(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7140268号
(P7140268)

(45)発行日　令和4年9月21日(2022.9.21)

(24)登録日　令和4年9月12日(2022.9.12)

(51)国際特許分類
G06F 21/55 (2013.01)

FI
G06F 21/55 340

請求項の数 21 （全27頁）

(21)出願番号　特願2021-508423(P2021-508423)
(86)(22)出願日　平成31年3月25日(2019.3.25)
(86)国際出願番号　PCT/JP2019/012496
(87)国際公開番号　WO2020/194449
(87)国際公開日　令和2年10月1日(2020.10.1)
審査請求日　令和3年9月22日(2021.9.22)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100110928
弁理士　速水 進治
(72)発明者　西岡 淳
東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者　榮 純明
東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者　磯山 和彦
東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者　市原 悦子

最終頁に続く

(54)【発明の名称】　警告装置、制御方法、及びプログラム

(57)【特許請求の範囲】

【請求項１】

対象システムにおいて発生したイベントの集合であるイベント集合を第１の抽象レベルで表す第１の検出イベント情報を取得し、前記取得した第１の検出イベント情報によって表される前記イベント集合を第２の抽象レベルで表す第２の検出イベント情報を生成する第１生成部と、

それぞれが脅威活動を表す複数の脅威情報の中から、第１の前記検出イベント情報及び第２の前記検出イベント情報のうちの少なくとも一方との関連度が高い前記脅威情報を特定する特定部と、

前記特定された脅威情報と、その脅威情報との関連度が高い前記検出イベント情報に対応する抽象レベルである合致レベルとに基づいて、前記対象システムで発生している脅威に関する警告情報を生成する第２生成部と、を有する警告装置。

【請求項２】

前記イベントは、前記対象システム上で動作するプロセスの活動を表す、請求項１に記載の警告装置。

【請求項３】

前記第１の抽象レベルで表されたイベント集合では、イベントの主体であるプロセスの実行ファイル又はイベントの客体であるファイルについて、その識別情報が示され、

前記第２の抽象レベルで表されたイベント集合では、イベントの主体であるプロセスの実行ファイル又はイベントの客体であるファイルについて、その種類が示される、請求項

１又は２に記載の警告装置。
【請求項４】
前記脅威情報は、その脅威情報が表すイベント集合を第１の抽象度で表す第１の脅威イベント情報と、その脅威情報が表すイベント集合を第２の抽象度で表す第２の脅威イベント情報とを含み、
前記特定部は、
第１の前記検出イベント情報と各前記脅威情報の第１の脅威イベント情報との間で第１関連度を算出し、
第２の前記検出イベント情報と各前記脅威情報の第２の脅威イベント情報との間で第２関連度を算出し、
第１関連度又は第２関連度の少なくとも一方が閾値以上である前記脅威情報を特定する、請求項１乃至３いずれか一項に記載の警告装置。
【請求項５】
前記第１生成部は、前記第１関連度が閾値以上である前記脅威情報が存在しない場合に、前記第２の検出イベント情報の生成を行う、請求項４に記載の警告装置。
【請求項６】
前記特定部は、前記検出イベント情報に示されるイベント集合と前記脅威イベント情報に示されるイベント集合との間で合致するイベントの総数を、前記脅威イベント情報に示されるイベント集合に含まれるイベントの総数で割ることで、前記検出イベント情報と前記脅威イベント情報との間の関連度を算出する、請求項４又は５に記載の警告装置。
【請求項７】
前記特定部は、前記検出イベント情報に示されるイベント集合と前記脅威イベント情報に示されるイベント集合との間で合致する各イベントに付された重みの総和を、前記脅威イベント情報に示されるイベント集合に含まれる各イベントに付された重みの総和で割ることで、前記検出イベント情報と前記脅威イベント情報との間の関連度を算出する、請求項４又は５に記載の警告装置。
【請求項８】
前記脅威イベント情報は、各イベントについてそのイベントを数値で表したイベント値を示し、
前記特定部は、
前記検出イベント情報に示されている各イベントについて、そのイベントを数値で表したイベント値を算出し、
前記検出イベント情報に示されている各イベント値と、前記脅威イベント情報に示されている各イベント値とを比較することで、前記検出イベント情報に示されているイベントと前記脅威イベント情報に示されているイベントとが合致するか否かを判定する、請求項４乃至７いずれか一項に記載の警告装置。
【請求項９】
前記脅威イベント情報は、前記イベント集合に含まれるイベントで扱われるデータのサイズに関する条件を示し、
前記特定部は、前記検出イベント情報と前記脅威イベント情報との間の関連度を、前記検出イベント情報に示されるイベント集合と前記脅威イベント情報に示されるイベント集合との間でイベントが合致する度合い、及び前記検出イベント情報によって示されるイベントにおいて前記脅威イベント情報に示される前記条件が満たされるか否かの判定の結果に基づいて算出する、請求項４乃至８いずれか一項に記載の警告装置。
【請求項１０】
前記警告情報は、前記検出イベント情報と前記特定された脅威情報との間で合致するイベントが前記合致レベルに応じた度合いで強調されている情報を含む、請求項１乃至９いずれか一項に記載の警告装置。
【請求項１１】
コンピュータによって実行される制御方法であって、

