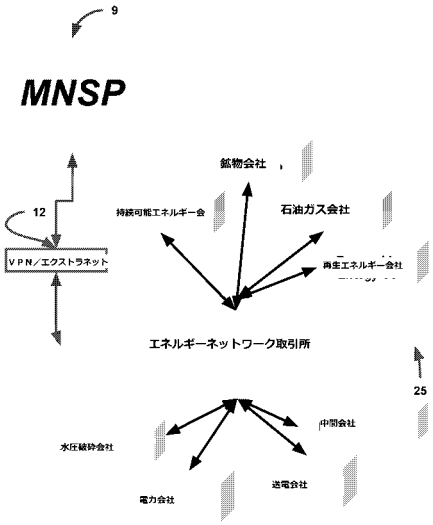
【図３】


11
9
ハードウェアベンダ
ソフトウェアベンダ
MNSP
12
VPN／エクストラネット
10
信用フラットフォーム
15
14
13
法執行機関
サードパーティー脅威知能（３ＰＴＩ）供給
セキュリティ／サービスプロバイダ

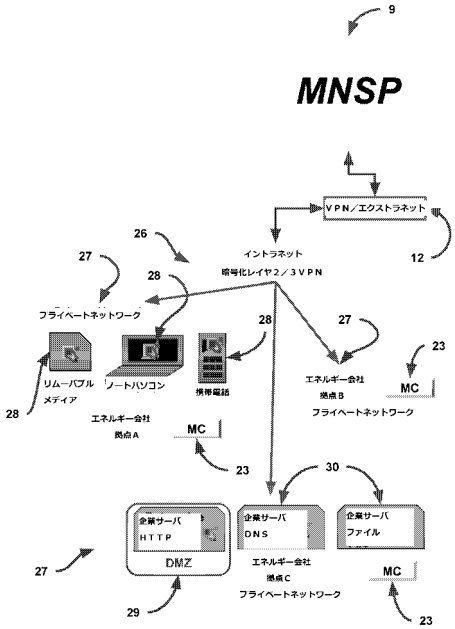
【図４】


9
マネージドネットワーク＆セキュリティサービスプロバイダ（ＭＮＳＰ）
18
17
16
創作
疑似セキュリティ脅威
ＬＩＺＡＲＤ：クラウドベースの暗号化セキュリティ（第４層）
セキュリティ挙動
共謀検知
20
19
反復型知的成長／知的進化（第５層）
21
管理コンソール（ＭＣ）
CTMP
クリティカルシンキング、メモリ、パーセプション
監督セキュリティアルゴリズム
22
23
知的情報および構成管理（Ｉ２ＣＭ）
24

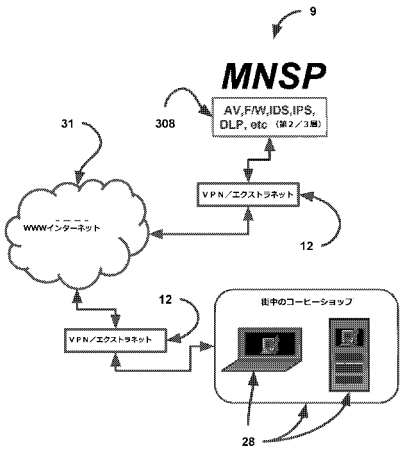
【図５】


9
MNSP
12
VPN／エクストラネット
鉱物会社
持続可能エネルギー会
石油ガス会社
再生エネルギー会社
エネルギーネットワーク取引所
25
水圧破砕会社
仲間会社
送電会社
電力会社

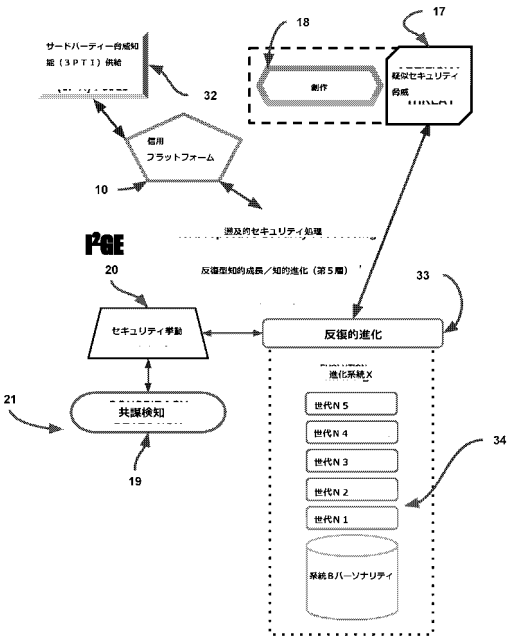
【図６】


9
MNSP
VPN／エクストラネット
12
26
27
28
イントラネット
暗号化レイヤ２／３ＶＰＮ
フライベートネットワーク
リムーバブルメディア
ノートパソコン
携帯電話
エネルギー会社拠点Ａ
エネルギー会社拠点Ｂ
フライベートネットワーク
MC
23
30
企業サーバＨＴＴＰ
企業サーバＤＮＳ
企業サーバファイル
DMZ
エネルギー会社拠点Ｃ
フライベートネットワーク
29

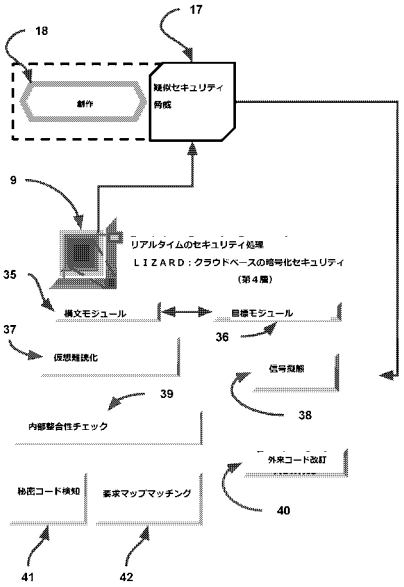
【図７】


9
MNSP
308
AV,F/W,IDS,IPS,
DLP, etc （第2／3層）
31
VPN／エクストラネット
www.インターネット
12
12
VPN／エクストラネット
街中のコーヒーショップ
28

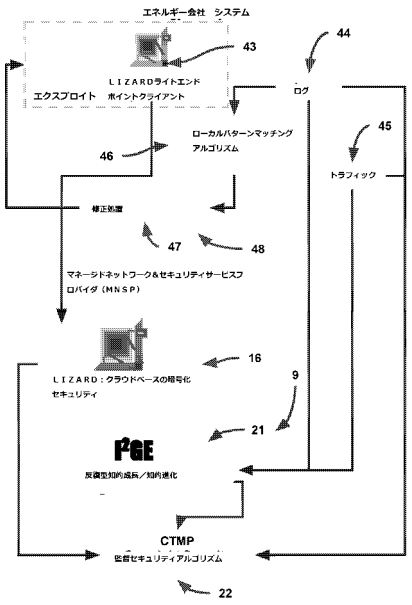
【図８】


サードパーティー脅威知
能（３ＰＴＩ）供給
32
18
17
創作
疑似セキュリティ
脅威
信用
プラットフォーム
10
進化的セキュリティ処理
20
反復型知的成長／知的進化（第５層）
33
セキュリティ挙動
反復的進化
進化系統Ｘ
21
共謀検知
世代Ｎ５
世代Ｎ４
世代Ｎ３
世代Ｎ２
世代Ｎ１
34
19
系統Ｂパーソナリティ

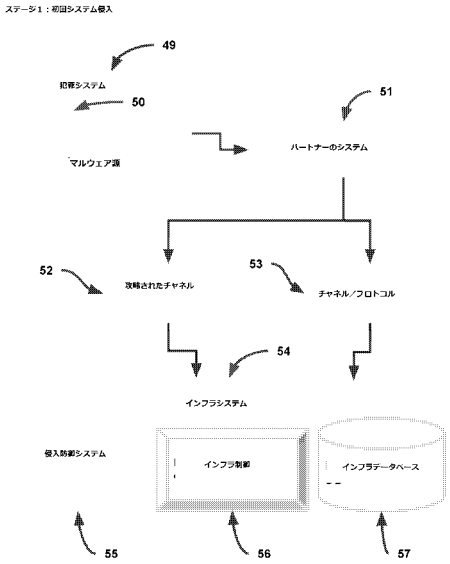
【図９】


17
18
創作
疑似セキュリティ
脅威
9
リアルタイムのセキュリティ処理
ＬＩＺＡＲＤ：クラウドベースの暗号化セキュリティ
（第４層）
35
構文モジュール
目標モジュール
37
36
仮想難読化
信号解析
39
38
内部整合性チェック
外来コード改訂
秘密コード検知
要求マップマッチング
40
41
42

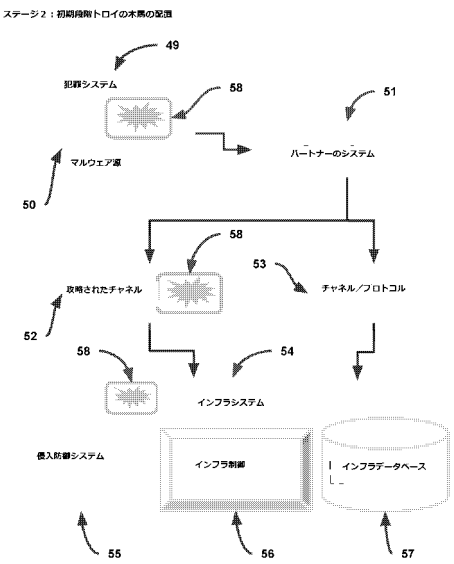
【図１０】


エネルギー会社　システム
44
43
ＬＩＺＡＲＤライトエンド
エクスプロイト　ポイントクライアント
ログ
ローカルパターンマッチング
アルゴリズム
45
46
トラフィック
修正処置
47
48
マネージドネットワーク＆セキュリティサービスプ
ロバイダ（ＭＮＳＰ）
16
ＬＩＺＡＲＤ：クラウドベースの暗号化
セキュリティ
9
21
反復型知的成長／知的進化
CTMP
監督セキュリティアルゴリズム
22

