【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成30年11月15日(2018.11.15)

【公表番号】特表2017-534105(P2017-534105A)
【公表日】平成29年11月16日(2017.11.16)
【年通号数】公開・登録公報2017-044
【出願番号】特願2017-516098(P2017-516098)
【国際特許分類】
Ｇ０６Ｆ　13/00　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　13/00　　３５１Ｚ

【手続補正書】
【提出日】平成30年9月25日(2018.9.25)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】０１２９
【補正方法】変更
【補正の内容】
【０１２９】
上記の明細書において、本発明の実施形態を、実装毎に異なり得る多くの具体的な詳細に関して説明した。従って、明細書および図面は、本発明を限定するものではなく、説明するものと見なされるものである。本発明の範囲、および本発明の範囲であることが出願人によって意図されるものは、本願の特許請求の範囲が発行される特定の形態における、その後の修正（あれば）を含む、本願の特許請求の範囲の文言およびその等価の範囲のみによって示される。この点に関して、本願の特許請求の範囲には、特定の請求項の従属関係が述べられているが、本願の従属項の特徴は、本願の他の従属項の特徴、および独立項の特徴と適宜組み合わせられ得るものであり、特許請求の範囲に記載されている特定の従属関係のみに従うものではないことを留意されたい。
以下、本発明の好ましい実施形態を項分け記載する。
実施形態１
ポリシーを記述しているグローバルポリシーデータを格納するデータリポジトリと、
第１のコンピュータハードウェアによって少なくとも部分的に実装された複数のコンピュータアセットであって、該複数のコンピュータアセットのうちの各アセットが、クライアント装置からのメッセージを受信し、前記アセットを実装するコンピュータ装置において、前記ポリシーを記述しているローカルポリシーデータを格納し、前記ポリシーのうちのどのポリシーが前記メッセージのうちのどのメッセージに適用されるかを決定し、前記ポリシーのうちのどのポリシーが前記メッセージのうちのどのメッセージに適用されるかに基づいて、前記メッセージに関して行われるポリシーに基づくアクションを識別し、前記メッセージから記録されたメッセージ情報を解析部コンポーネントに送信し、前記グローバルポリシーデータに対する更新を反映するよう前記ローカルポリシーデータを更新するよう構成された、複数のコンピュータアセットと、
第２のコンピュータハードウェアによって少なくとも部分的に実装された解析部コンポーネントであって、前記複数のコンピュータアセットのうちの各コンピュータアセットから前記メッセージ情報を受信し、前記複数のコンピュータアセットのうちの各コンピュータアセットからの前記メッセージ情報を集合的に解析し、前記メッセージ情報の集合的な解析に基づいて、新たなポリシーを生成し、該新たなポリシーを記述するよう前記グローバルポリシーデータを更新するよう構成された解析部コンポーネントと
を含むことを特徴とするコンピュータシステム。