対象システムにおいて発生したイベントの集合であるイベント集合を第１の抽象レベルで表す第１の検出イベント情報を取得し、前記取得した第１の検出イベント情報によって表される前記イベント集合を第２の抽象レベルで表す第２の検出イベント情報を生成する第１生成ステップと、
それぞれが脅威活動を表す複数の脅威情報の中から、第１の前記検出イベント情報及び第２の前記検出イベント情報のうちの少なくとも一方との関連度が高い前記脅威情報を特定する特定ステップと、
前記特定された脅威情報と、その脅威情報との関連度が高い前記検出イベント情報に対応する抽象レベルである合致レベルとに基づいて、前記対象システムで発生している脅威に関する警告情報を生成する第２生成ステップと、を有する制御方法。

【請求項１２】
前記イベントは、前記対象システム上で動作するプロセスの活動を表す、請求項１１に記載の制御方法。

【請求項１３】
前記第１の抽象レベルで表されたイベント集合では、イベントの主体であるプロセスの実行ファイル又はイベントの客体であるファイルについて、その識別情報が示され、
前記第２の抽象レベルで表されたイベント集合では、イベントの主体であるプロセスの実行ファイル又はイベントの客体であるファイルについて、その種類が示される、請求項１１又は１２に記載の制御方法。

【請求項１４】
前記脅威情報は、その脅威情報が表すイベント集合を第１の抽象度で表す第１の脅威イベント情報と、その脅威情報が表すイベント集合を第２の抽象度で表す第２の脅威イベント情報とを含み、
前記特定ステップにおいて、
第１の前記検出イベント情報と各前記脅威情報の第１の脅威イベント情報との間で第１関連度を算出し、
第２の前記検出イベント情報と各前記脅威情報の第２の脅威イベント情報との間で第２関連度を算出し、
第１関連度又は第２関連度の少なくとも一方が閾値以上である前記脅威情報を特定する、請求項１１乃至１３いずれか一項に記載の制御方法。

【請求項１５】
前記第１生成ステップにおいて、前記第１関連度が閾値以上である前記脅威情報が存在しない場合に、前記第２の検出イベント情報の生成を行う、請求項１４に記載の制御方法。

【請求項１６】
前記特定ステップにおいて、前記検出イベント情報に示されるイベント集合と前記脅威イベント情報に示されるイベント集合との間で合致するイベントの総数を、前記脅威イベント情報に示されるイベント集合に含まれるイベントの総数で割ることで、前記検出イベント情報と前記脅威イベント情報との間の関連度を算出する、請求項１４又は１５に記載の制御方法。

【請求項１７】
前記特定ステップにおいて、前記検出イベント情報に示されるイベント集合と前記脅威イベント情報に示されるイベント集合との間で合致する各イベントに付された重みの総和を、前記脅威イベント情報に示されるイベント集合に含まれる各イベントに付された重みの総和で割ることで、前記検出イベント情報と前記脅威イベント情報との間の関連度を算出する、請求項１４又は１５に記載の制御方法。

【請求項１８】
前記脅威イベント情報は、各イベントについてそのイベントを数値で表したイベント値を示し、
前記特定ステップにおいて、
前記検出イベント情報に示されている各イベントについて、そのイベントを数値で表