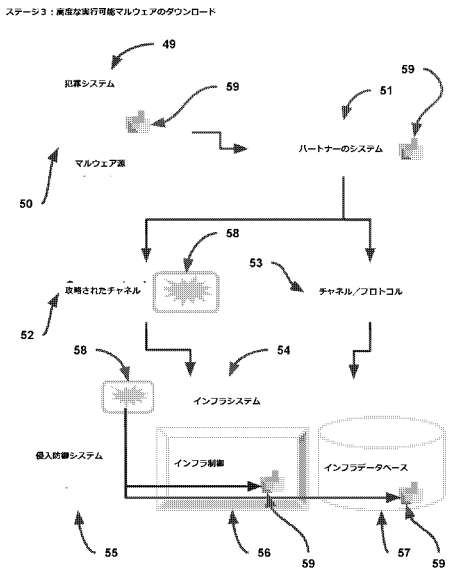
【図１１】



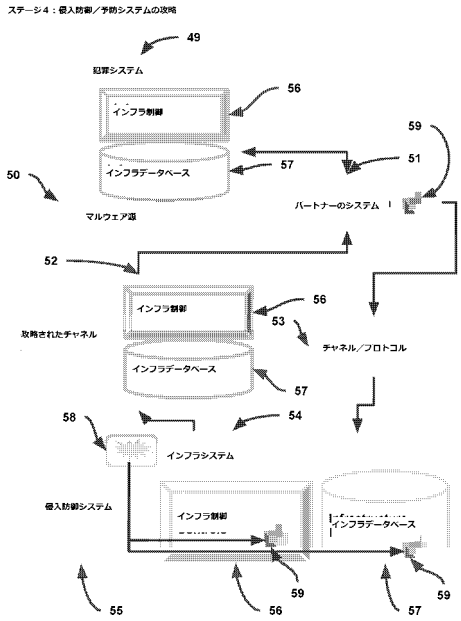
【図１２】



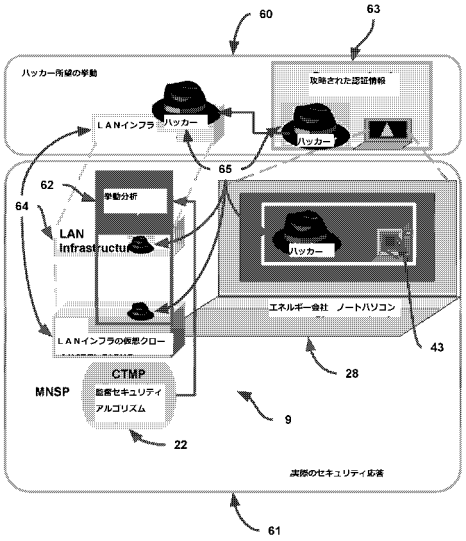
【図１３】



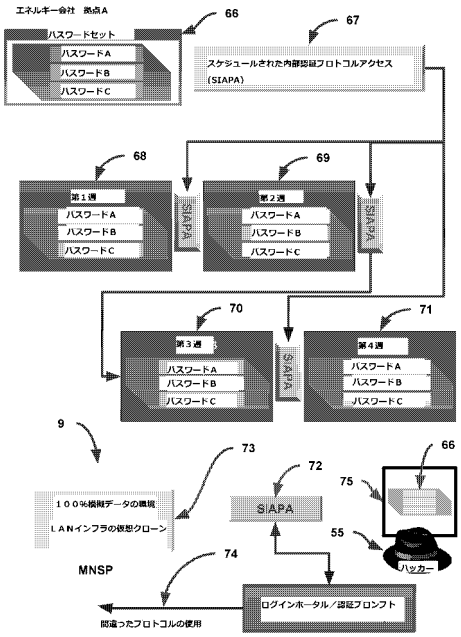
【図１４】



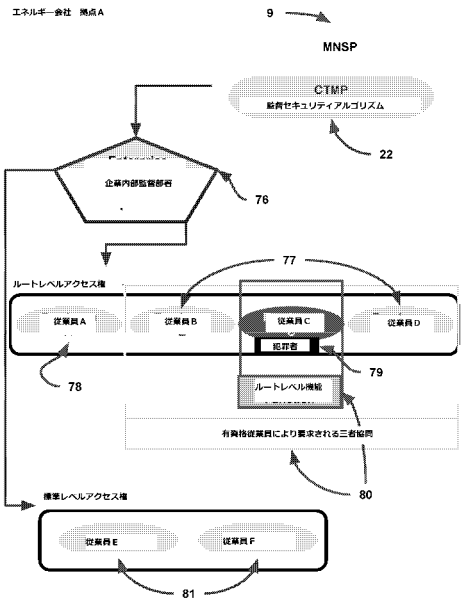
【図１５】



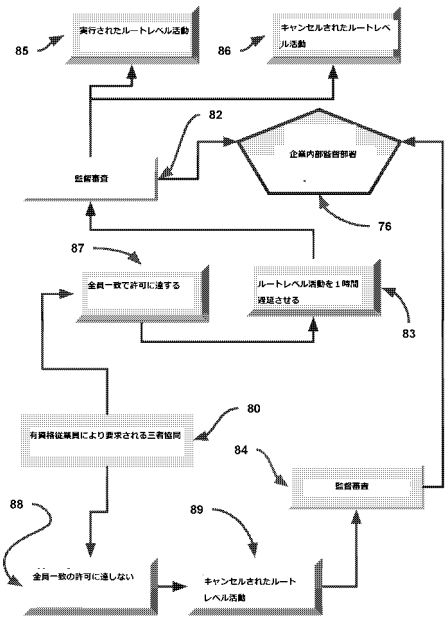
【図１６】



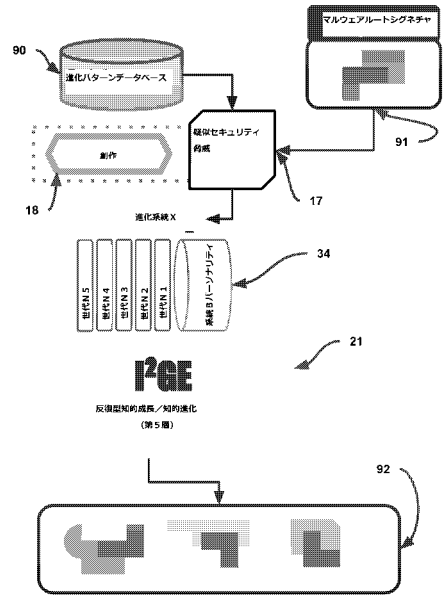
【図１７】



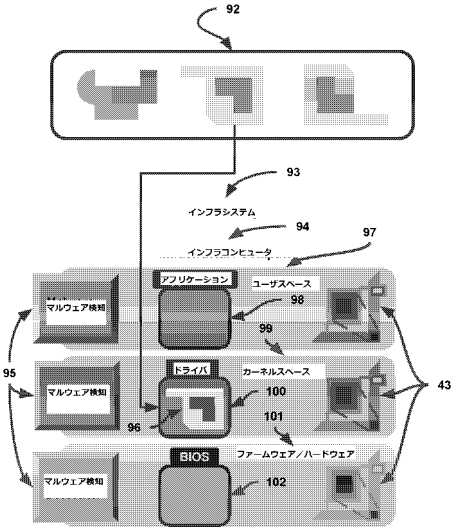
【図１８】



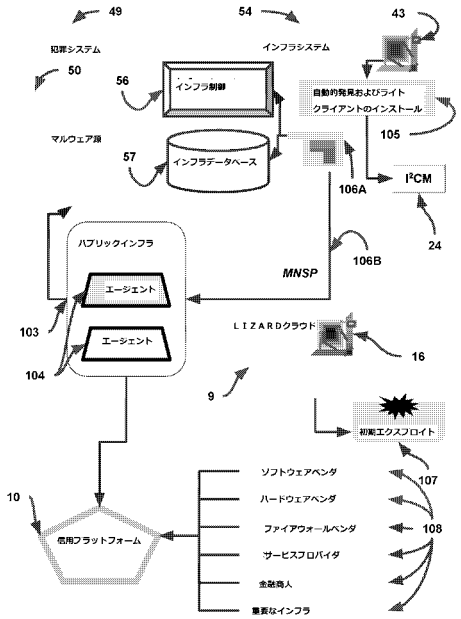
【図１９】



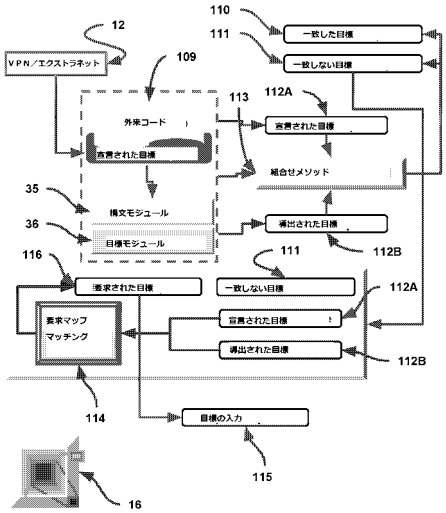
【図２０】



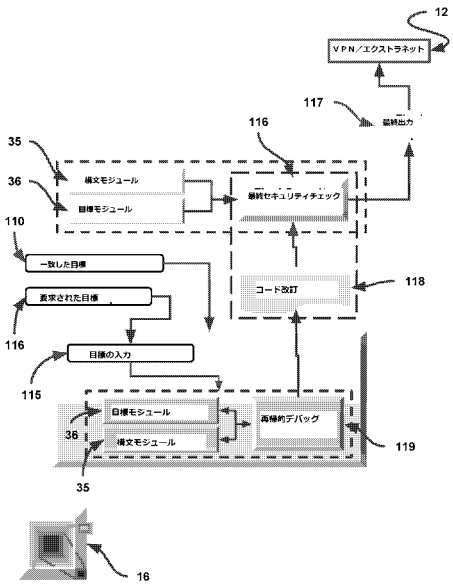
【図２１】



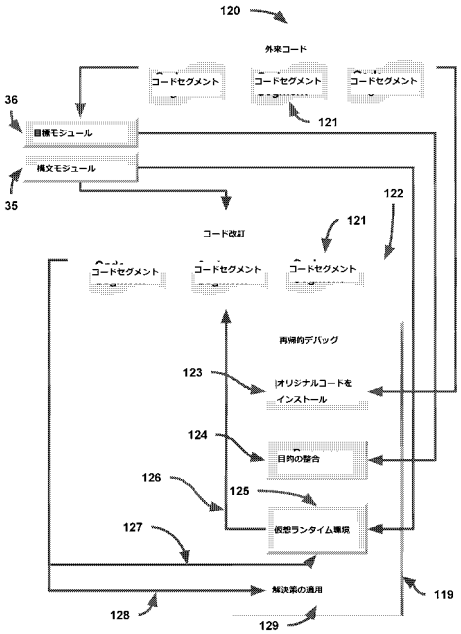
【図２２】



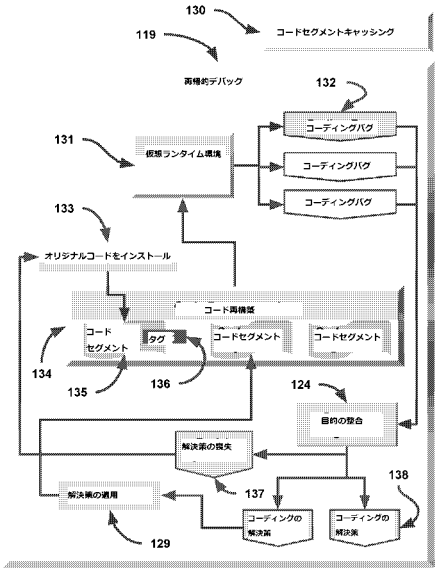
【図２３】



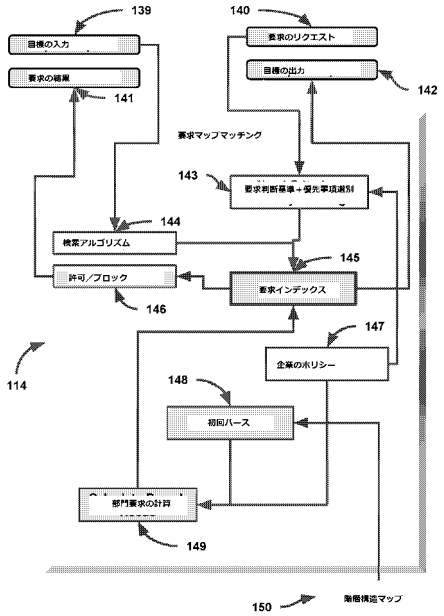
【図２４】



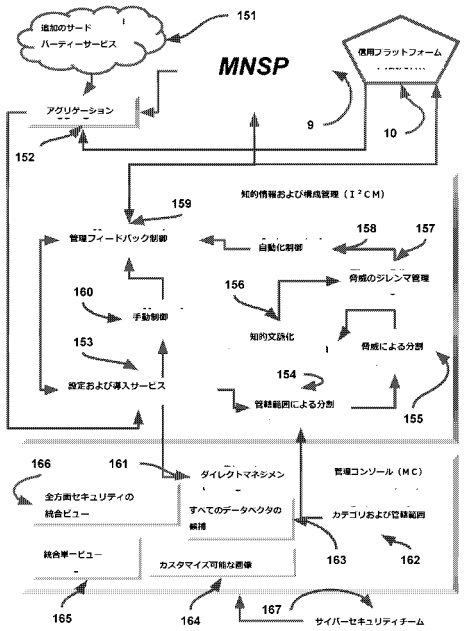
【図２５】



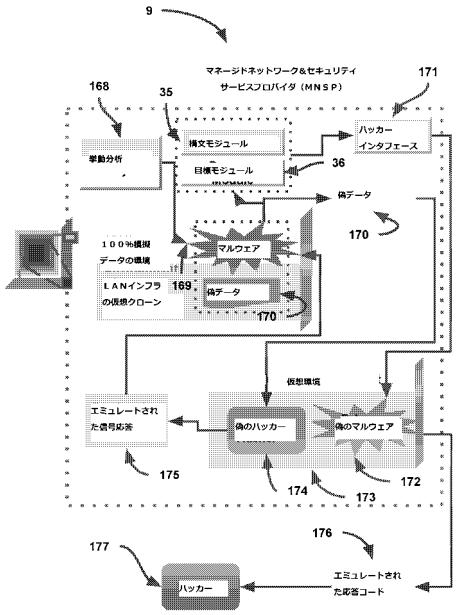
【図２６】



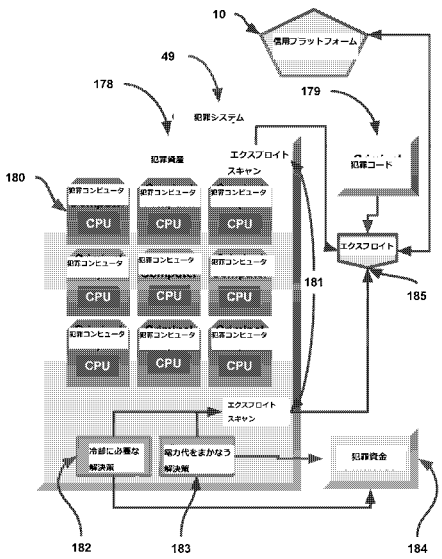
【図２７】



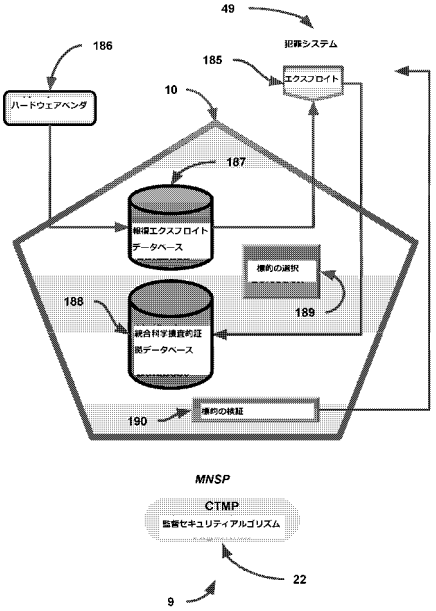
【図２８】



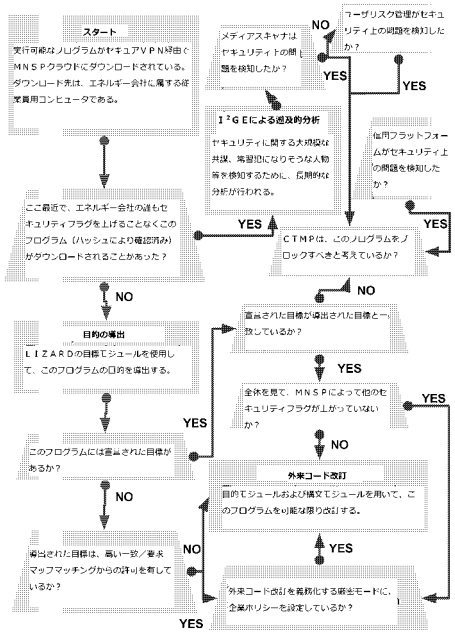
【図２９】



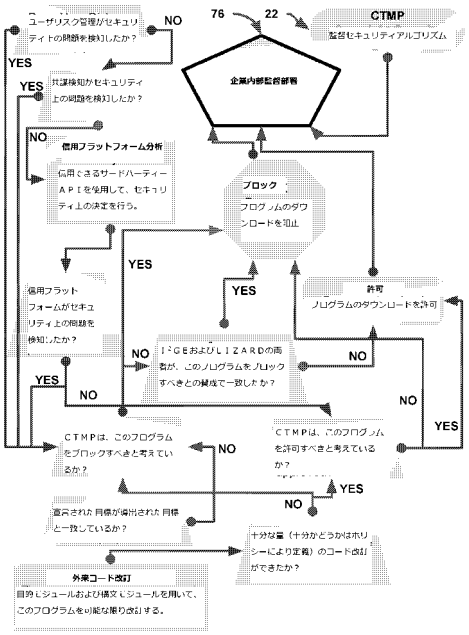
【図３０】



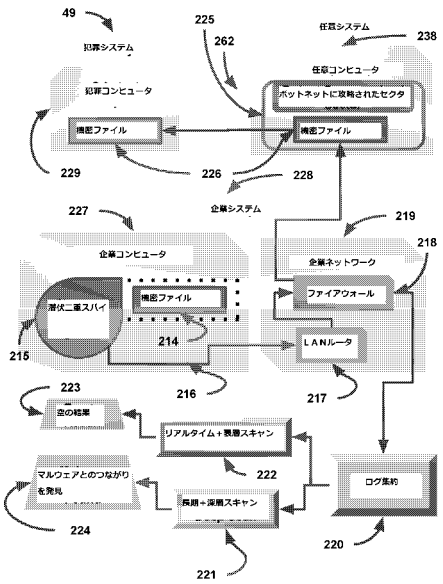
【図３１】



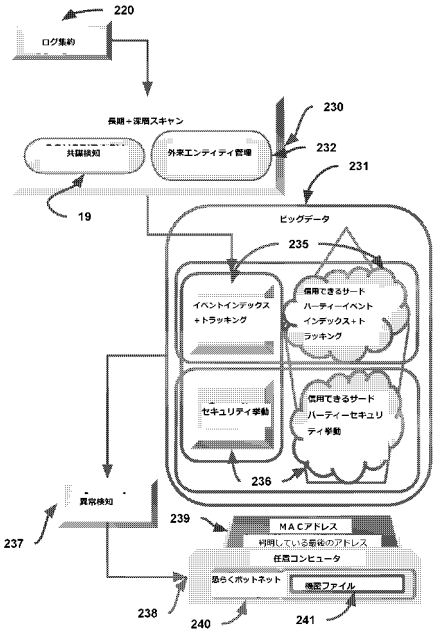
【図３２】



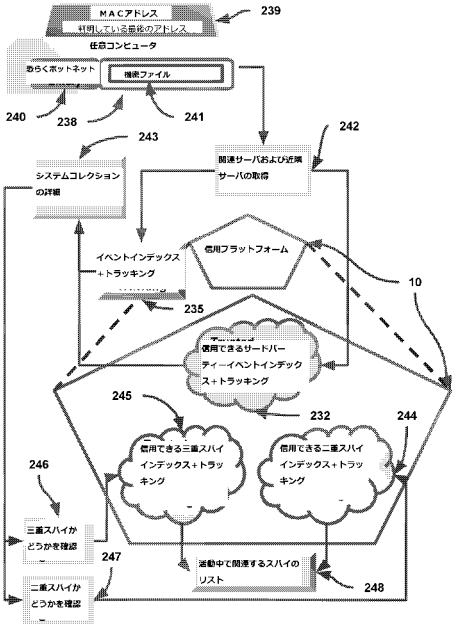
【図３３】



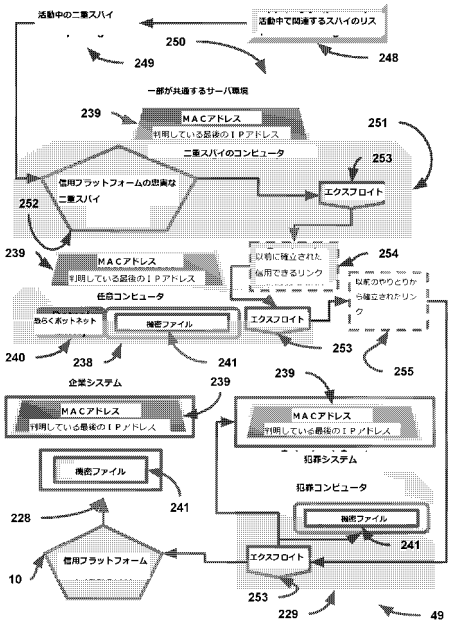
【図３４】



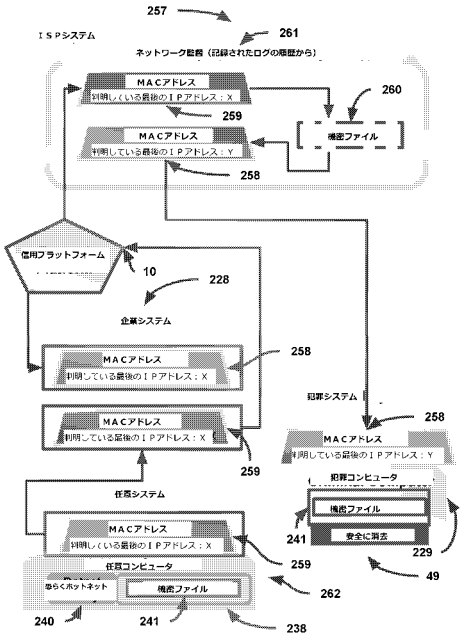
【図３５】



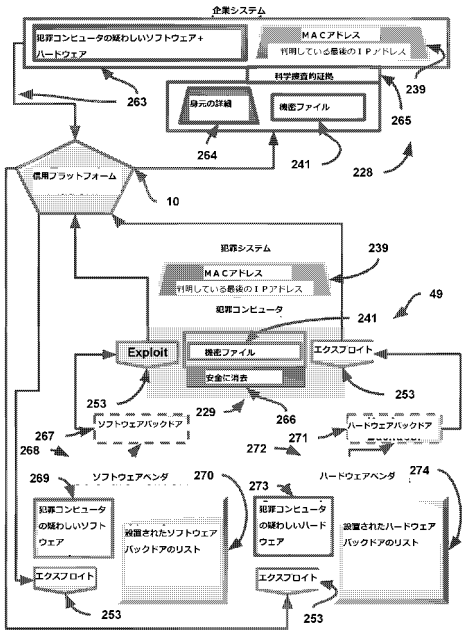
【図３６】



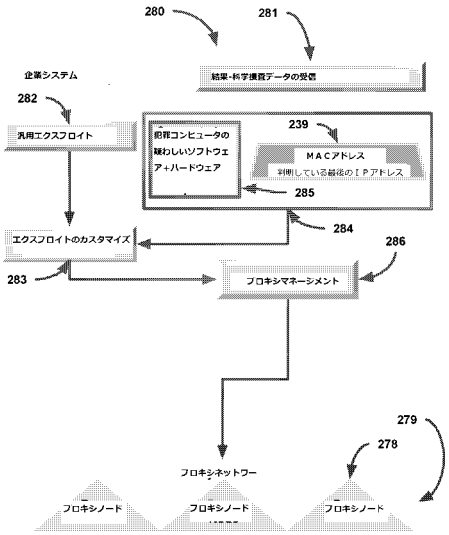