実施形態２
前記複数のコンピュータアセットのうちの各アセットが第１のネットワークのエッジに配置されており、前記クライアント装置が第２のネットワーク内に配置されている、実施形態１記載のコンピュータシステム。
実施形態３
前記複数のコンピュータアセットおよび前記解析部が、前記コンピュータシステムの第１の領域内に配置されており、前記コンピュータシステムが、別の複数のコンピュータアセットおよび別の解析部を各領域が含む１以上の更なる領域を更に含み、前記データリポジトリが前記第１の領域と前記１以上の更なる領域とによって共有されている、実施形態１記載のコンピュータシステム。
実施形態４
前記ポリシーのうちの各ポリシーが、該ポリシーが所与のメッセージに適用されるか否かを決定するための論理と、前記ポリシーが前記所与のメッセージに適用される場合に、該所与のメッセージに関して行われる、１以上の具体的なポリシーに基づくアクションを示す１以上の指示とを示すデータ構造である、実施形態１記載のコンピュータシステム。
実施形態５
前記解析部が、前記集合的に解析されたメッセージ情報からの、システムレベルのポリシーによって記述されている条件が存在するという決定に基づき、前記新たなポリシーのうちの１以上のポリシーを識別し、前記記載されている条件に照らしてブロックまたはリダイレクトされるメッセージを識別するための論理を含む１以上のアセットレベルのポリシーを生成し、該生成された１以上のアセットレベルのポリシーを含むよう前記グローバルポリシーデータを更新するよう更に構成された、実施形態１記載のコンピュータシステム。
実施形態６
前記解析部が、前記集合的に解析されたメッセージ情報に基づいて、前記コンピュータシステムに対する分散型の攻撃を識別し、該分散型の攻撃に関与するメッセージを識別するための論理を含む第１のポリシーを生成し、該第１のポリシーを記述するよう前記グローバルポリシーデータを更新するよう更に構成された、実施形態１記載のコンピュータシステム。
実施形態７
前記解析部が、前記集合的に解析されたメッセージ情報に基づいて、前記複数のコンピュータアセットのうちの第１のアセットにおいて生じている攻撃を識別し、該攻撃に関与するメッセージを識別するための論理を含む第１のポリシーを生成し、該第１のポリシーを記述するよう前記グローバルポリシーデータを更新するよう更に構成され、
前記複数のコンピュータアセットのうちの第２のアセットであって、該第２のアセットのローカルポリシーデータが更新されるときに前記攻撃に関与するメッセージをまだ受信していない第２のアセットが、前記更新されたグローバルポリシーデータに基づいて、前記第１のポリシーを記述するよう前記第２のアセットの前記ローカルポリシーデータを更新し、前記第１のポリシーに基づいて、前記攻撃に関与するメッセージをブロックまたはリダイレクトするよう構成された、
実施形態１記載のコンピュータシステム。
実施形態８
前記メッセージが、前記複数のアセットが行うよう指定されたアクションを示しており、各前記アセットが、前記ポリシーが適用されるメッセージに対して、前記示されている指定されたアクションの代わりにまたはそれに加えて、前記適用されるポリシーに基づくアクションを行うよう構成された、実施形態１記載のコンピュータシステム。
実施形態９
前記ポリシーのうちの所与のポリシーによって示されているポリシーに基づくアクションが、前記所与のポリシーが適用されるあらゆるメッセージをブロックすること、前記所与のポリシーが適用されるあらゆるメッセージをリダイレクトすること、または、前記所

与のポリシーが適用されるあらゆるメッセージにアセットが正常に応答することを許可することのうちの１つである、実施形態１記載のコンピュータシステム。
実施形態１０
前記複数のコンピュータアセットのうちの或るアセットが、たとえ該アセットが前記解析部コンポーネントおよび前記データリポジトリにアクセスできないときでも、前記アセットの前記ローカルポリシーデータからのポリシーをメッセージに適用するよう構成された、実施形態１記載のコンピュータシステム。
実施形態１１
１以上のコンピュータ装置によって実装されるコンピュータアセットにおいて、ポリシーを記述しているローカルポリシーデータを格納する工程と、
前記コンピュータアセットにおいて、クライアント装置からのメッセージを受信する工程と、
前記コンピュータアセットにおいて、前記ポリシーのうちのどのポリシーが前記メッセージのうちのどのメッセージに適用されるかを決定する工程と、
前記コンピュータアセットにおいて、前記ポリシーのうちのどのポリシーが前記メッセージのうちのどのメッセージに適用されるかに基づいて、前記メッセージに関して行われるポリシーに基づくアクションを識別する工程と、
前記コンピュータアセットから、前記メッセージから記録されたメッセージ情報を解析部コンポーネントに送信する工程と、
前記コンピュータアセットによって、前記解析部コンポーネントによって生成されたグローバルポリシーデータに対する更新を反映するよう前記ローカルポリシーデータを更新する工程と
を含むことを特徴とするデータ処理方法。
実施形態１２
前記ポリシーのうちの各ポリシーが、該ポリシーが所与のメッセージに適用されるか否かを決定するための論理と、前記ポリシーが適用される場合に、前記所与のメッセージに関して行われる、１以上の具体的なポリシーに基づくアクションを示す１以上の指示とを示すデータ構造である、実施形態１１記載の方法。
実施形態１３
前記メッセージが、前記複数のコンピュータアセットが行うよう指定されたアクションを示しており、
前記方法が、前記ポリシーが適用されるメッセージに対して示されている前記指定されたアクションの代わりにまたはそれに加えて、適用されるポリシーに基づくアクションを行う工程を更に含む、
実施形態１１記載の方法。
実施形態１４
たとえ前記アセットが前記解析部コンポーネントおよび前記グローバルポリシーデータにアクセスできないときでも、前記ローカルポリシーデータからのポリシーをメッセージに適用する工程を更に含む、実施形態１１記載の方法。
実施形態１５
前記解析部コンポーネントにおいて、前記コンピュータアセットを含む複数のコンピュータアセットのうちの各アセットにおいて記録されたメッセージ情報を受信する工程と、
前記解析部コンポーネントによって、前記複数のコンピュータアセットのうちの各コンピュータアセットにおいて記録された前記メッセージ情報を集合的に解析する工程と、
前記解析部コンポーネントによって、前記メッセージ情報の集合的な解析に基づいて、新たなポリシーを生成する工程と、
前記解析部コンポーネントによって、前記新たなポリシーを記述するよう前記グローバルポリシーデータを更新する工程と
を更に含む、実施形態１１記載の方法。
実施形態１６