したイベント値を算出し、
　前記検出イベント情報に示されている各イベント値と、前記脅威イベント情報に示されている各イベント値とを比較することで、前記検出イベント情報に示されているイベントと前記脅威イベント情報に示されているイベントとが合致するか否かを判定する、請求項１４乃至１７いずれか一項に記載の制御方法。
【請求項１９】
　前記脅威イベント情報は、前記イベント集合に含まれるイベントで扱われるデータのサイズに関する条件を示し、
　前記特定ステップにおいて、前記検出イベント情報と前記脅威イベント情報との間の関連度を、前記検出イベント情報に示されるイベント集合と前記脅威イベント情報に示されるイベント集合との間でイベントが合致する度合い、及び前記検出イベント情報によって示されるイベントにおいて前記脅威イベント情報に示される前記条件が満たされるか否かの判定の結果に基づいて算出する、請求項１４乃至１８いずれか一項に記載の制御方法。
【請求項２０】
　前記警告情報は、前記検出イベント情報と前記特定された脅威情報との間で合致するイベントが前記合致レベルに応じた度合いで強調されている情報を含む、請求項１１乃至１９いずれか一項に記載の制御方法。
【請求項２１】
　請求項１１乃至２０いずれか一項に記載の制御方法の各ステップをコンピュータに実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
　本発明はコンピュータシステムにおける脅威の検出に関する。
【背景技術】
【０００２】
　コンピュータシステムでは、マルウエアなどといった脅威が発生しうる。そこで、このような脅威に関してコンピュータシステムを監視する技術が開発されている。
【０００３】
　例えば特許文献１の技術は、対象システムにおけるデータの送受信の態様を解析した結果に基づいて、脅威事例データベースから、対象システムに想定される脅威を抽出する。例えばこの発明は、「一般利用者が、インターネットを介し、ＩＤやパスワードを暗号化せずに平文でサーバへ送信する」という処理が行われていることについて、「利用者になりすまされる」という脅威が想定されるという情報を出力する。
【先行技術文献】
【特許文献】
【０００４】
【文献】特開２００８－１５２５５６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
　特許文献１では、データの送受信に関連して発生する脅威のみが対象となっている。そのため、データの送受信以外によって生じる脅威を検出することはできない。
【０００６】
　本発明は、上述の課題に鑑みてなされたものであり、その目的の一つは、様々な脅威の発生を検出できる技術を提供することである。
【課題を解決するための手段】
【０００７】
　本発明の警告装置は、１）対象システムにおいて発生したイベントの集合であるイベント集合を第１の抽象レベルで表す第１の検出イベント情報を取得し、取得した第１の検出

イベント情報によって表されるイベント集合を第２の抽象レベルで表す第２の検出イベント情報を生成する第１生成部と、２）それぞれが脅威活動を表す複数の脅威情報の中から、第１の検出イベント情報及び第２の検出イベント情報のうちの少なくとも一方との関連度が高い脅威情報を特定する特定部と、３）特定された脅威情報と、その脅威情報との関連度が高い検出イベント情報に対応する抽象レベルである合致レベルとに基づいて、対象システムで発生している脅威に関する警告情報を生成する第２生成部と、を有する。

【０００８】

本発明の制御方法は、コンピュータによって実行される。当該制御方法は、１）対象システムにおいて発生したイベントの集合であるイベント集合を第１の抽象レベルで表す第１の検出イベント情報を取得し、取得した第１の検出イベント情報によって表されるイベント集合を第２の抽象レベルで表す第２の検出イベント情報を生成する第１生成ステップと、２）それぞれが脅威活動を表す複数の脅威情報の中から、第１の検出イベント情報及び第２の検出イベント情報のうちの少なくとも一方との関連度が高い脅威情報を特定する特定ステップと、３）特定された脅威情報と、その脅威情報との関連度が高い検出イベント情報に対応する抽象レベルである合致レベルとに基づいて、対象システムで発生している脅威に関する警告情報を生成する第２生成ステップと、を有する。

【０００９】

本発明のプログラムは、本発明の制御方法が有する各ステップをコンピュータに実行させる。

【発明の効果】

【００１０】

本発明によれば、様々な脅威の発生を検出できる技術が提供される。

【図面の簡単な説明】

【００１１】

上述した目的、およびその他の目的、特徴および利点は、以下に述べる好適な実施の形態、およびそれに付随する以下の図面によってさらに明らかになる。

【図１】実施形態１の警告装置の動作の概要を表す図である。

【図２】実施形態１の警告装置の構成を例示する図である。

【図３】警告装置を実現するための計算機を例示する図である。

【図４】実施形態１の警告装置によって実行される処理の流れを例示するフローチャートである。

【図５】イベントを表す情報の構造をテーブル形式で例示する図である。

【図６】イベント集合を構成する方法を例示する図である。

【図７】イベント集合を構成する方法を例示する図である。

【図８】イベント集合を構成する方法を例示する図である。

【図９】３つ以上の抽象レベルを利用するケースを例示する図である。

【図１０】イベント集合に加え、読み書きされるデータのサイズに基づいて、脅威活動を定めるケースを例示する図である。

【図１１】警告情報を例示する図である。

【発明を実施するための形態】

【００１２】

以下、本発明の実施の形態について、図面を用いて説明する。尚、すべての図面において、同様な構成要素には同様の符号を付し、適宜説明を省略する。また、特に説明する場合を除き、各ブロック図において、各ブロックは、ハードウエア単位の構成ではなく、機能単位の構成を表している。