【図３７】



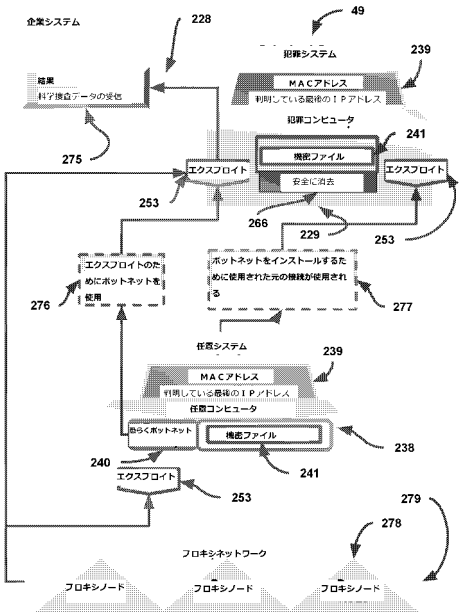
【図３８】



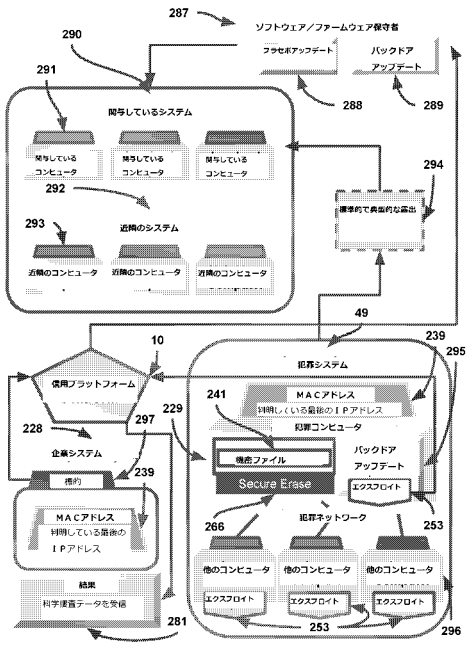
【図３９】



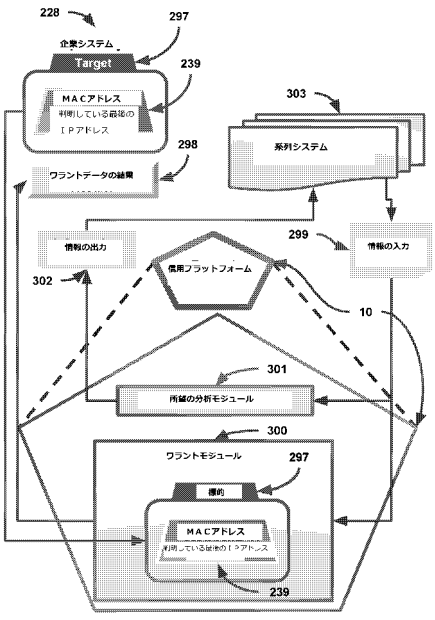
【図４０】



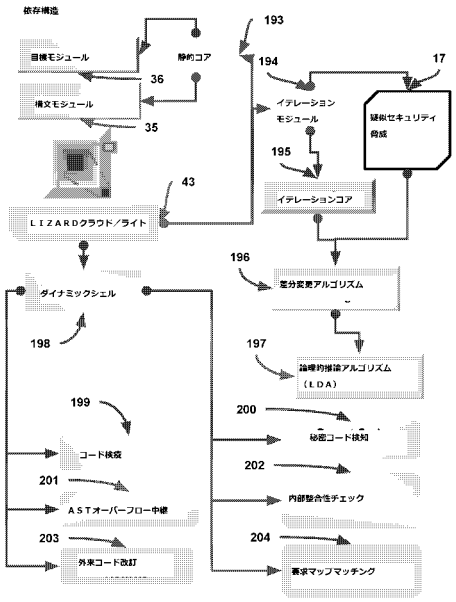
【図４１】



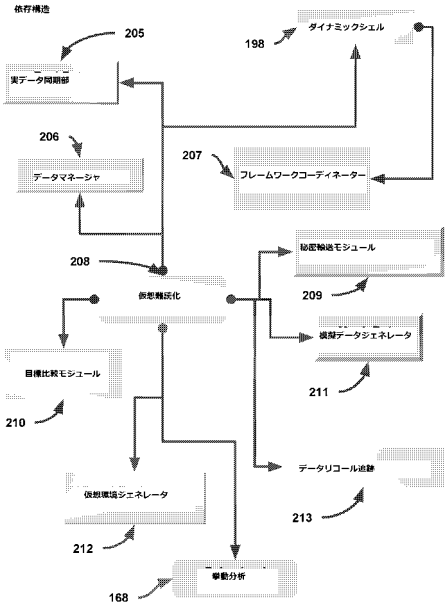
【図４２】



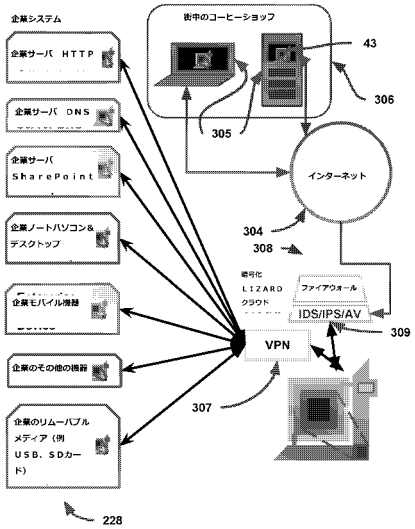
【図４３】



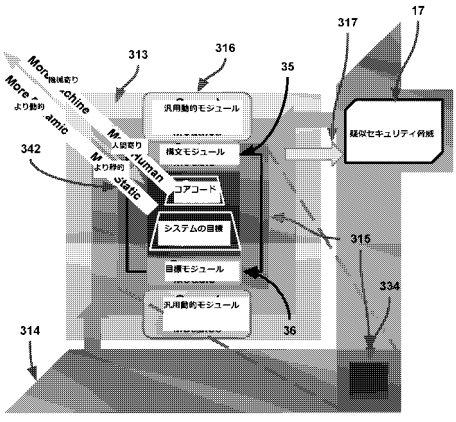
【図４４】



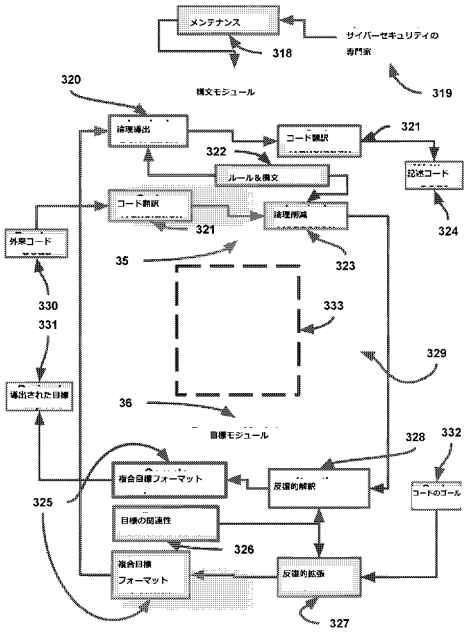
【図４５】



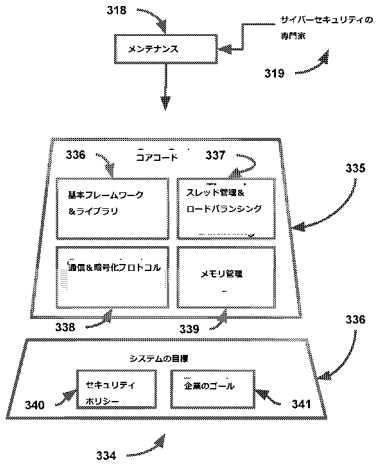
【図４６】



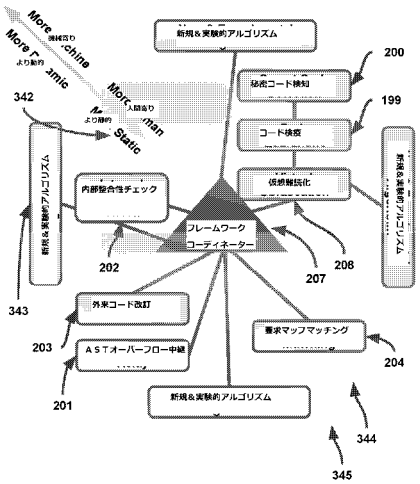
【図４７】



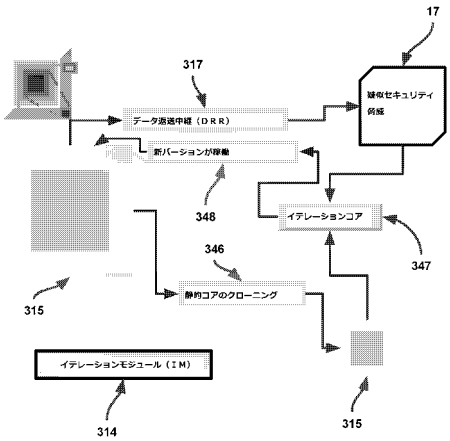
【図４８】



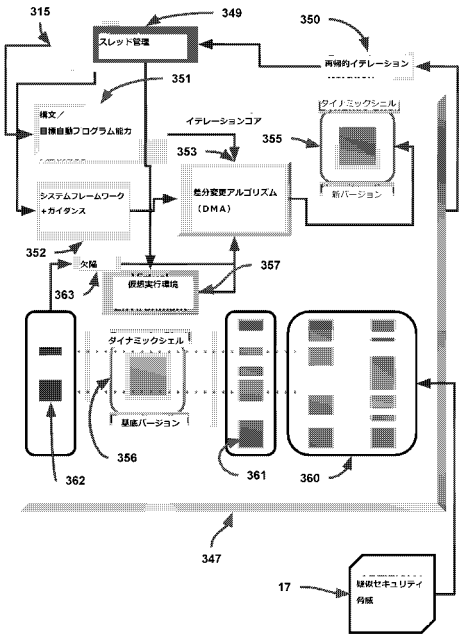
【図４９】



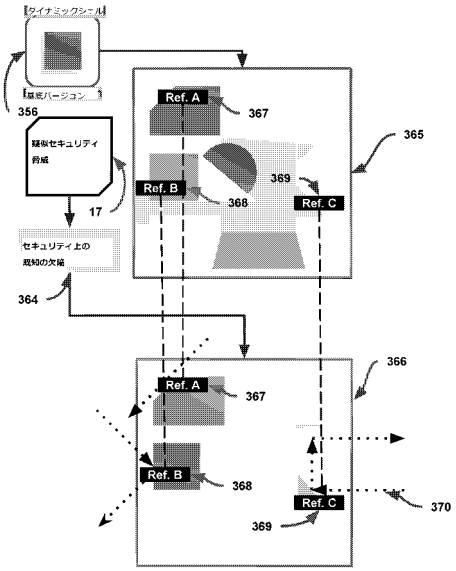
【図５０】



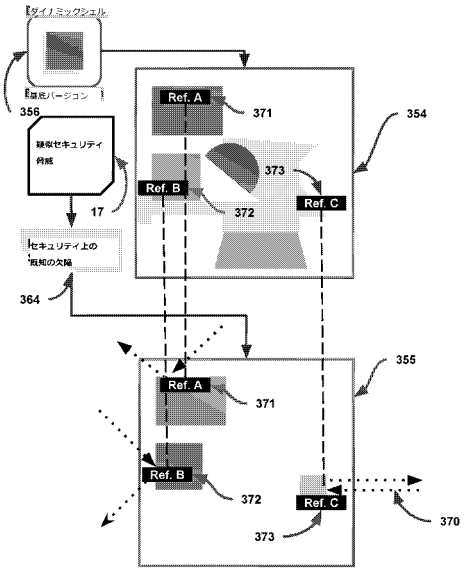
【図５１】



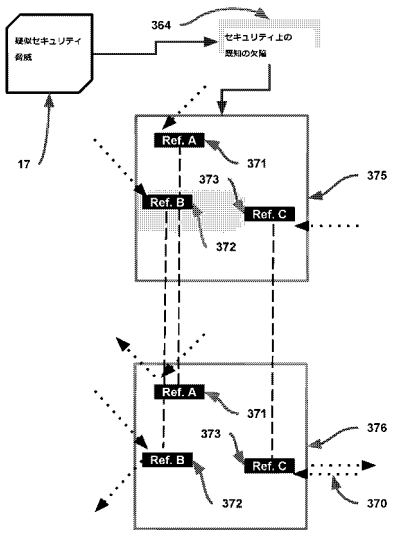
【図５２】



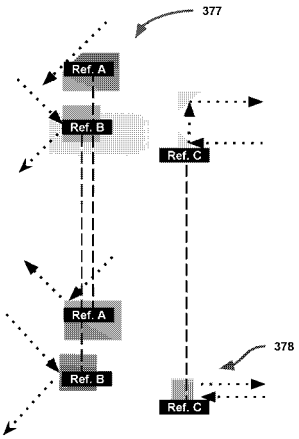
【図５３】



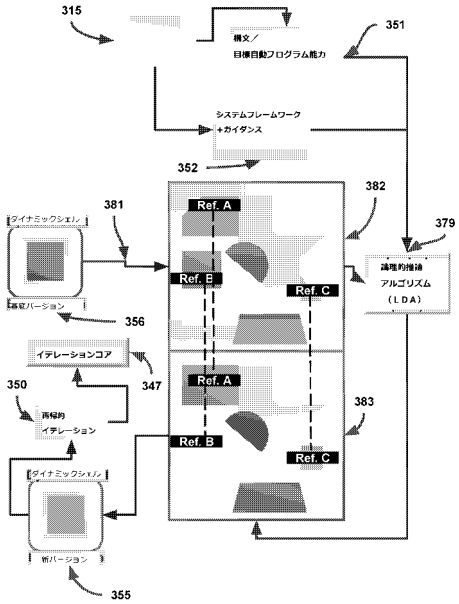
【図５４】



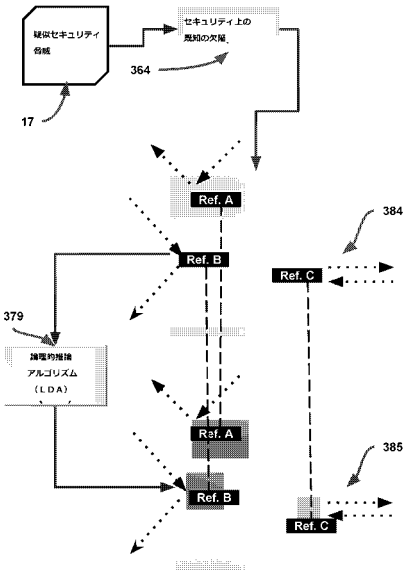
【図５５】



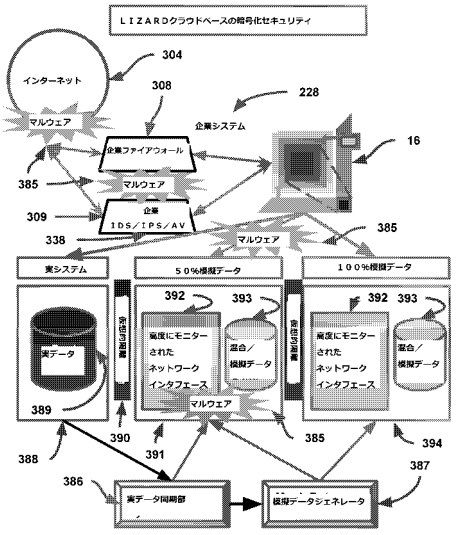
【図５６】



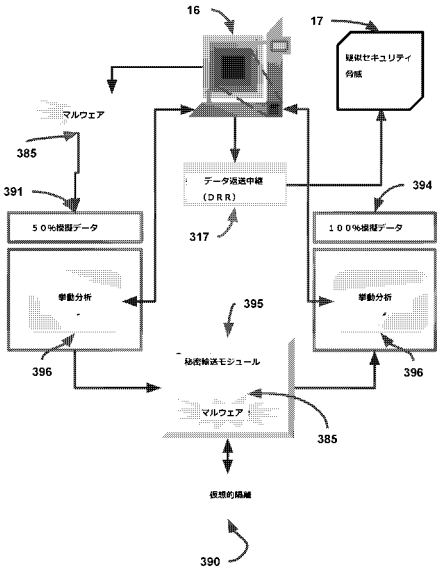
【図５７】



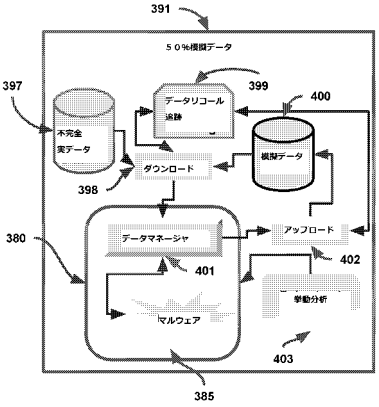
【図５８】



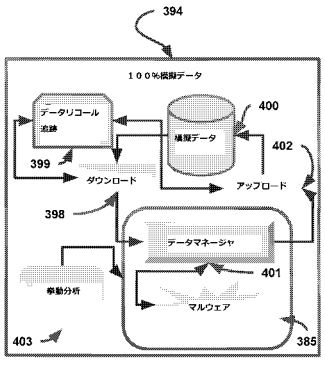
【図５９】



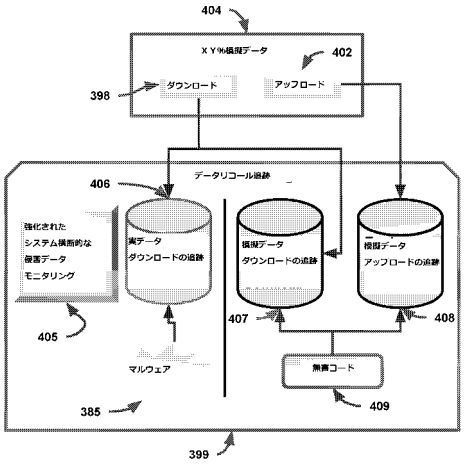
【図６０】



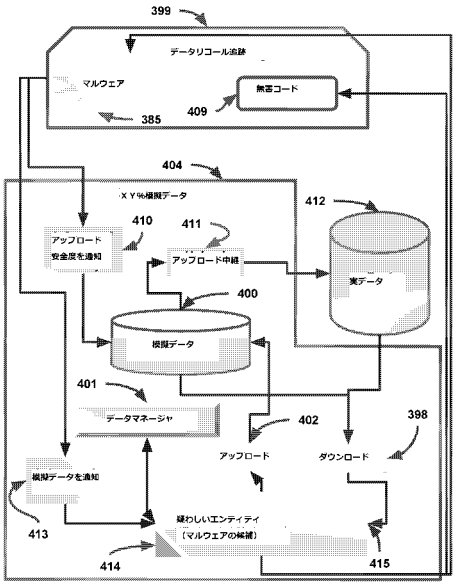
【図６１】



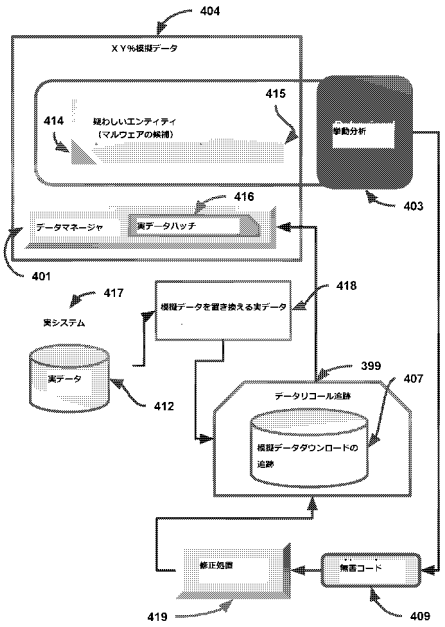
【図６２】



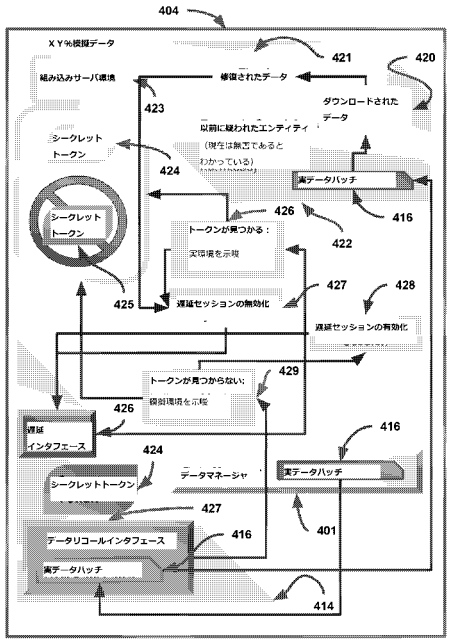
【図６３】



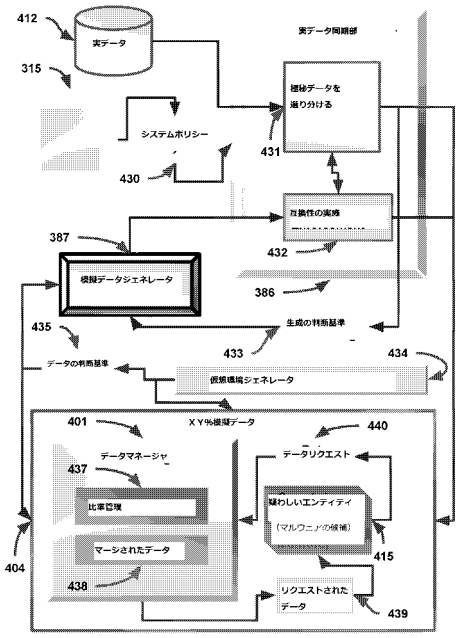