解析部コンポーネントを実装する１以上のコンピュータ装置によって行われるデータ処理方法であって、
複数のコンピュータアセットのうちの各アセットから、該アセットによって受信されたメッセージを記述しているメッセージ情報を受信する工程と、
前記複数のコンピュータアセットのうちの各コンピュータアセットからの前記メッセージ情報を集合的に解析する工程と、
前記メッセージ情報の集合的な解析に基づいてポリシーを生成する工程であって、該ポリシーが、該ポリシーが適用されるメッセージを識別するための論理と、前記ポリシーが適用される前記メッセージに関して行われるポリシーに基づくアクションとを記述している、ポリシーを生成する工程と、
前記ポリシーを記述するようグローバルポリシーデータリポジトリを更新する工程と、
前記複数のコンピュータアセットに、少なくとも前記グローバルポリシーデータリポジトリ内の前記ポリシーを記述しているポリシーデータを送信する工程と、
を含むことを特徴とする方法。
実施形態１７
前記解析部コンポーネントが、それぞれ異なる複数のコンピュータアセットに関して実施形態１６記載の工程を行うよう各解析部が構成された複数の解析部のうちの１つであり、
前記グローバルポリシーデータリポジトリが、少なくとも前記複数の解析部によって共有されている、
実施形態１６記載の方法。
実施形態１８
前記メッセージ情報からの、システムレベルのポリシーによって記述されている条件が存在するという決定に基づき、前記ポリシーのうちの１以上のポリシーを識別する工程と、
前記記載されている条件に照らしてブロックまたはリダイレクトされるメッセージを識別するための論理を含む１以上のアセットレベルのポリシーを生成する工程と、
前記生成された１以上のアセットレベルのポリシーを含むよう前記グローバルポリシーデータを更新する工程と
を更に含む、実施形態１６記載の方法。
実施形態１９
前記メッセージ情報の集合的な解析に基づいて、前記複数のコンピュータアセットを含むコンピュータシステムに対する分散型の攻撃を識別する工程と、
前記分散型の攻撃に関与するメッセージを識別するための論理を含む第１のポリシーを生成する工程と、
前記第１のポリシーを記述するよう前記グローバルポリシーデータを更新する工程と
を更に含む、実施形態１６記載の方法。
実施形態２０
前記解析部コンポーネントが、前記メッセージ情報に基づいて、第１のコンピュータアセットにおいて生じている攻撃を識別する工程と、
前記複数のコンピュータアセットのうちの少なくとも第２のアセットであって、該第２のアセットが前記攻撃に関与するメッセージを受信したことを示す前記第２のアセットからのメッセージ情報を前記解析部コンポーネントがまだ受信していない前記第２のアセットにおいて、前記攻撃に関与するメッセージを識別するための論理を含む第１のポリシーを生成する工程と、
前記第１のポリシーを記述するよう前記グローバルポリシーデータを更新する工程と
を更に含む、実施形態１６記載の方法。