【００１３】

［実施形態１］

＜概要＞

図１は、実施形態１の警告装置の動作の概要を表す図である。図１は警告装置２０００の動作についての理解を容易にするための概念的な図であり、警告装置２０００の動作を

具体的に限定するものではない。

【００１４】

警告装置２０００は、監視対象のシステム（以下、対象システム）で発生したイベントの集合（互いに関連する１つ以上のイベントのまとまり）について、そのイベント集合が対象システムで生じている何らかの脅威を表しているか否かを特定する。イベントとしては、例えば、プロセスによるデータの読み書きや他のプロセスの起動などといった様々なものを扱うことができる。そして、イベント集合が表している脅威が特定されたら、警告装置２０００は、その脅威に関する警告情報４０を出力する。

【００１５】

ここで、対象システムにおける脅威とは、不正アクセスによるシステムへの不正操作や情報漏洩などを意味する。例えば、対象システムの中でマルウエアが活動しているといったことが、脅威の一例である。

【００１６】

上述した機能を実現するために、例えば警告装置２０００は以下のように動作する。警告装置２０００は、第１検出イベント情報１０を取得する。第１検出イベント情報１０は、対象システムで発生したイベント集合を（各イベントを）、第１の抽象レベル（抽象度合い）で表す。さらに警告装置２０００は、第１検出イベント情報１０を用いて第２検出イベント情報２０を生成する。第２検出イベント情報２０は、第１検出イベント情報１０によって表されるイベント集合を（各イベントを）、第２の抽象レベルで表す。

【００１７】

ここで、イベントの表し方の抽象レベルとは、イベントをどの程度抽象的に表すかの度合いを意味する。イベントは、より低い抽象レベルで表すほど、より具体的に表されることになる。例えば、イベントの主体のプロセスを実行ファイルの名称で表すケースと、実行ファイルの種類（ブラウザなどといったアプリケーションの種類）で表すケースとでは、前者の方がイベントをより具体的に表しているといえる。そのため、前者の表現の方が後者の表現よりも抽象レベルが低い。

【００１８】

ここで、第２の抽象レベルは、第１の抽象レベルよりも抽象度が高い。すなわち、第２検出イベント情報２０は、第１検出イベント情報１０によって表されているイベント集合を、より高い抽象度で表現した情報である。例えば第１検出イベント情報１０はイベントの主体や客体をその識別情報（例えば、ファイル名の本体及び拡張子）で表す一方で、第２検出イベント情報２０はイベントの主体や客体をそれらの種類を表す情報（例えば拡張子）で表す。以下、第１検出イベント情報１０と第２検出イベント情報２０を総称して検出イベント情報とも表記する。

【００１９】

さらに警告装置２０００は、様々な脅威それぞれについて予め定められている脅威情報３０を利用する。脅威情報３０では、その脅威情報３０で表す脅威（その脅威情報３０に対応する脅威）がイベント集合で表されている。

【００２０】

より具体的には、脅威情報３０は、第１脅威イベント情報３２及び第２脅威イベント情報３４を含む。第１脅威イベント情報３２では、脅威を表すイベント集合が第１の抽象レベルで表されている。一方、第２脅威イベント情報３４では、脅威を表すイベント集合が第２の抽象レベルで表されている。すなわち、１つの脅威情報３０に含まれる第１脅威イベント情報３２と第２脅威イベント情報３４は、同一の脅威を表すイベント集合を互いに異なる抽象度で表す。以下、第１脅威イベント情報３２と第２脅威イベント情報３４を総称して脅威イベント情報とも表記する。

【００２１】

警告装置２０００は、複数の脅威情報３０の中から、検出イベント情報との関連度が高い脅威イベント情報を示すものを特定する。具体的には、第１検出イベント情報１０との関連度が高い第１脅威イベント情報３２を示すか、又は第２検出イベント情報２０との関