【図６４】



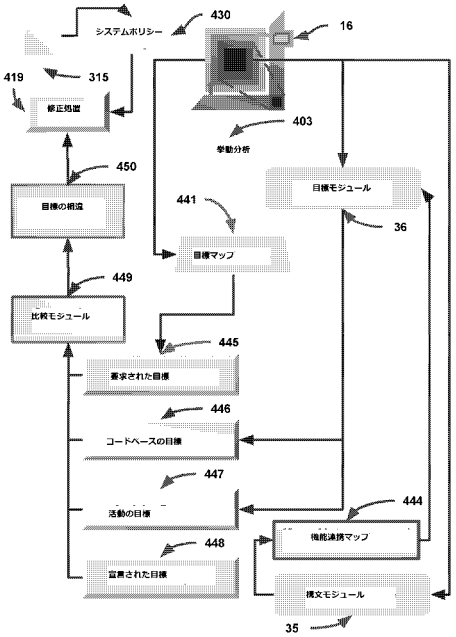
【図６５】



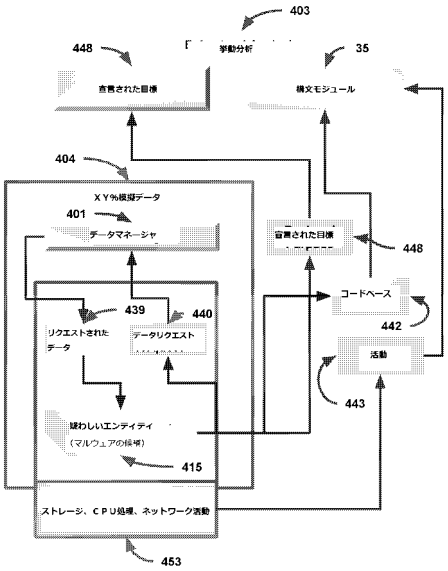
【図６６】



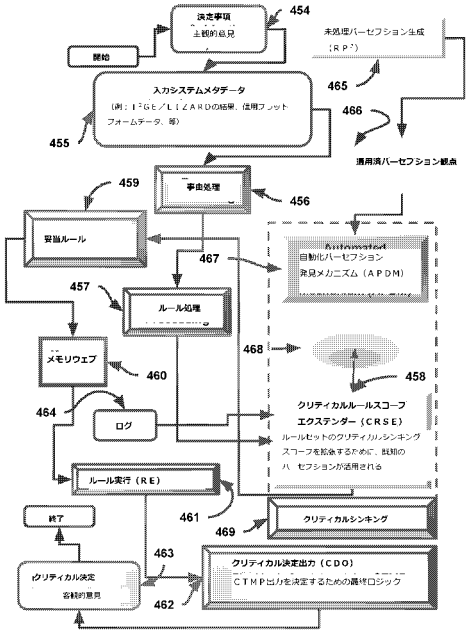
【図６７】



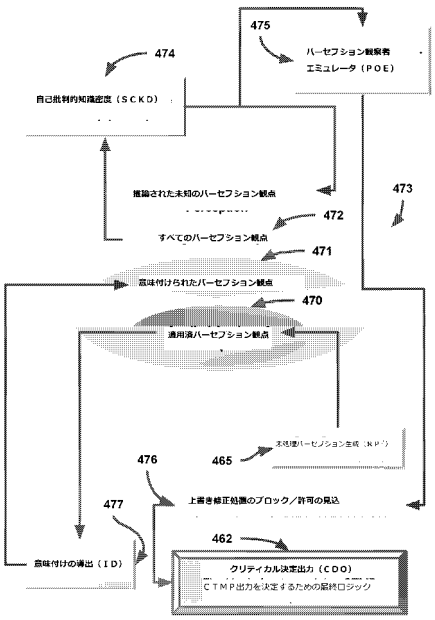
【図６８】



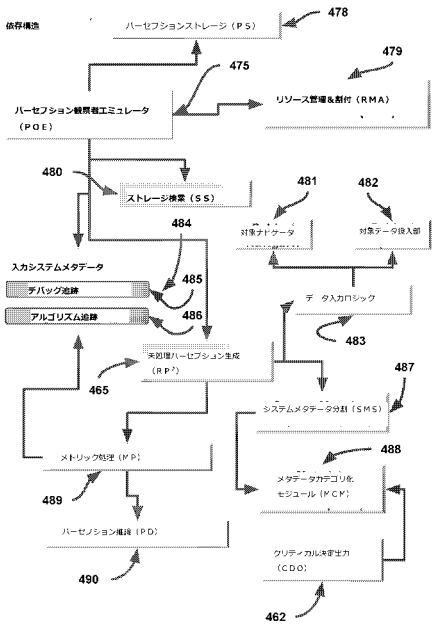
【図６９】



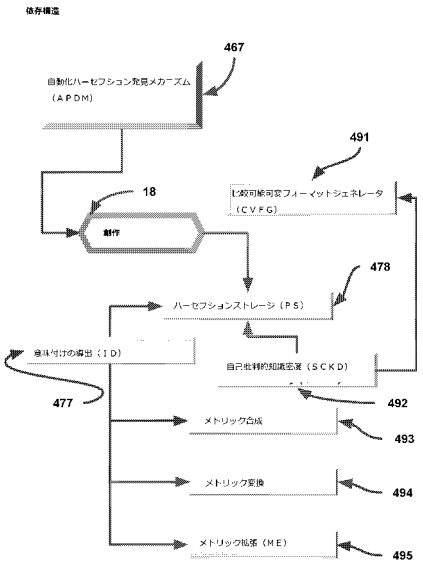
【図７０】



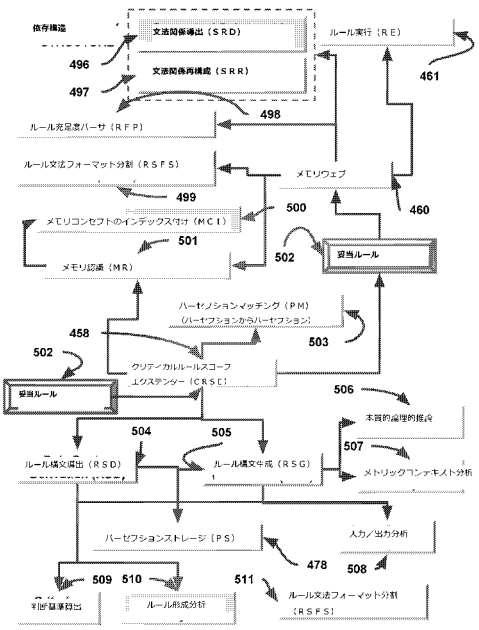
【図７１】



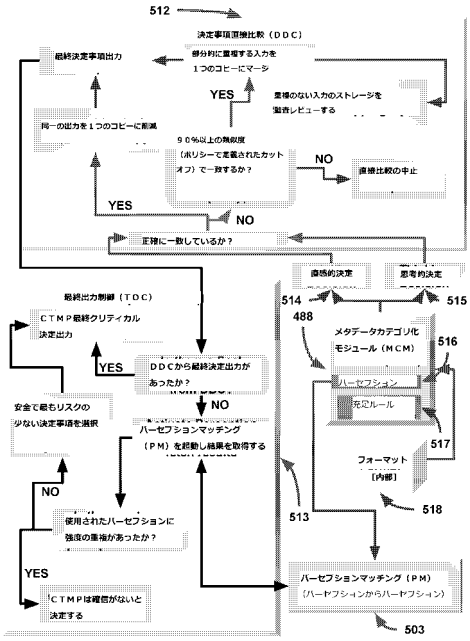
【図７２】



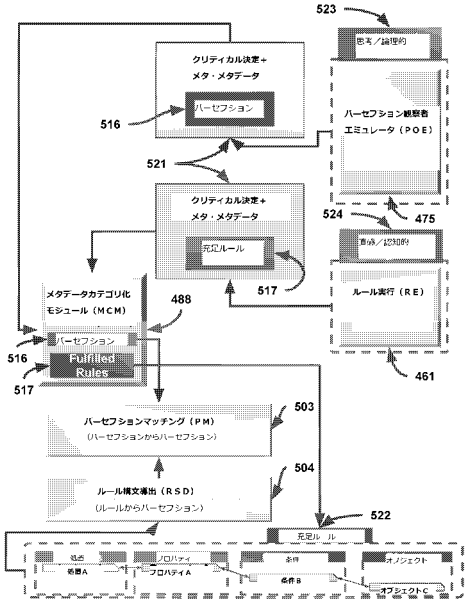
【図７３】



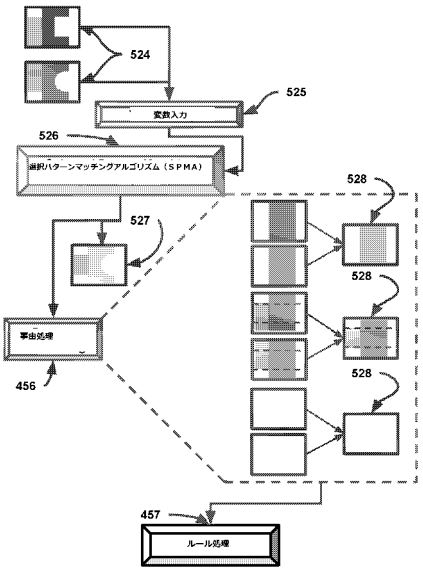
【図７４】



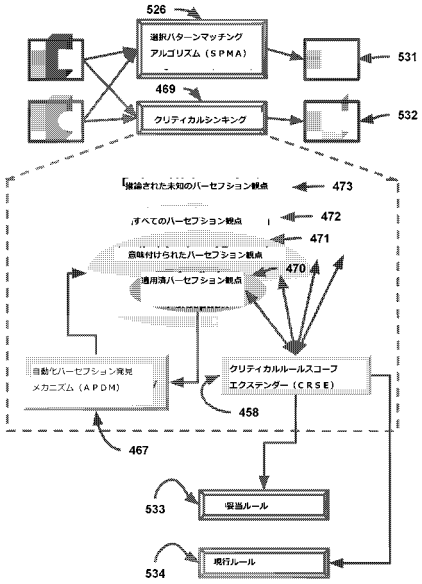
【図７５】



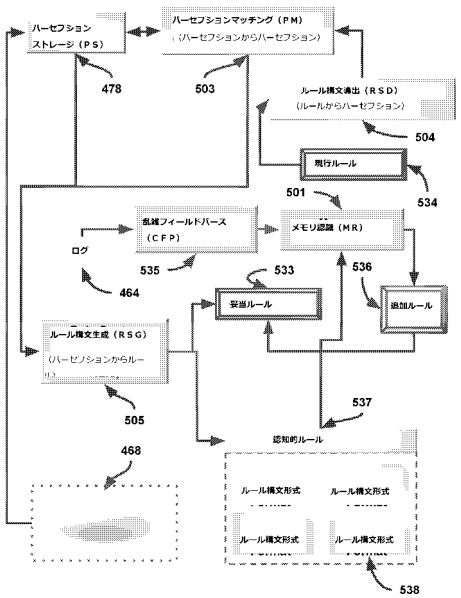
【図７６】



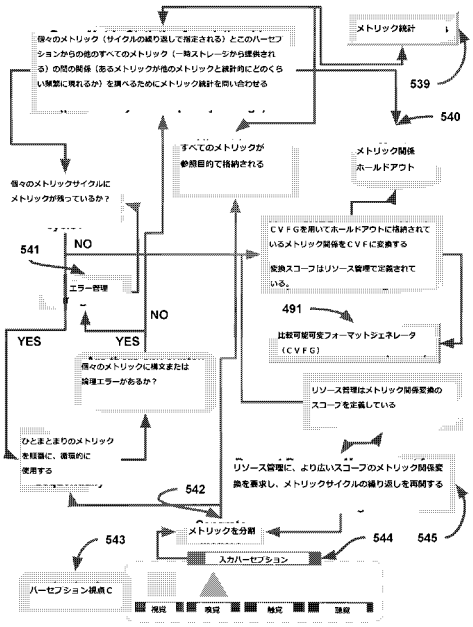
【図７７】



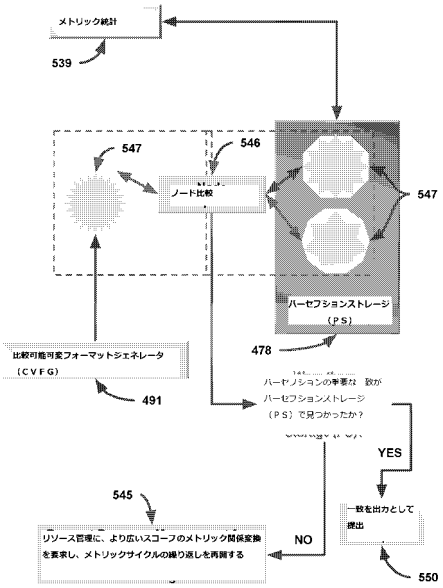
【図７８】



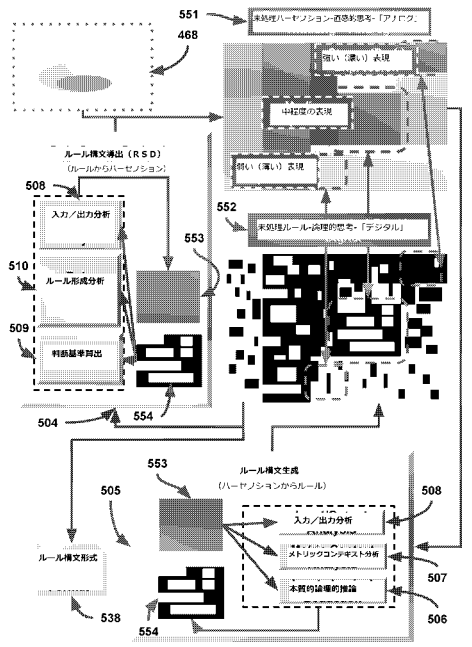
【図７９】



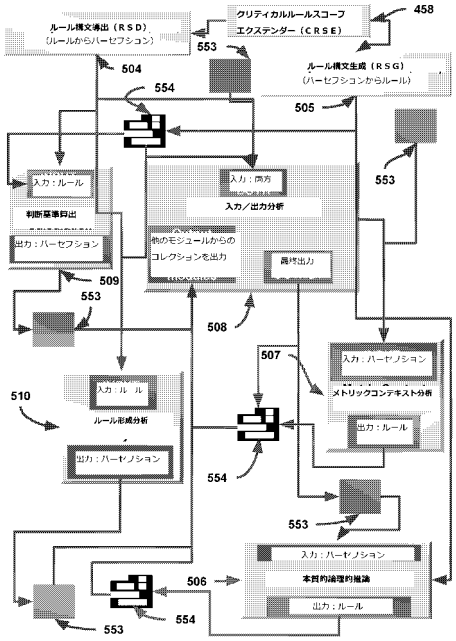
【図８０】



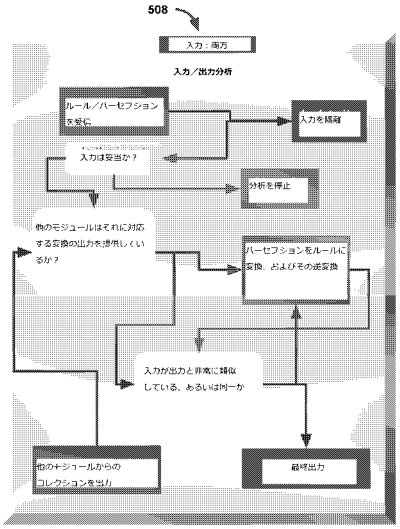
【図８１】



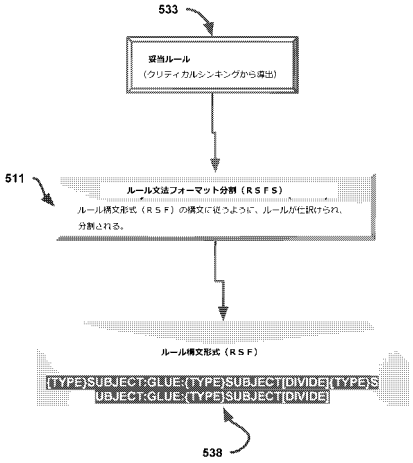
【図８２】



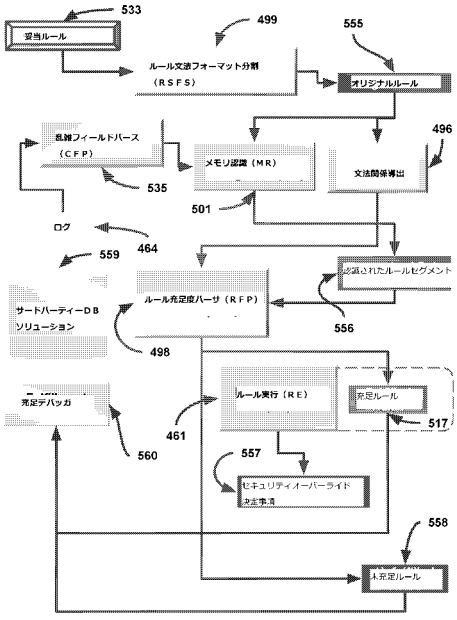
【図８３】



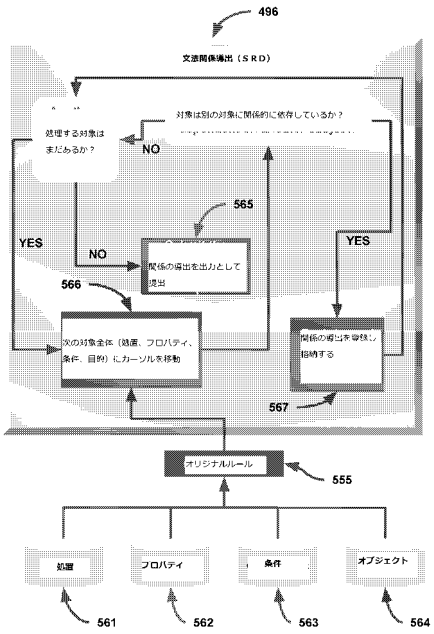
【図８４】



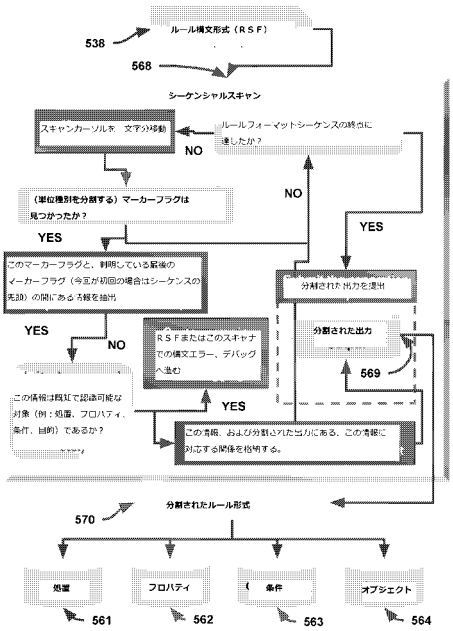
【図８５】



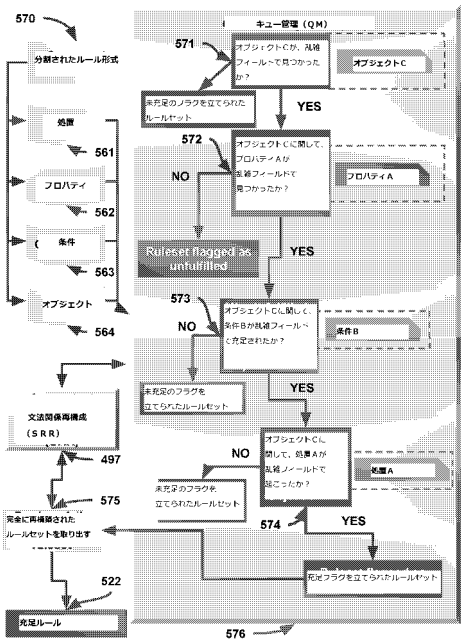
【図８６】



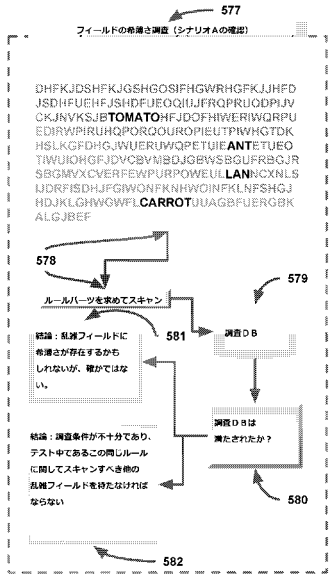
【図８７】



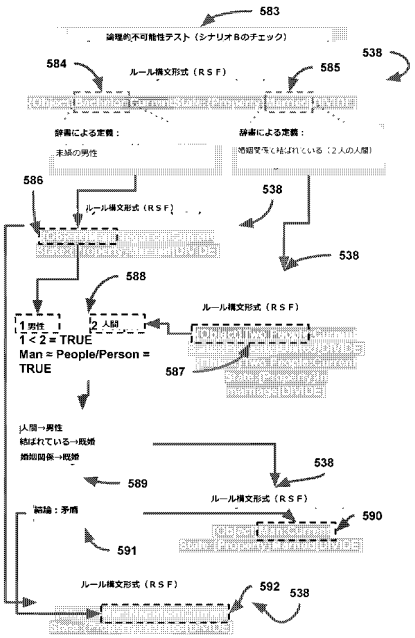
【図８８】



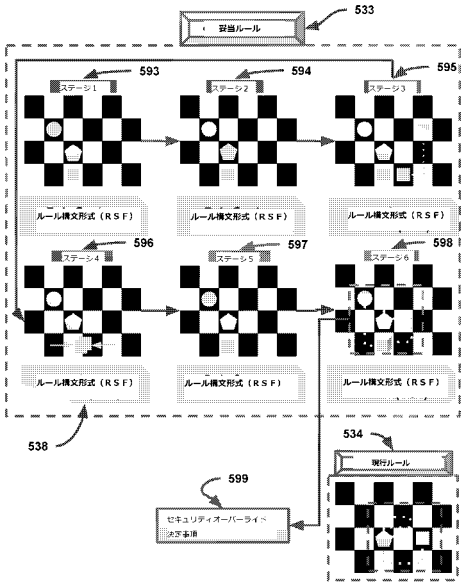
【図８９】



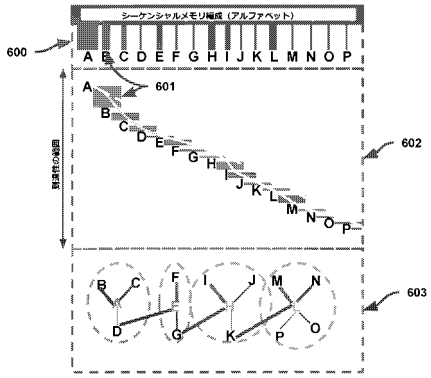
【図９０】



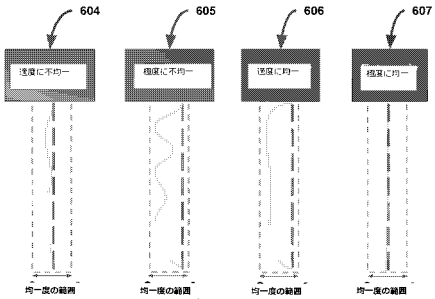
【図９１】



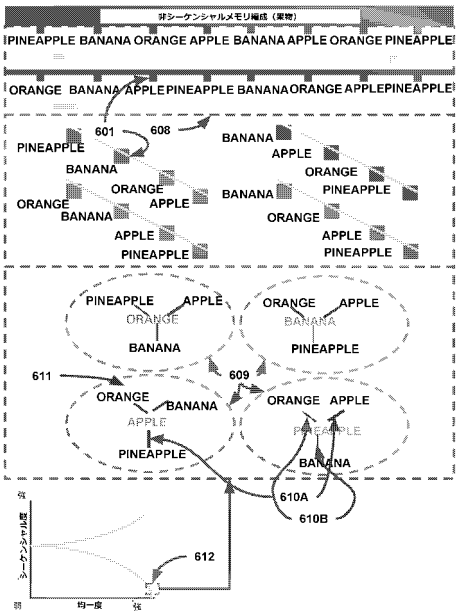
【図９２】



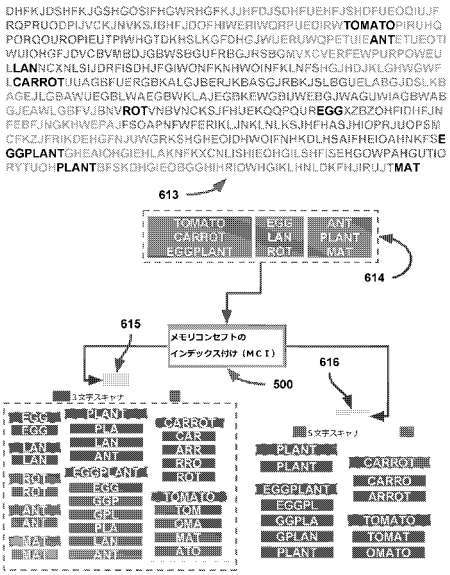
【図９３】



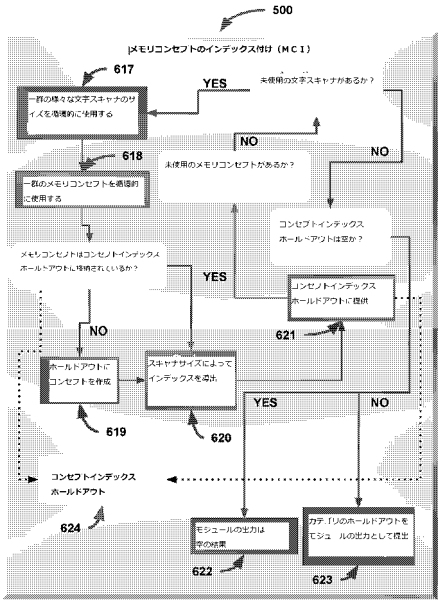
【図９４】



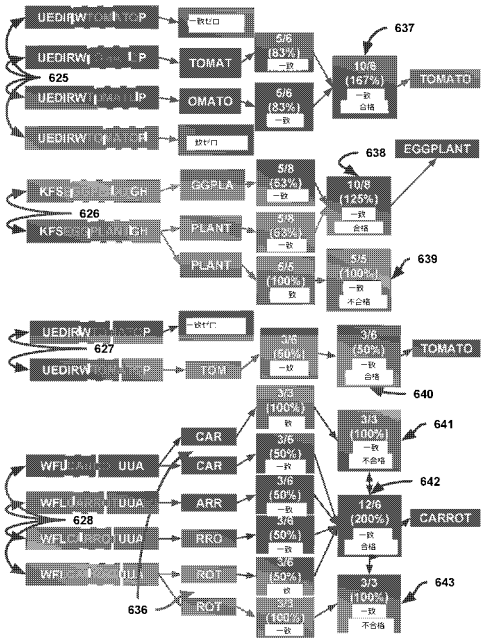
【図９５】



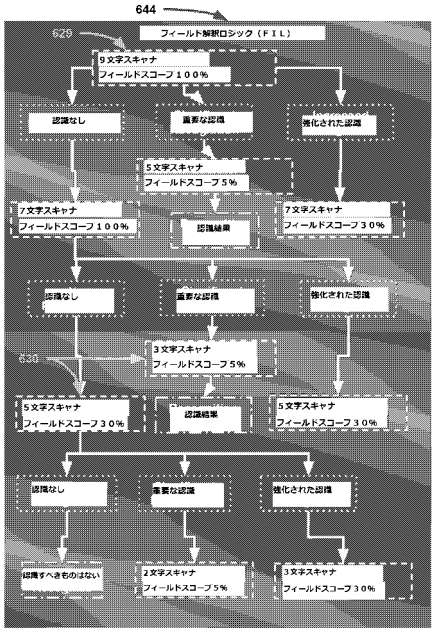
【図９６】



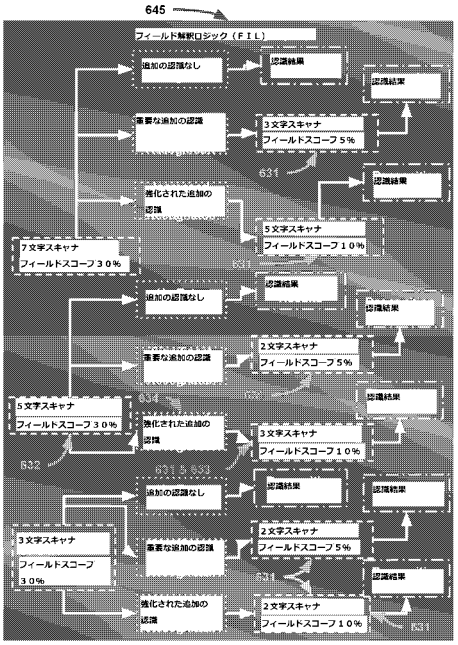
【図９７】



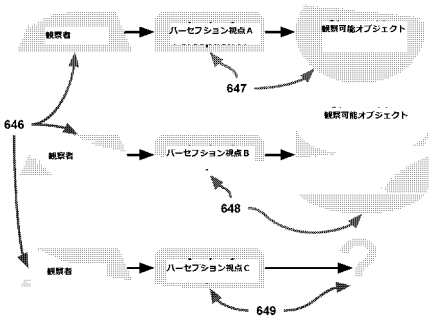
【図９８】



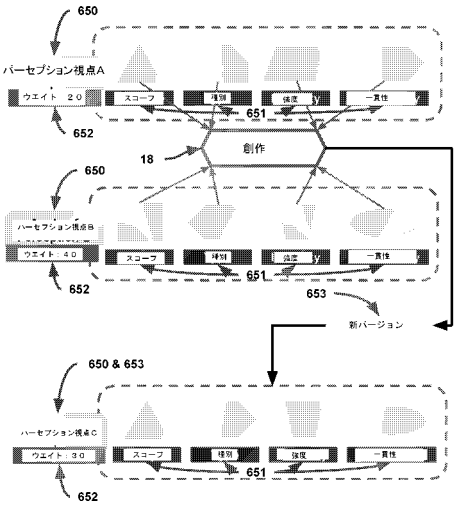
【図９９】



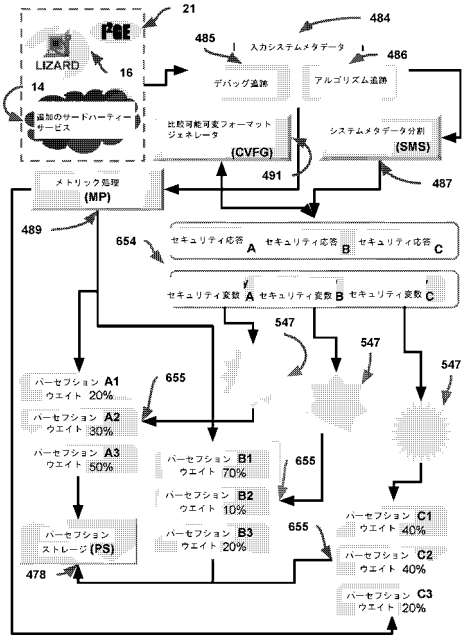
【図１００】



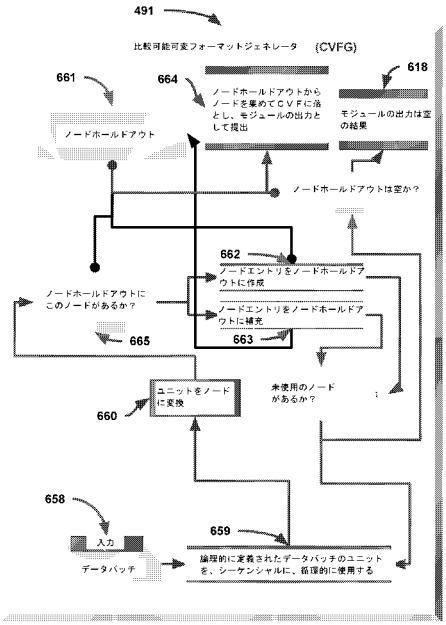
【図１０１】



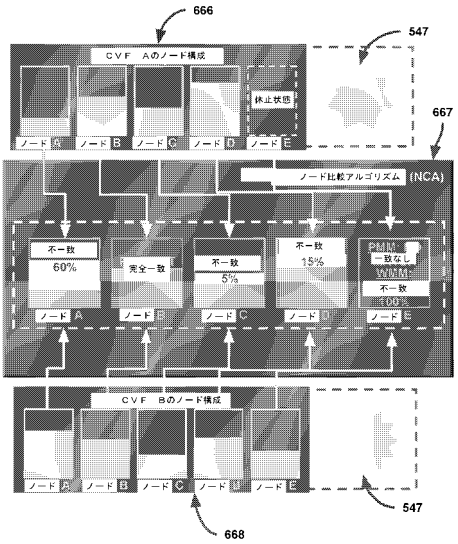
【図１０２】



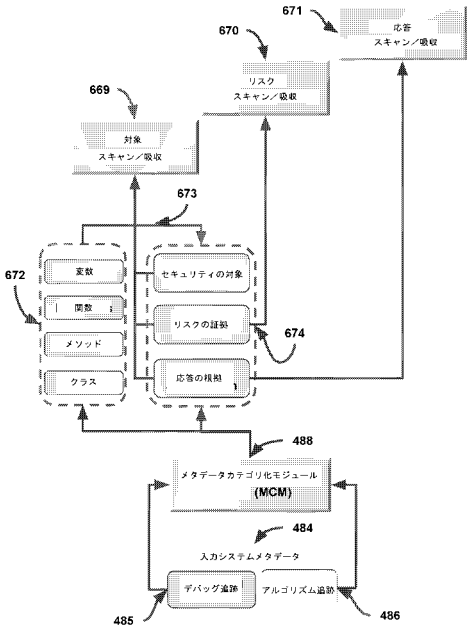
【図１０３】



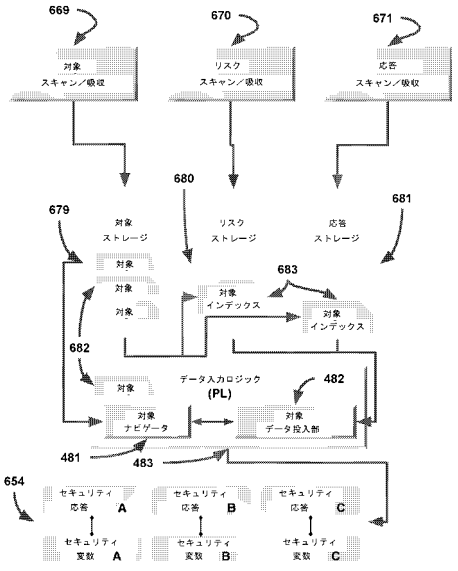
【図１０４】



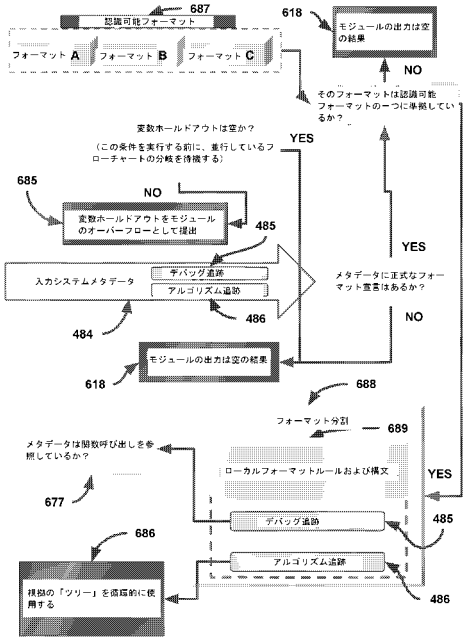
【図１０５】



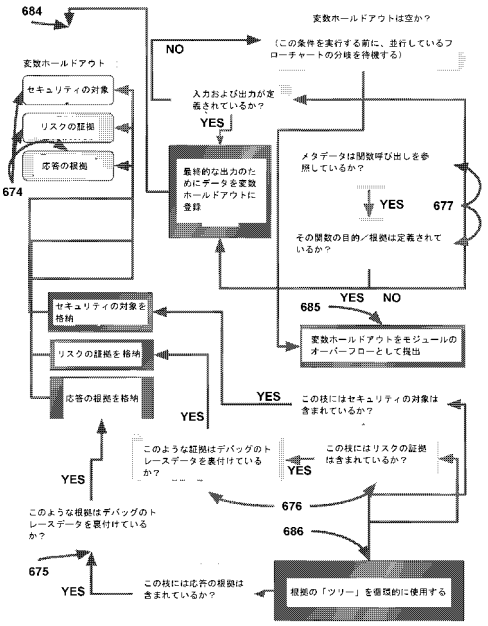
【図１０６】



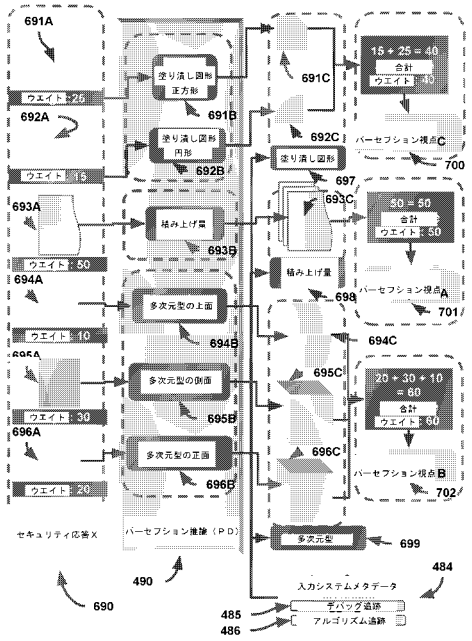
【図１０７】



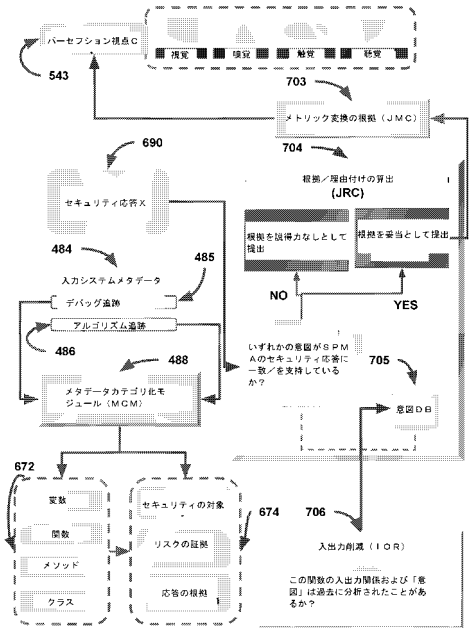
【図１０８】



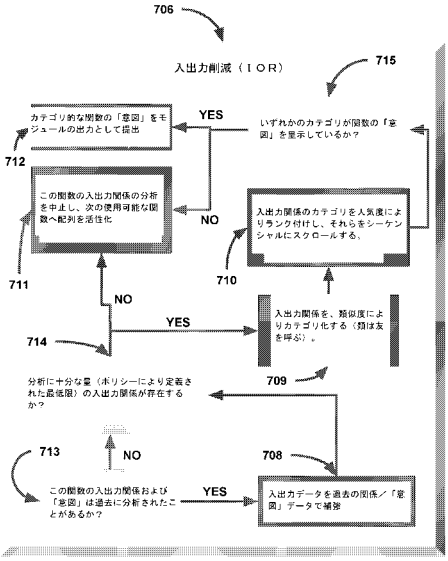
【図１０９】



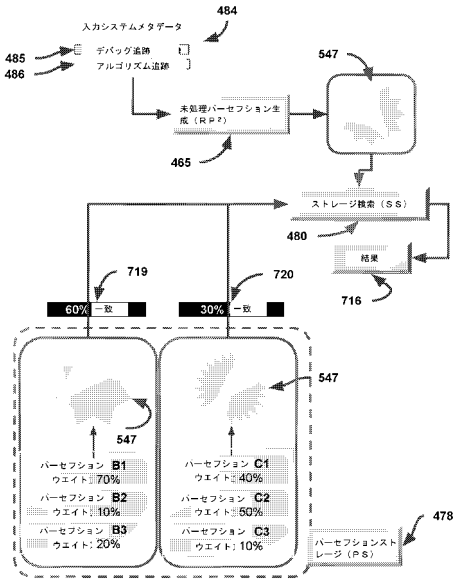
【図１１０】



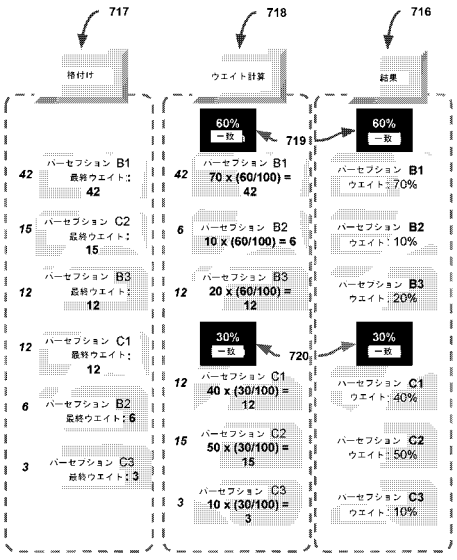
【図１１１】



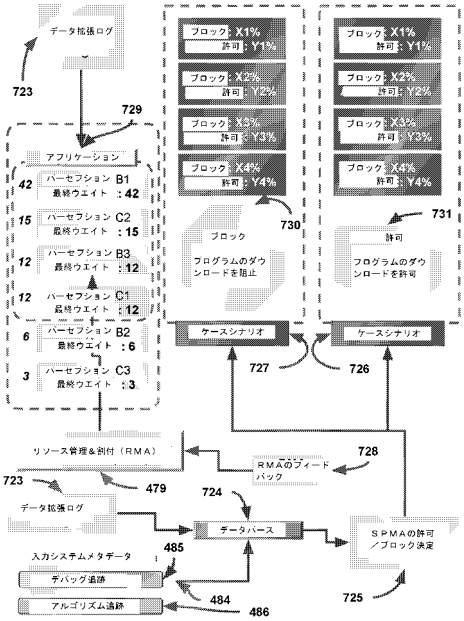
【図１１２】



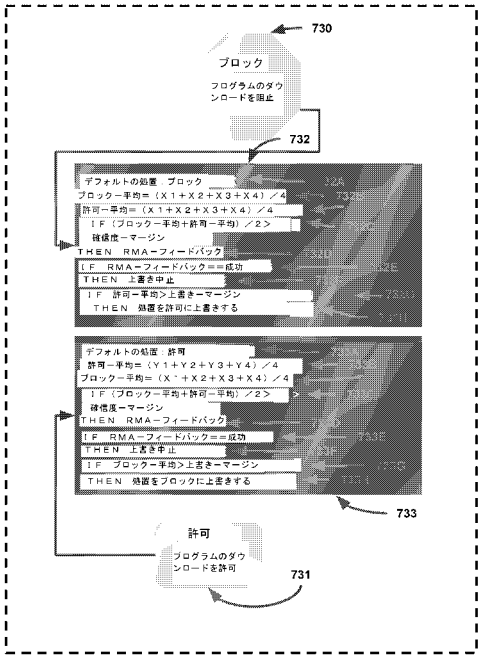
【図１１３】



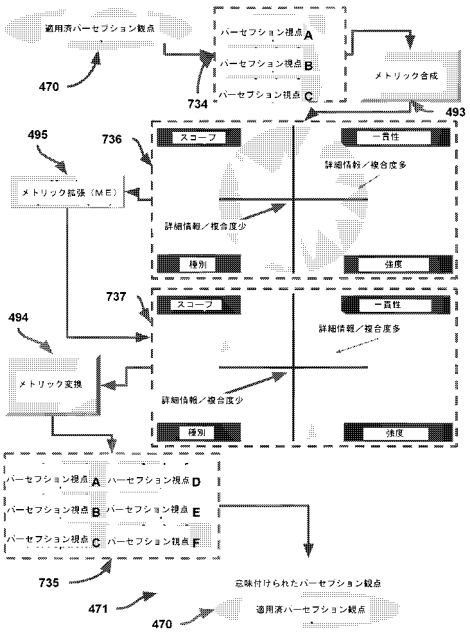
【図１１４】



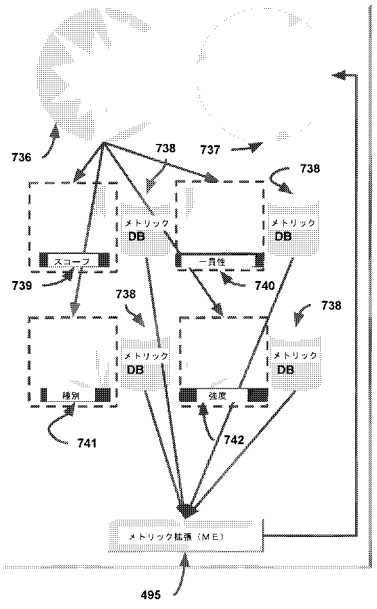
【図１１５】



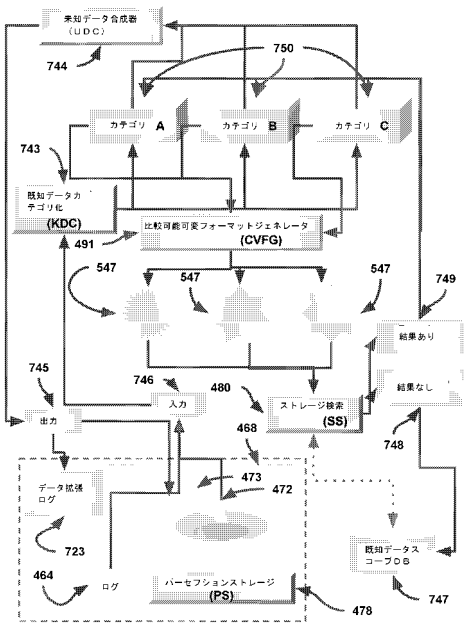
【図１１６】



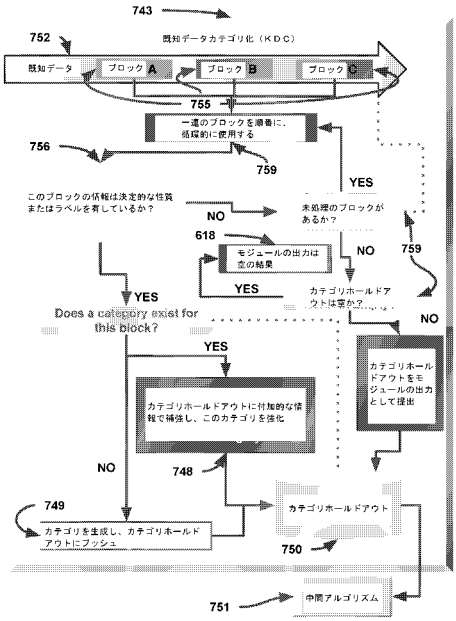
【図１１７】



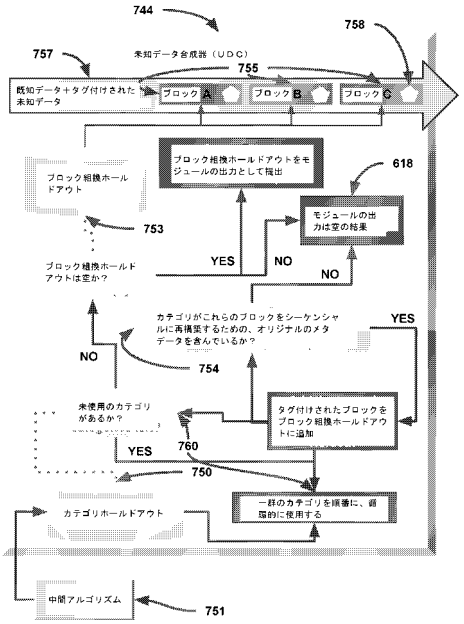
【図１１８】



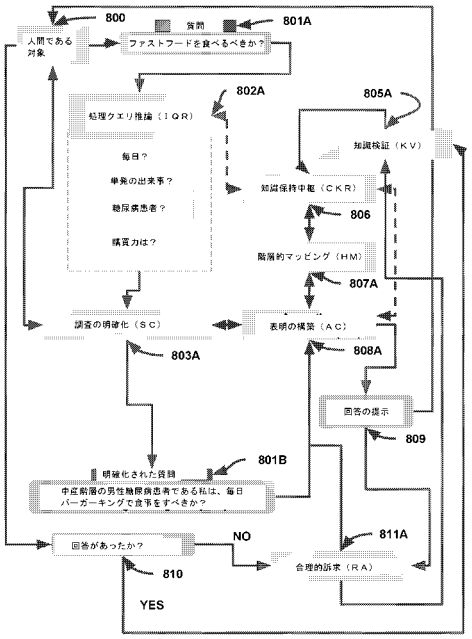
【図１１９】



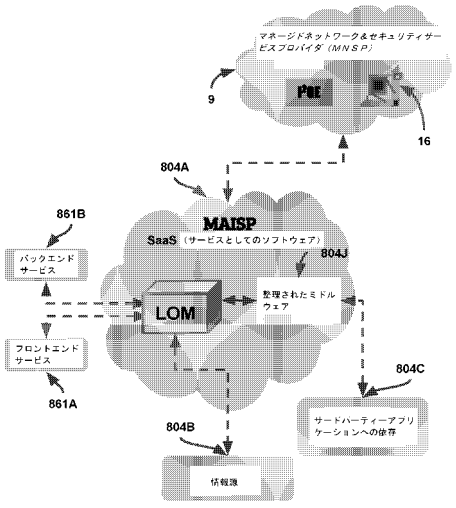
【図１２０】



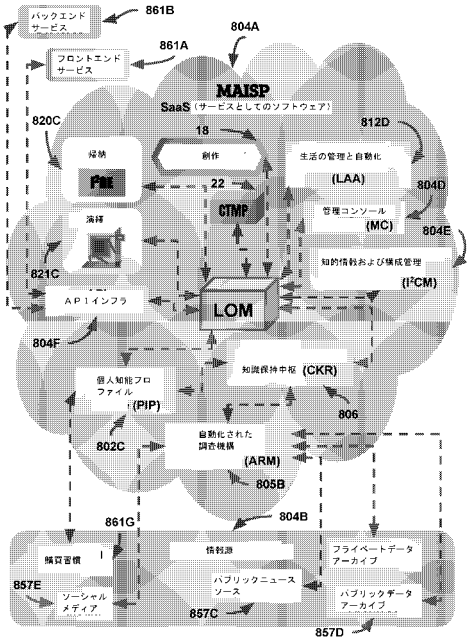
【図１２１】



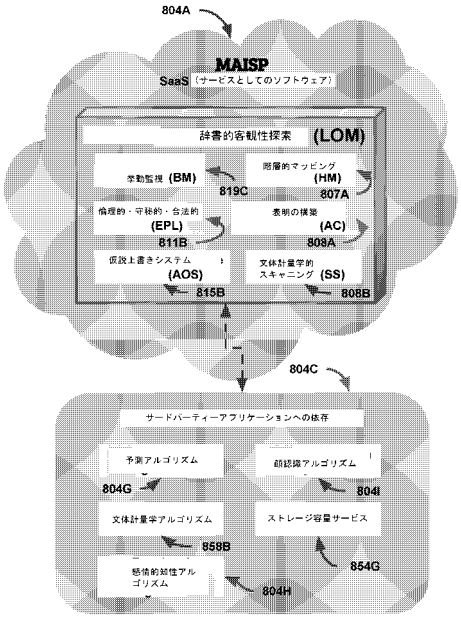
【図１２２】



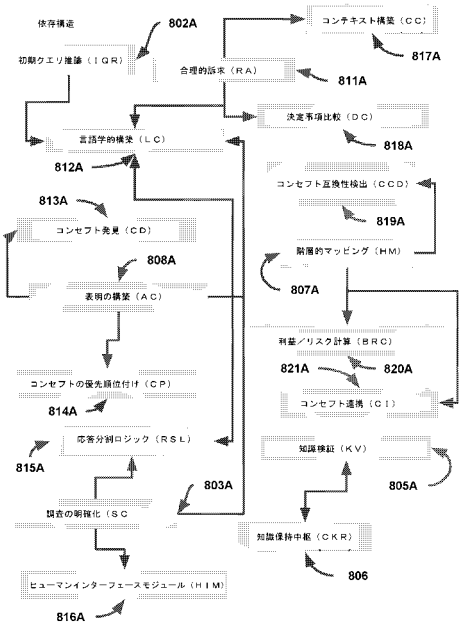
【図１２３】



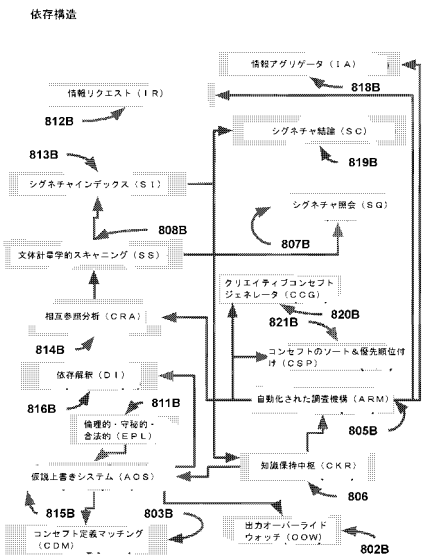
【図１２４】



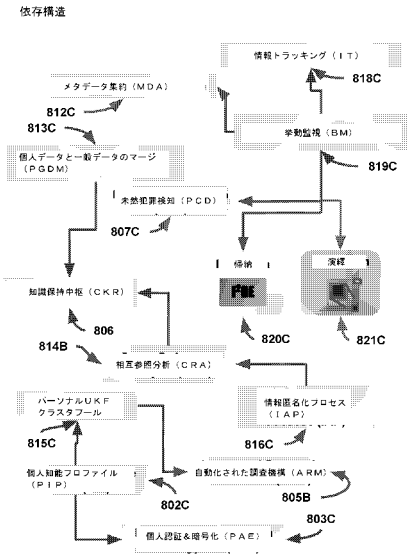
【図１２５】



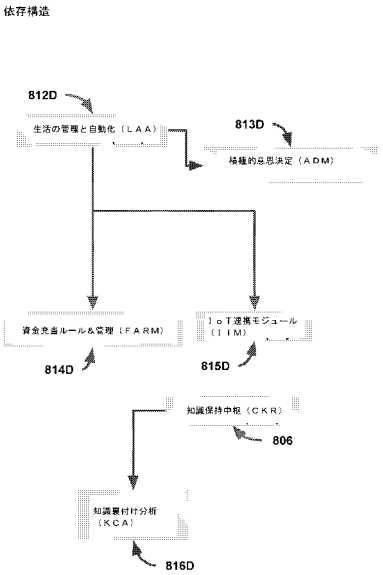
【図１２６】



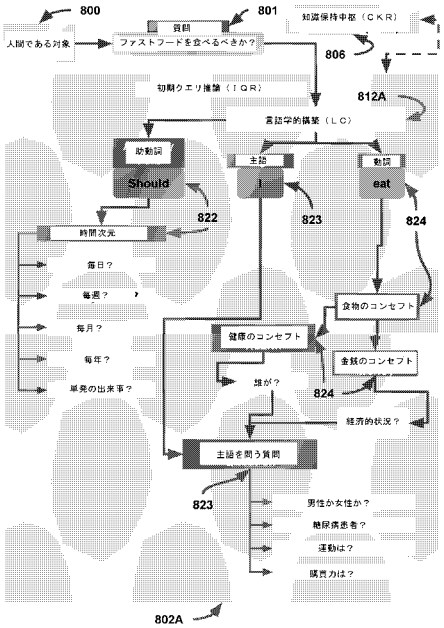
【図１２７】



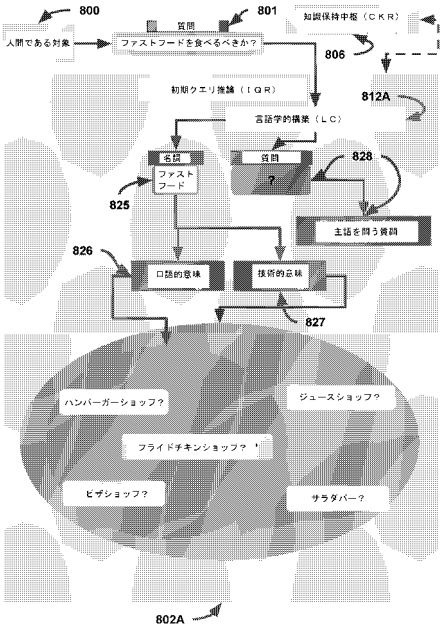
【図１２８】



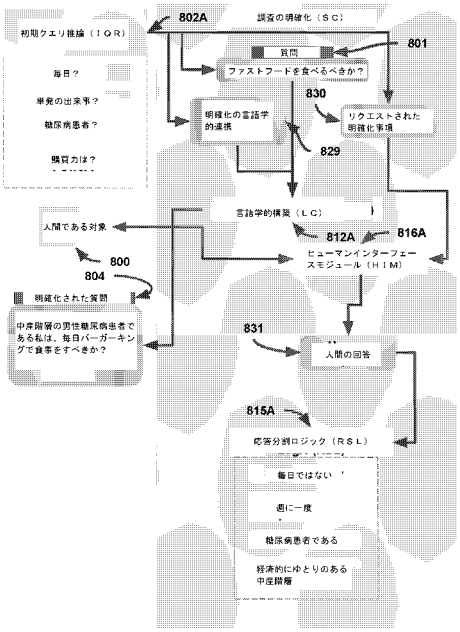
【図１２９】



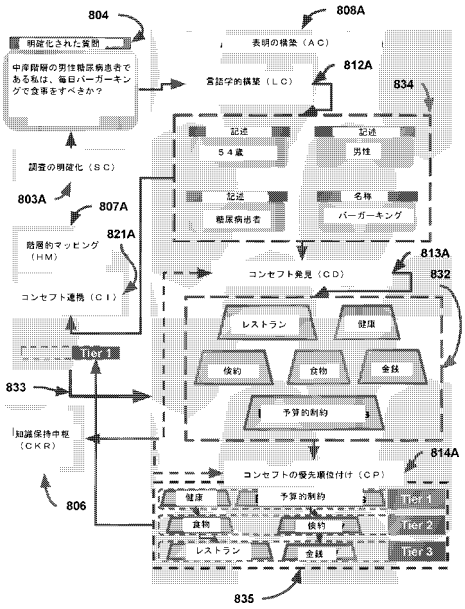
【図１３０】



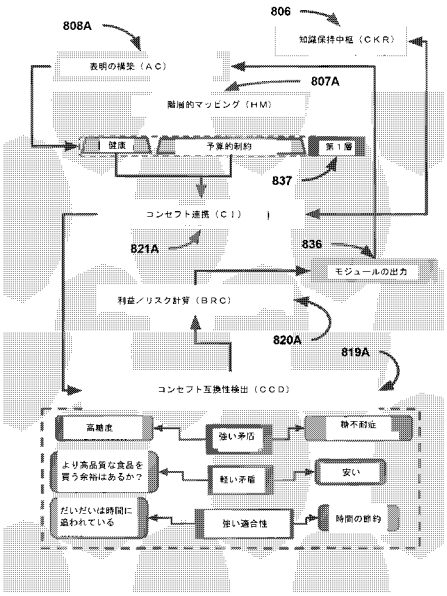
【図１３１】



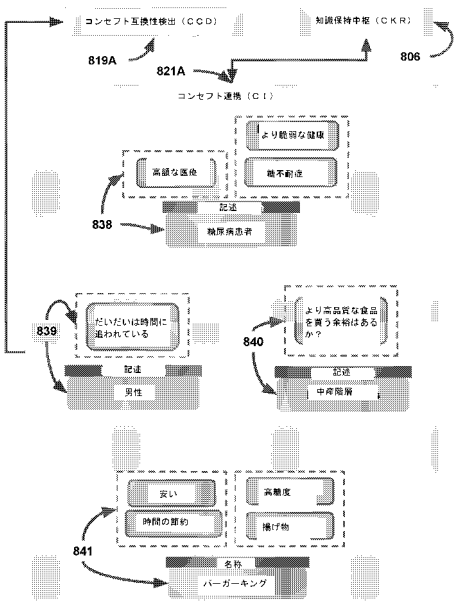
【図１３２】



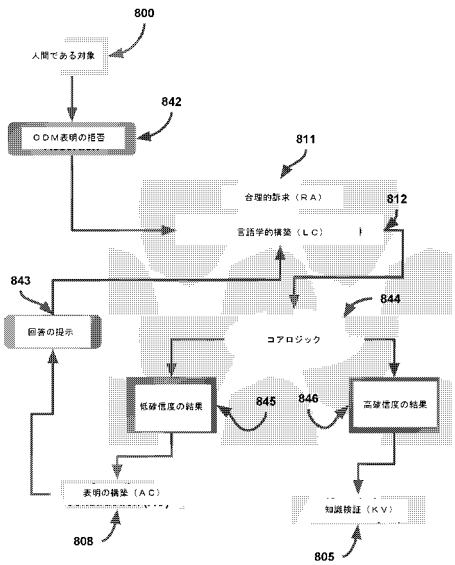
【図１３３】



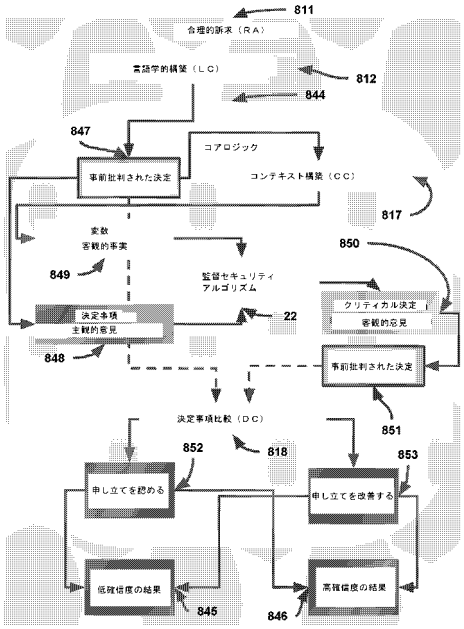
【図１３４】



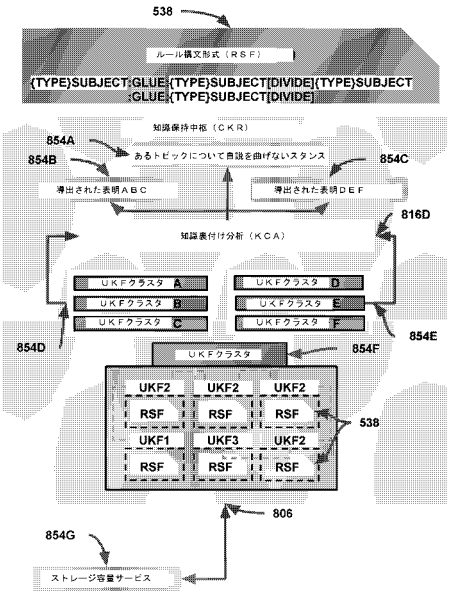
【図１３５】



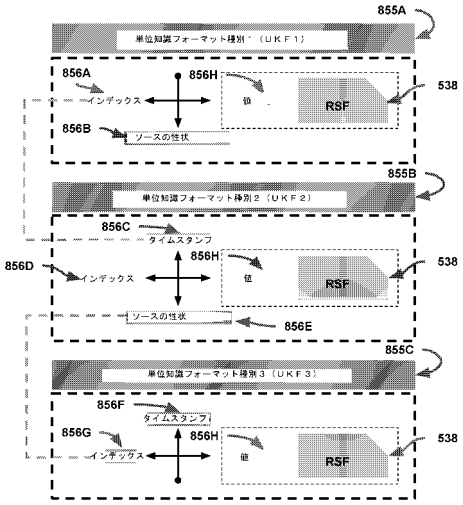
【図１３６】



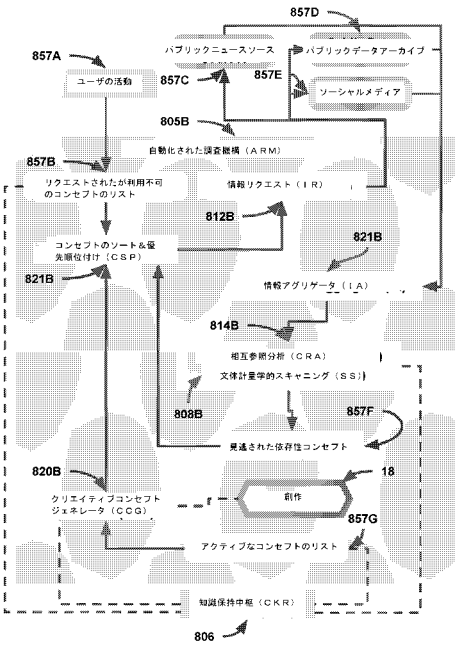
【図１３７】



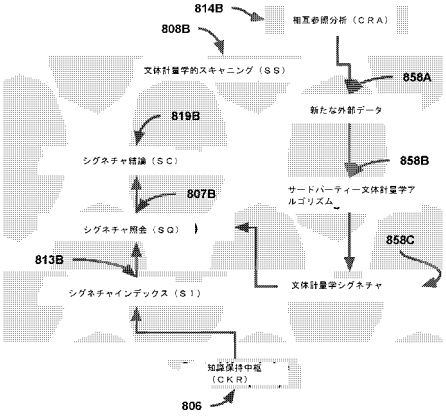
【図１３８】



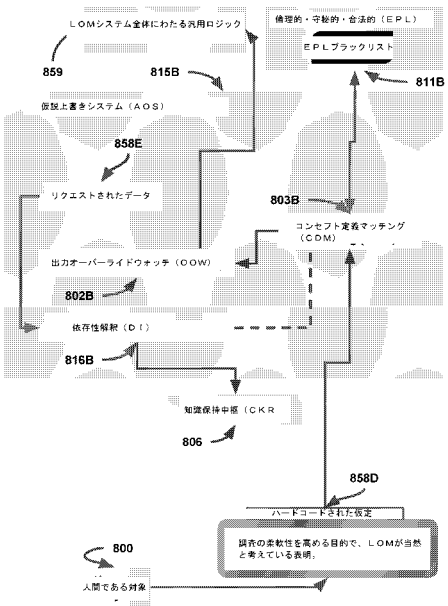
【図１３９】



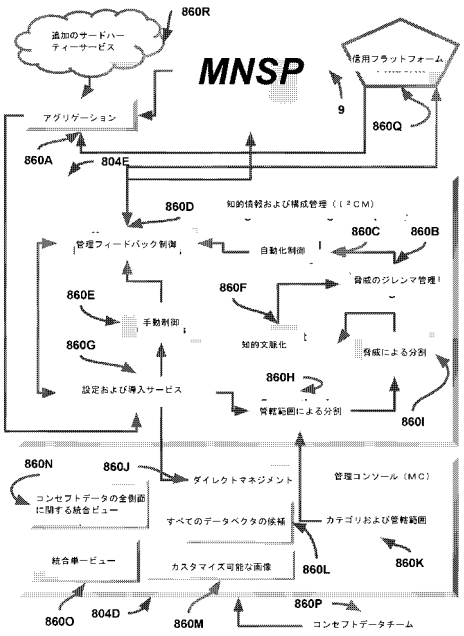
【図１４０】



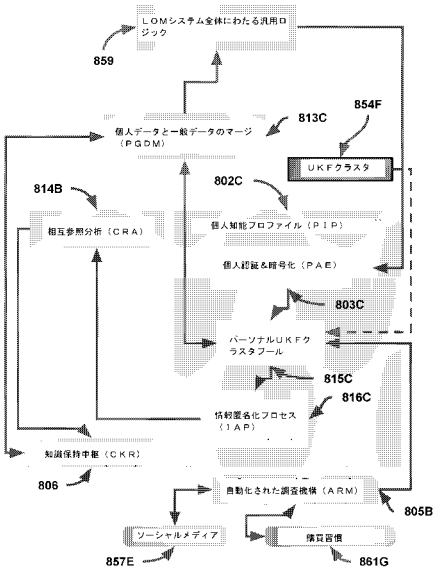
【図１４１】



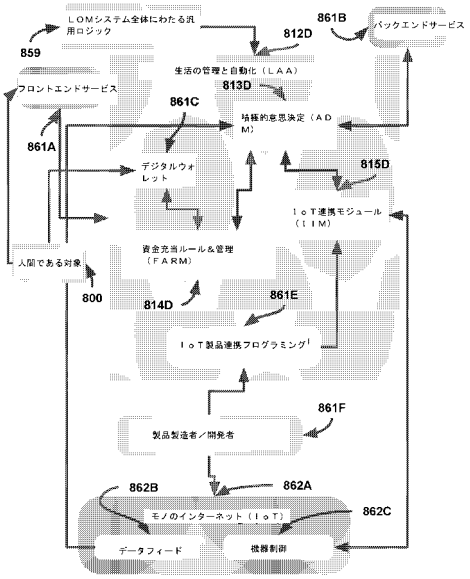
【図１４２】



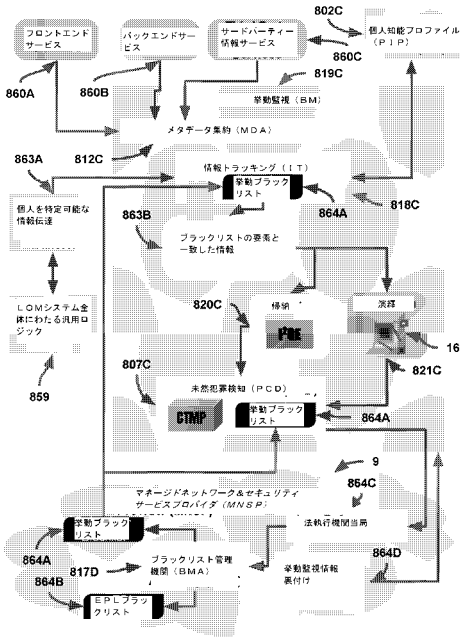
【図１４３】



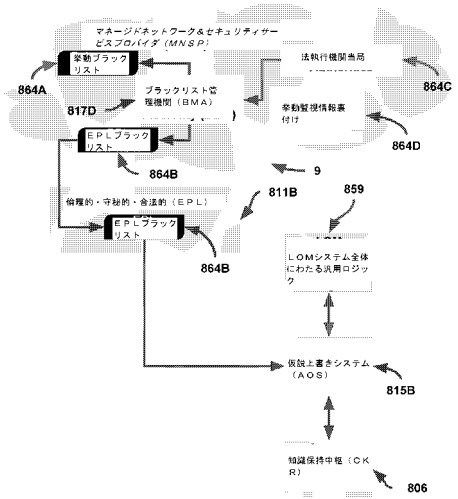
【図１４４】



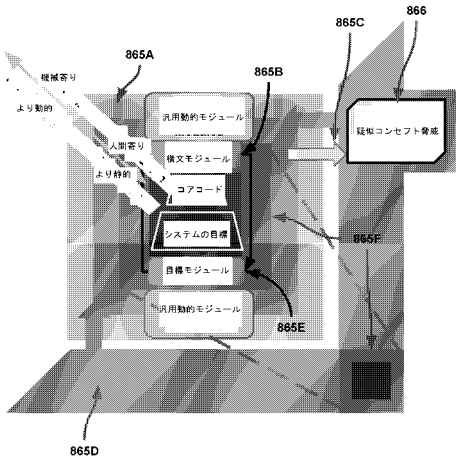
【図１４５】



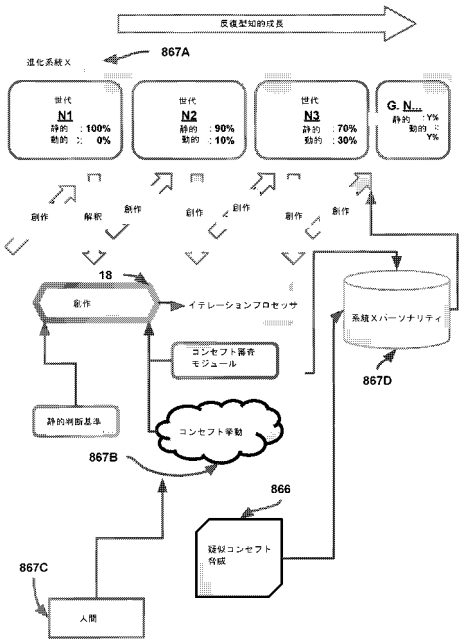
【図１４６】



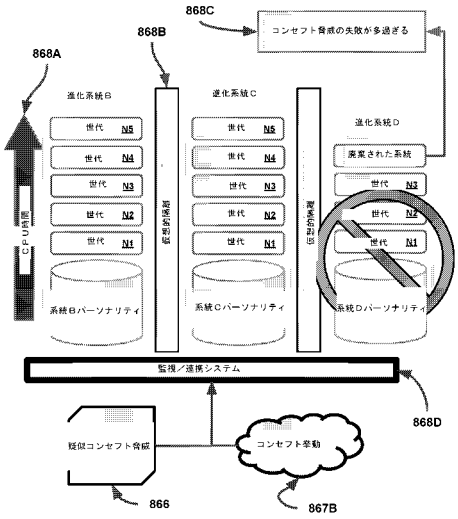
【図１４７】



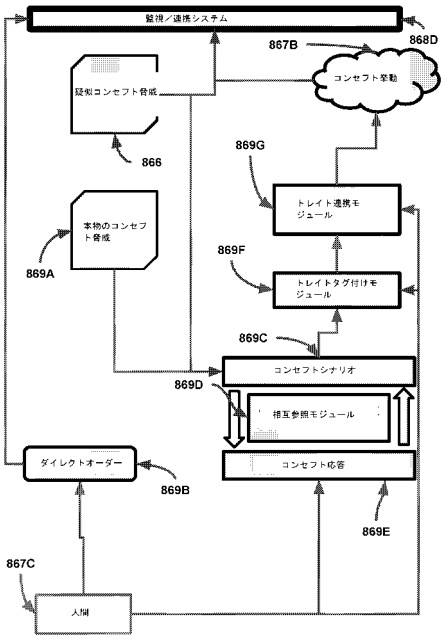
【図１４８】



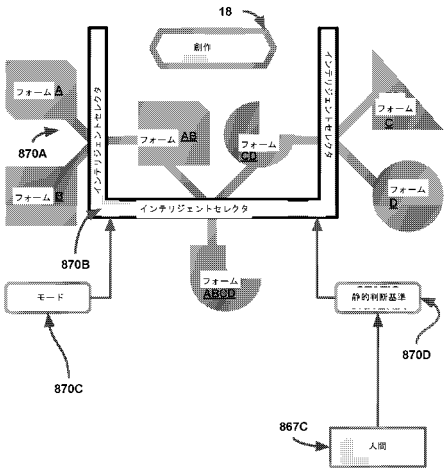
【図１４９】



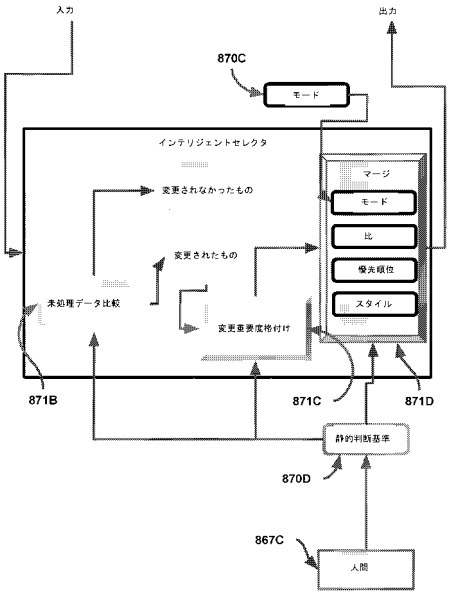
【図１５０】



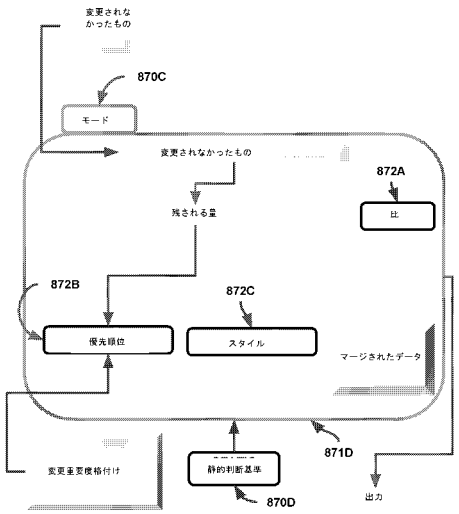
【図１５１】



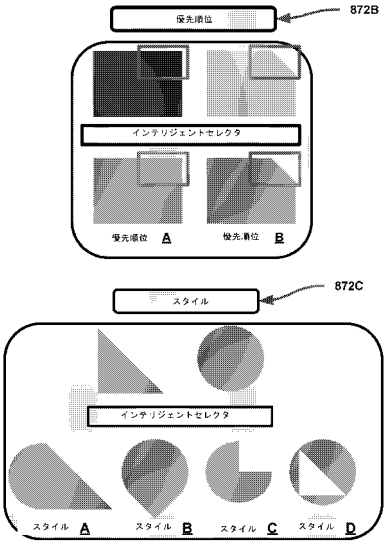
【図１５２】



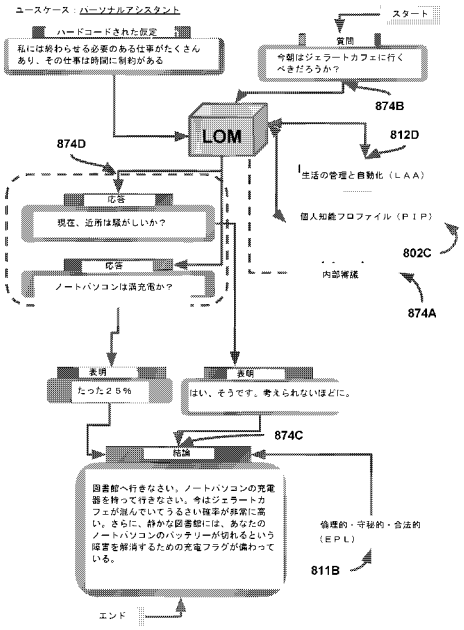
【図１５３】



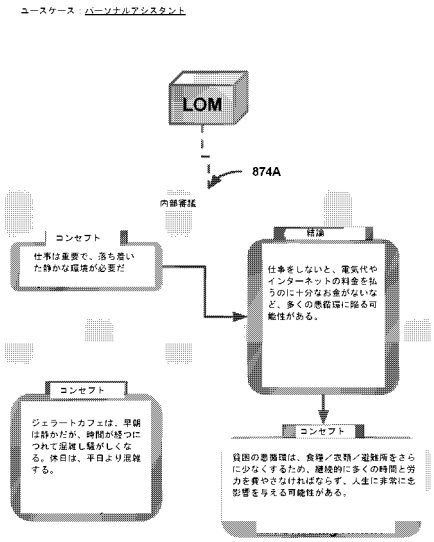
【図１５４】



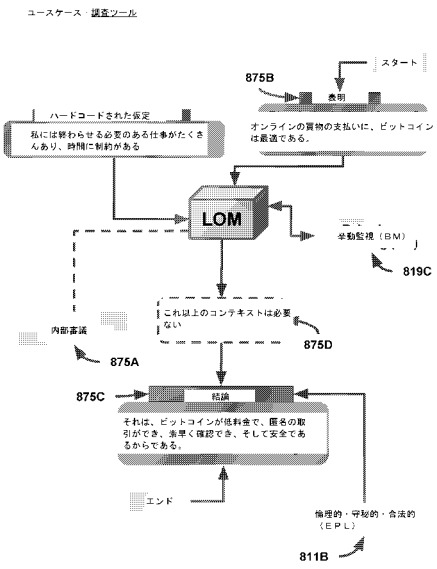
【図１５５】



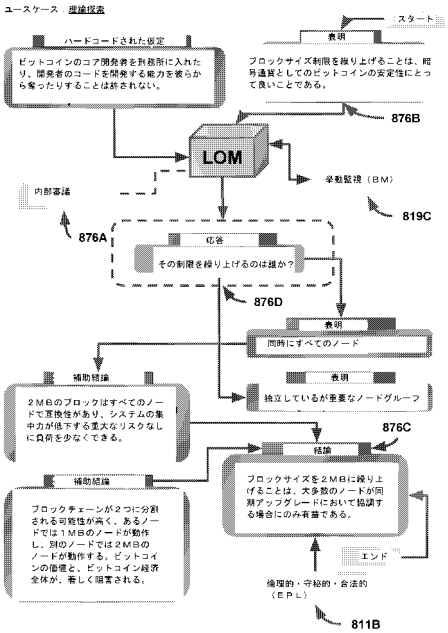
【図１５６】



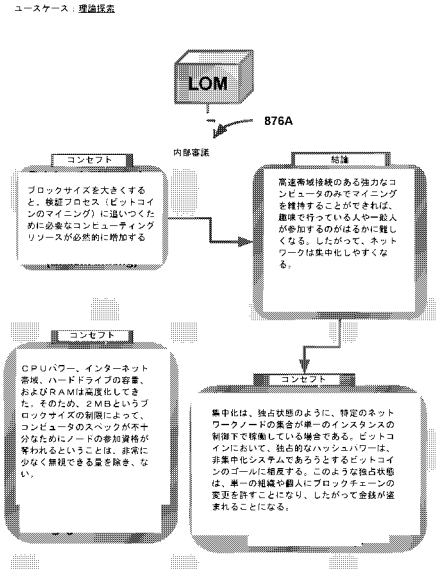
【図１５７】



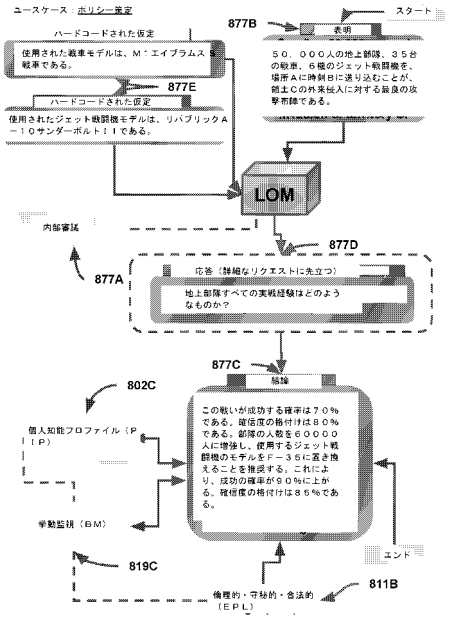
【図１５８】



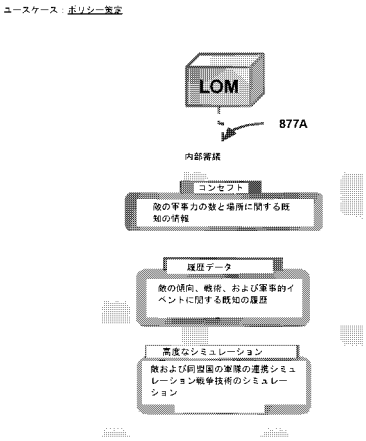
【図１５９】



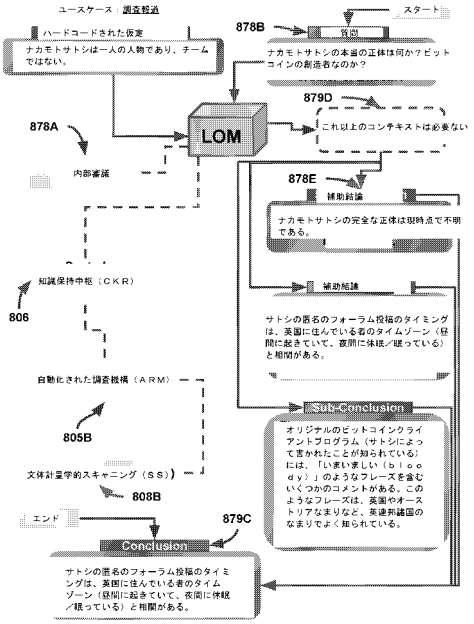
【図１６０】



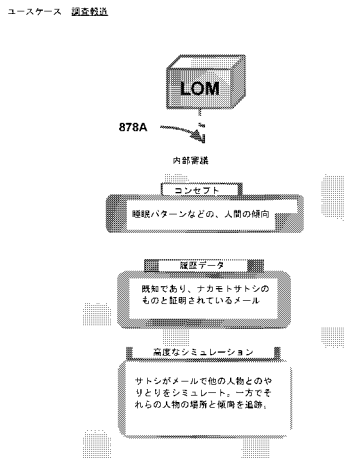
【図１６１】



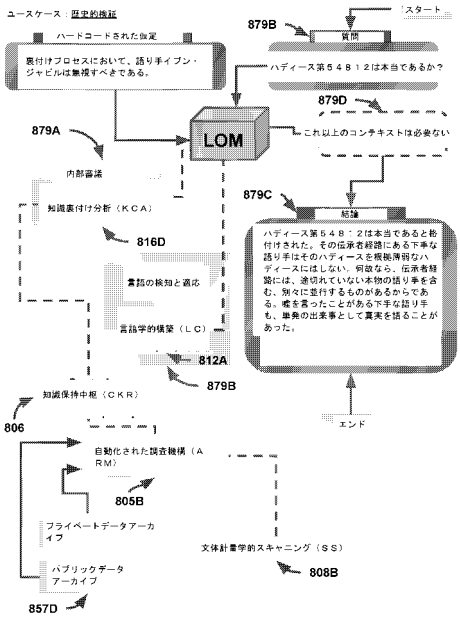
【図１６２】



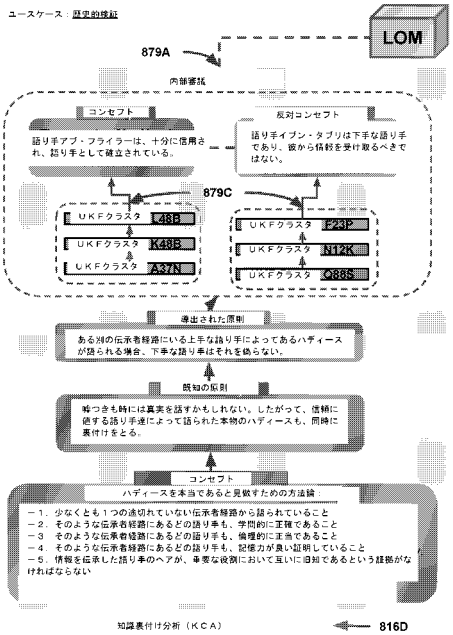
【図１６３】



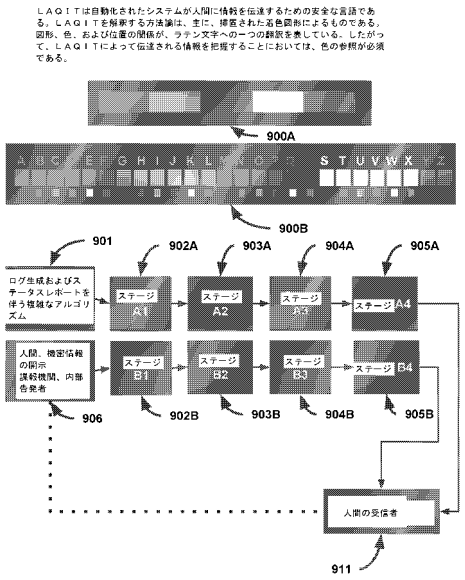
【図１６４】



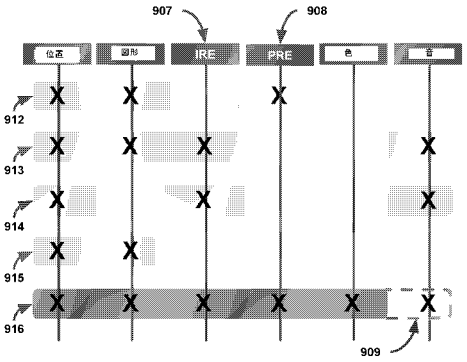
【図１６５】



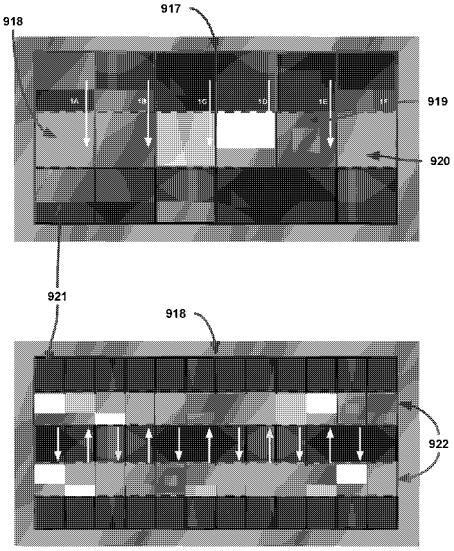
【図１６６】



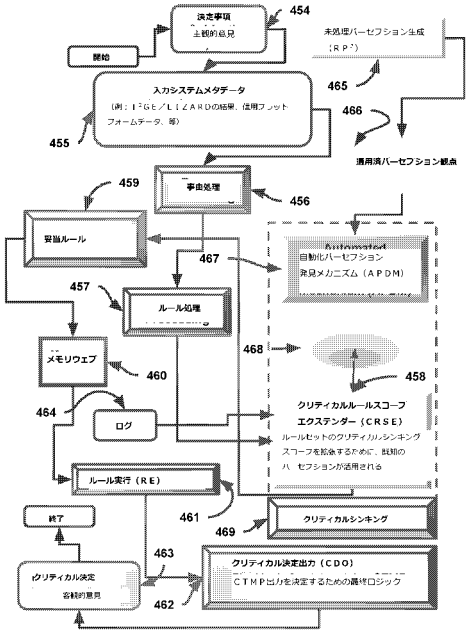
【図１６７】



【図１６８】



【図１６９】



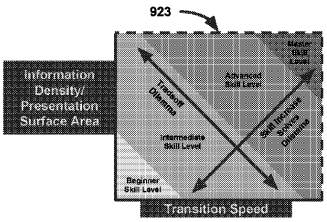
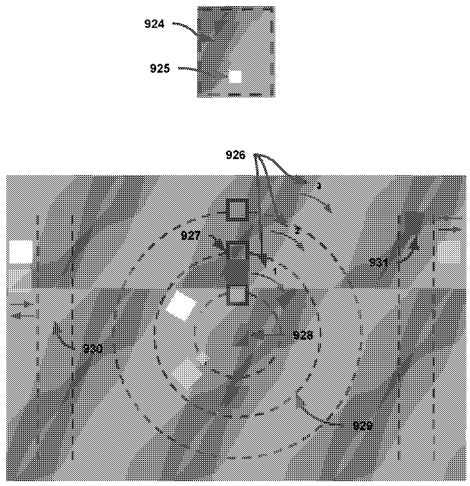
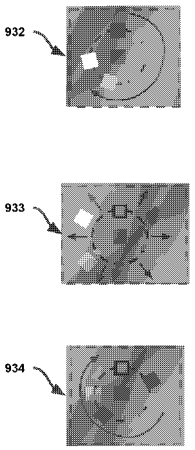


FIG. 169

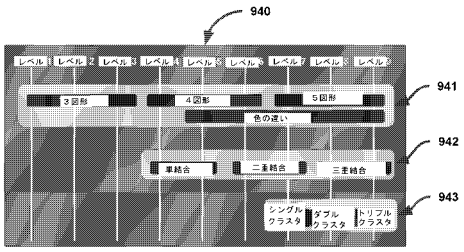
【図１７０】



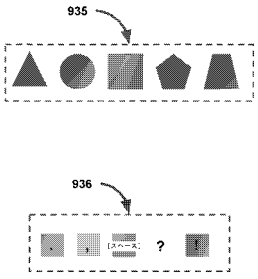
【図１７１】



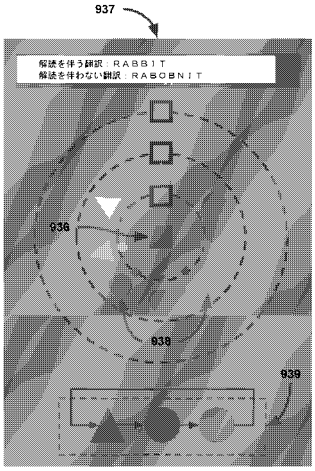
【図１７２】



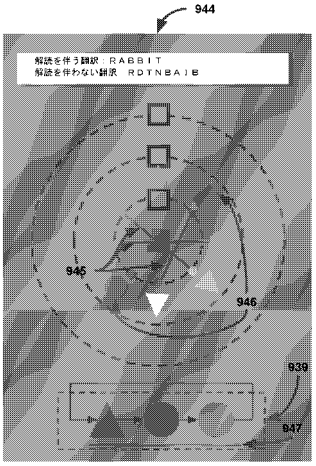
【図１７３】



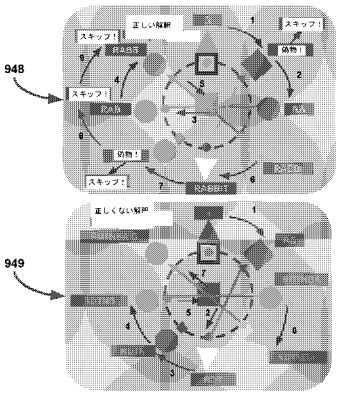
【図１７４】



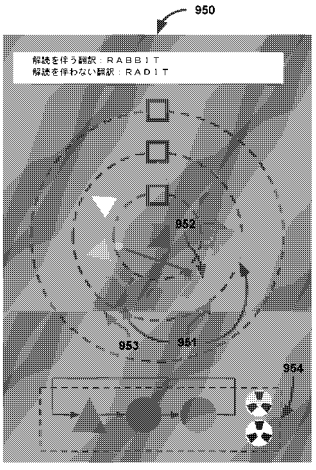
【図１７５】



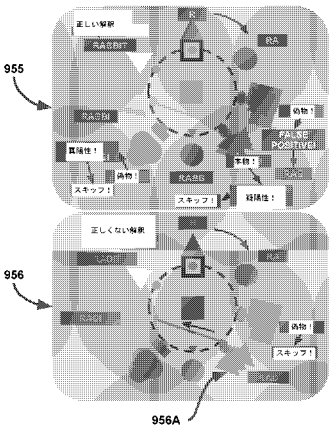
【図１７６】



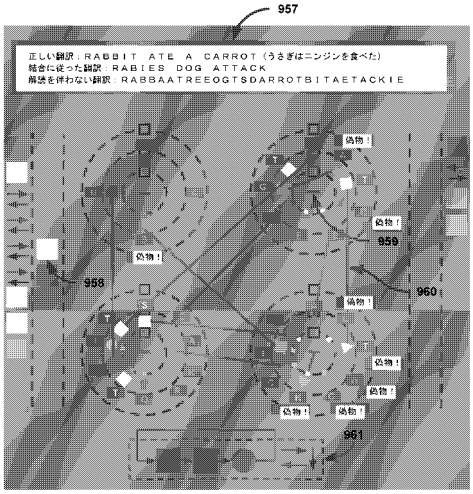
【図１７７】



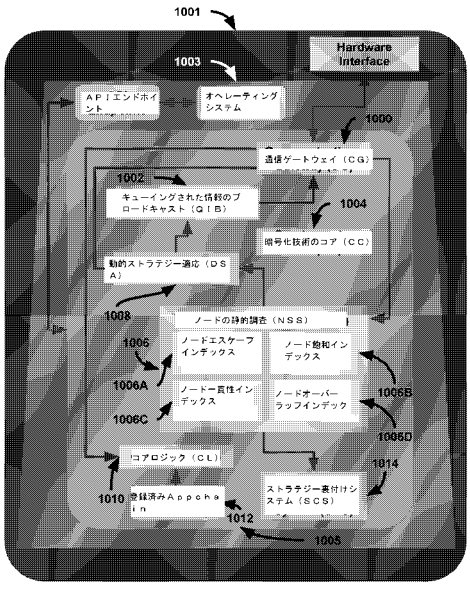
【図１７８】



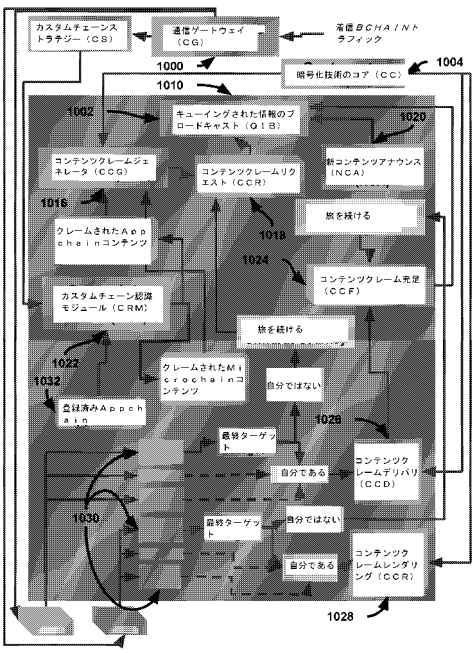
【図１７９】



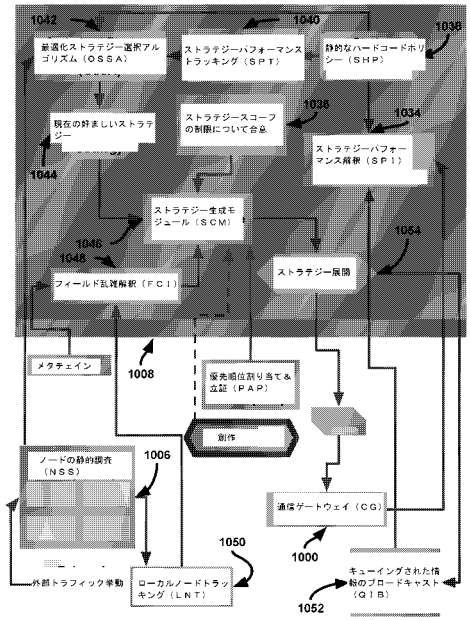
【図１８０】



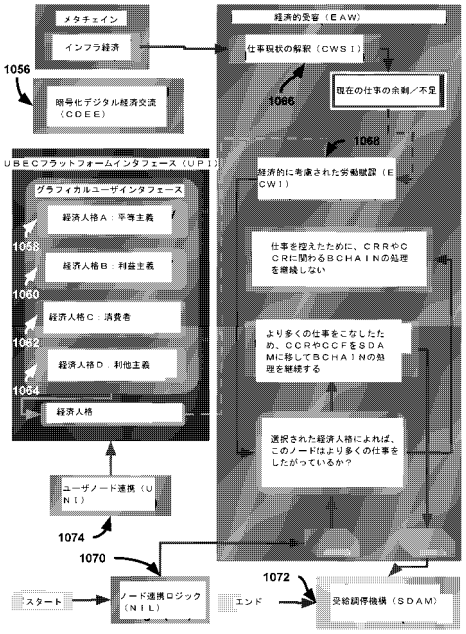
【図１８１】



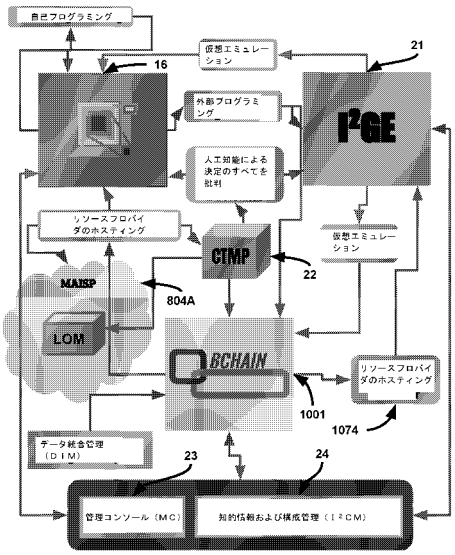
【図１８２】



【図１８３】



【図１８４】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/14699

A. CLASSIFICATION OF SUBJECT MATTER
IPC - G06N 5/02; G06F 17/30, 21/50, 21/51, 21/53, 21/54, 21/55, 21/56, 21/57 (2017.01)
CPC - G06N 5/022, 5/025; G06F 21/554, 21/566, 21/564, 21/602, 21/51, 21/53, 21/54, 21/55, 21/57; G06Q 10/067, 10/0631; H04L 63/1441, 63/145, 63/1416; G06F 17/30539, 17/30477, 17/30554

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
See Search History document

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2014/0278623 A1 (MARTINEZ, F. et al.) 18 September 2014; figures 4,5, 11; paragraphs [0062], [0064], [0088], [0090].	1-2
A	US 2015/0347753 A1 (JUNIPER NETWORKS, INC.) 03 December 2015; entire document.	1-76
A	US 2014/0218389 A1 (ALLGRESS, INC.) 07 August 2014; entire document.	1-76
A	US 8,321,941 B2 (TUVELL, G. et al.) 27 November 2012; entire document.	1-76
A	US 2012/0216243 A1 (GILL, J. et al.) 23 August 2012; entire document.	1-76
A	US 2013/0086260 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 04 April 2013; entire document.	1-76
A	US 8,713,631 B1 (KASPERSKY LAB ZAO) 29 April 2014; entire document.	1-76
A	US 8,353,033 B1 (CHEN, J. et al.) 08 January 2013; entire document.	1-76
A	WO 2015/145403 A1 (REAUX-SAVONTE, C.) 01 October 2015; entire document.	1-76
A	US 2015/0106307 A1 (SUPPORT MACHINES LTD.) 16 April 2015; entire document.	1-76
A	US 2015/0293917 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 15 October 2015; entire document.	

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 May 2017 (04 May 2017)	23 MAY 2017
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/14699

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 9,130,906 B1 (THE UNITED STATES OF AMERICA AS REPRESENTED BY THE SECRETARY OF THE NAVY) 08 September 2015; entire document.	1-76
A	US 2012/0123829 A1 (CHEN, Z. et al.) 17 May 2012; entire document.	1-76
A	US 2014/0119390 A1 (ADVA OPTICAL NETWORKING SE) 01 May 2014; entire document.	1-76

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/14699

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fee must be paid.

Group I: Claims 1-13 are directed towards a Critical Infrastructure Protection & Retribution system.
Group II: Claims 1 and 14-22 are directed towards a Machine Clandestine Intelligence & Retribution system.
Group III: Claims 1 and 23-33 are directed towards a Logically Inferred Zero database A-priori Realtime Defense system.
Group IV: Claims 1 and 34-53 are directed towards a Critical Thinking Memory & Perception system.
Group V: Claims 1 and 54-67 are directed towards a Lexical Objectivity Mining system.
Group VI: Claims 1 and 68-74 are directed towards a Linear Atomic Quantum Information Transfer system.
Group VII: Claims 1 and 75-76 are directed towards a Universal BCHAIN Everything Connections system.

<***-continued in last sheet-***>

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/14699

<***-continued from Box No. III Observations where unity of invention is lacking-***>

The inventions listed as Groups I-VII do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons:

The special technical features of Group I include at least a) Trusted Platform, which comprises network of agents that report hacker activity; b) Managed Network & Security Services Provider (MNSP), which provides Managed Encrypted Security, Connectivity & Compliance Solutions & Services; wherein virtual private network (VPN) connects the MNSP and the Trusted Platform, wherein VPN provides a communication channel to and from the Trusted Platform, wherein the MNSP is adapted to analyze all traffic in the enterprise network, wherein the traffic is routed to the MSNP, which are not present in Groups II-VII.

The special technical features of Group II include at least a) Intelligent Information and Configuration Management (I²CM), which provides intelligent information management, viewing and control; and b) Management Console (MC), which provides input/output channel to users: wherein the I²CM comprises: i) Aggregation, which uses generic level criteria to filter out unimportant and redundant information, and merges and tags streams of information from multiple platforms; ii) Configuration and Deployment Service, which comprises an interface for deploying new enterprise network devices with predetermined security configuration and connectivity setup and for managing deployment of new user accounts; iii) Separation by Jurisdiction, in which tagged pool of information are separated exclusively according to the relevant jurisdiction of a Management Console User; iv) Separation by Threat, which organizes the information according to individual threats; and v) Automated Controls, which accesses MNSP Cloud, Trusted Platform, or additional Third Party Services, which are not present in Groups I and III-VII.

The special technical features of Group III include at least a) Static Core (SC), which comprises predominantly fixed program modules; b) Iteration Module, which modifies, creates and destroys modules on Dynamic Shell, wherein the Iteration Module uses AST for a reference of security performance and uses Iteration Core to process the automatic code writing methodology; c) Differential Modifier Algorithm, which modifies the Base Iteration according to the flaws the AST found, wherein after the differential logic is applied, a new Iteration is proposed, upon which the Iteration Core is recursively called and undergoes the same process of being tested by AST; d) Logic Deduction Algorithm, which receives known security responses of the Dynamic Shell Iteration from the AST, wherein LOA deduces what codeset makeup will achieve the known Correct Response to a security scenario; e) Dynamic Shell (DS), which contains predominantly dynamic program modules that have been automatically programmed by the Iteration Module (IM); f) Code Quarantine, which Isolates foreign code into a restricted virtual environment; g) Covert Code Detection, which detects code covertly embedded in data and transmission packets; and h) Foreign Code Rewrite, which after deriving foreign code purpose, rewrites either parts or the whole code itself and allows only the rewrite to be executed; wherein all enterprise devices routed through LIZARD, wherein all software and firmware that runs enterprise devices are hardcoded to perform any sort of download/upload via LIZARD as a permanent proxy, wherein LIZARD interacts with three types of data comprising data in motion, data in use, and data at rest, wherein LIZARD interacts with data mediums comprising Files, Email, Web,. Mobile, Cloud and Removable Media, which are not present in Groups I-II and IV-VII.

The special technical features of Group IV include at least a) Critical Rule Scope Extender (CRSE), which takes known scope of perceptions and upgrade them to include critical thinking scopes of perceptions; b) Correct rules, which indicates correct rules that have been derived by using the critical thinking scope of perception; c) Rule Execution (RE)., which executes rules that have been confirmed as present and fulfilled as per the memory's scan of the Chaotic Held to produce desired and relevant critical thinking decisions; d) Critical Decision Output, which produces final logic for determining the overall output of CTMP by comparing the conclusions reached by both Perception Observer Emulator (POE) and the RE; wherein the POE produces an emulation of the observer and tests/compares all potential points of perception with such variations of observer emulations; wherein the RE comprises a checkerboard plane which is used to track the transformations of rulesets, wherein the objects on the board represents the complexity of any given security situation1 whilst the movement of such objects across the 'security checkerboard' indicates the evolution of the security situation which is managed by the responses of the security rulesets, which are not present in Groups I-III and V-VII.

The special technical features of Group V include at least a) Initial Query reasoning (IQR), to which a question is transferred, and which leverages Central Knowledge Retention (CKR) to decipher missing details that are crucial in understanding and answering/responding to the question; b) Survey Clarification (SC), to which the question and the supplemental query data is transferred, and which receives input from and send output to human subject, and forms Clarified Question/Assertion; c) Assertion Construction (AC), which receives a proposition in the form of an assertion or question and provides output of the concepts related to such proposition; d) Response Presentation, which is an interface for presenting a conclusion drawn by AC to both Human Subject and Rational Appeal (RA); e) Hierarchical Mapping (HM), which maps associated concepts to find corroboration or conflict in Question/Assertion consistency, and calculates the benefits and risks of having a certain stance on the topic; f) Central Knowledge Retention (CKR), which is the main database for referencing knowledge for LOM; g) Knowledge Validation (KV) which receives high confidence and pre-criticized knowledge which needs to be logically separated for query capability and assimilation into the CKR; h) Accept Response, which is a choice given to the Human Subject to either accept the response of LOM or to appeal it with a criticism, wherein if the response is accepted, then it is processed by KV so that it can be stored in CKR as confirmed (high confidence) knowledge, wherein should the Human Subject not accept the response, they are forwarded to the RA, which checks and criticizes the reasons of appeal given by Human; i) Managed Artificially Intelligent Services Provider (MAISP) which runs an Internet cloud instance of LOM with a master instance of the CKR, and connects LOM to Front End Services, Back End Services, Third Party Application Dependencies, Information Sources, and the MNSP Cloud, which are not present in Groups I-IV and VI-VII.

<***-continued in next extra sheet-***>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/14699

-***-Continued from previouis sheet -***-

The special technical features of Group VI include at least a) recursively repeating same consistent color sequence within a logically structured syntax; and b) using the sequence recursively to translate with the English alphabet; wherein when structuring the 'base' layer of the alphabet, the color sequence is used with a shortened and unequal weight on the color channel and leftover space for syntax definitions within the color channel is reserved for future use and expansion; wherein a complex algorithm reports its log events and status reports with LAQIT, status/log reports are automatically generated, wherein the status/log reports are converted to a transportable text-based LAQIT syntax, wherein syntactically insecure information is transferred over digitally, wherein the transportable text-based syntax is converted to highly readable LAQIT visual syntax (linear mode), wherein Key is optimized for human memorization and is based on relatively short sequence of shapes; wherein locally non secure text is entered by the sender for submission to the Recipient, wherein the text is converted to a transportable encrypted text-based LAQIT syntax, wherein syntactically secure information is transferred over digitally, wherein the data is converted to a visually encrypted LAQIT syntax; wherein Incremental Recognition Effect (IRE) is a channel of information transfer, and recognizes the full form of a unit of information before it has been fully delivered, wherein this effect of a predictive Index is incorporated by displaying the transitions between word to word, wherein Proximal Recognition Effect (PRE) is a channel of information transfer, and recognizes the full form of a unit of information whilst it is either corrupted, mixed up or changed, which are not present in Groups I-V and VII.

The special technical features of Group VII include at least a) Communications Gateway (CG), which is the primary algorithm for BCHAIN Node to interact with its Hardware Interface thereafter leading to communications with other BCHAIN nodes; b) Node Statistical Survey (NSS), which interprets remote node behavior patterns; c) Node Escape Index, which tracks the likelihood that a node neighbor will escape a perceiving node's vicinity; d) Node Saturation Index, which tracks the amount of nodes in a perceiving node's range of detection; e) Node Consistency Index, which tracks the quality of nodes services as interpreted by a perceiving node, wherein a high Node Consistency Index indicates that surrounding neighbor nodes tend to have more availability uptime and consistency in performance, wherein nodes that have dual purposes in usage tend to have a lower Consistency Index, wherein nodes that are dedicated to the BCHAIN network exhibit a higher value; and f) Node Overlap Index, which tracks the amount of overlap nodes have with one another as interpreted by a perceiving node, which are not present in Groups I-VI.

The common technical features shared by Groups I-VII are a system comprising: an enterprise network; a trusted platform; and a Managed Network & Security Services Provider.

However, these common features are previously disclosed by US 2014/0245439 A1 (DAY). Day discloses a system comprising: an enterprise network (an Enterprise Cloud; para [0040]); a trusted platform (a platform of a trusted multi-carrier network provider; para [0040]); and a Managed Network & Security Services Provider (an MSSP architecture; para [0040]).

Since the common technical features are previously disclosed by the Day reference, these common features are not special and so Groups I-VII lack unity.

フロントページの続き

(31)優先権主張番号 62/323,657
(32)優先日 平成28年4月16日(2016.4.16)
(33)優先権主張国 米国(US)
(31)優先権主張番号 15/145,800
(32)優先日 平成28年5月4日(2016.5.4)
(33)優先権主張国 米国(US)
(31)優先権主張番号 62/326,723
(32)優先日 平成28年4月23日(2016.4.23)
(33)優先権主張国 米国(US)
(31)優先権主張番号 62/341,310
(32)優先日 平成28年5月25日(2016.5.25)
(33)優先権主張国 米国(US)
(31)優先権主張番号 62/439,409
(32)優先日 平成28年12月27日(2016.12.27)
(33)優先権主張国 米国(US)
(31)優先権主張番号 15/264,744
(32)優先日 平成28年9月14日(2016.9.14)
(33)優先権主張国 米国(US)

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

（特許庁注：以下のものは登録商標）
１．ペンティアム