連度が高い第２脅威イベント情報３４を示す脅威情報３０が特定される。
【００２２】
さらに警告装置２０００は、特定した脅威情報３０と、その脅威情報３０との関連度が高いものとして特定された検出イベント情報の抽象レベル（以下、合致レベル）とに基づいて、対象システムにおいて発生している脅威に関する警告情報４０を生成する。第１検出イベント情報１０と或る脅威情報３０の第１脅威イベント情報３２との関連度が高いと特定された場合には、合致レベルは第１の抽象レベルとなる。一方、第２検出イベント情報２０と或る脅威情報３０の第２脅威イベント情報３４との関連度が高いと特定された場合には、合致レベルは第２の抽象レベルとなる。そして警告装置２０００は、生成した警告情報４０を出力する。
【００２３】
＜作用効果＞
本実施形態の警告装置２０００によれば、検出イベント情報（対象システムで実際に発生したイベントの集合を示す情報）と脅威情報３０（脅威活動を表すイベント集合を示す情報）とを比較することにより、検出イベント情報と関連度の高い脅威情報３０が特定される。これにより、対象システムで発生している蓋然性が高い脅威を表す脅威情報３０を特定することができる。そして警告装置２０００は、特定した脅威情報３０に関する警告情報を生成・出力する。よって、警告装置２０００のユーザ（対象システムの管理者やユーザ）は、対象システムで発生している可能性がある脅威を容易に把握することができる。
【００２４】
ここで、イベントとしては、プロセスによるデータの読み書きや他のプロセスの起動などといった種々のイベントを扱うことができる。そのため、本実施形態の警告装置２０００によれば、データの送受信に限らず、対象システムにおける様々な活動に関して、脅威の発生を検出することができる。
【００２５】
さらに、本実施形態の警告装置２０００では、同一のイベント集合が、それぞれ抽象度の異なる複数の抽象レベルで表現される。具体的には、対象システムで実際に発生したイベントの集合について、そのイベント集合を第１の抽象レベルで表す第１検出イベント情報１０が得られる。さらに、第１検出イベント情報１０によって表されるイベント集合を第２の抽象レベルで表す第２検出イベント情報２０が生成される。また、脅威情報３０では、予め、脅威活動を表すイベント集合がそれぞれ異なる複数の抽象レベルで表現されている（第１脅威イベント情報３２及び第２脅威イベント情報３４）。
【００２６】
警告装置２０００は、第１検出イベント情報１０と第１脅威イベント情報３２との比較、及び第２検出イベント情報２０と第２脅威イベント情報３４との比較を行う。これにより、脅威活動を表すイベント集合と合致する脅威情報３０が特定できるだけでなく、これらがどの程度の抽象度で合致するのかについても特定できる。そして、警告装置２０００は、この「どの程度の抽象レベルで合致するのか」という点も考慮して、警告情報４０の生成を行う。よって、警告装置２０００のユーザは、対象システムで発生している可能性がある脅威を把握できることに加え、その脅威がどの程度の確からしさで発生しているのかについても把握することができる。
【００２７】
以下、本実施形態の警告装置２０００についてさらに詳細に説明する。
【００２８】
＜警告装置２０００の機能構成の例＞
図２は、実施形態１の警告装置２０００の構成を例示する図である。警告装置２０００は、第１生成部２０２０、特定部２０４０、第２生成部２０６０、及び出力部２０８０を有する。第１生成部２０２０は、第１検出イベント情報１０を取得し、第１検出イベント情報１０によって表されるイベント集合を第２の抽象レベルで表す第２検出イベント情報２０を生成する。特定部２０４０は、複数の脅威情報３０の中から、第１検出イベント情

報１０及び第２検出イベント情報２０のうちの少なくとも一方との関連度が高い脅威情報３０を特定する。第２生成部２０６０は、特定された脅威情報３０、及び脅威情報３０との関連度が高いイベント情報に対応する抽象レベルに基づいて、警告情報４０を生成する。出力部２０８０は、警告情報４０を出力する。

【００２９】

＜警告装置２０００のハードウエア構成＞

警告装置２０００の各機能構成部は、各機能構成部を実現するハードウエア（例：ハードワイヤードされた電子回路など）で実現されてもよいし、ハードウエアとソフトウエアとの組み合わせ（例：電子回路とそれを制御するプログラムの組み合わせなど）で実現されてもよい。以下、警告装置２０００の各機能構成部がハードウエアとソフトウエアとの組み合わせで実現される場合について、さらに説明する。

【００３０】

図３は、警告装置２０００を実現するための計算機１０００を例示する図である。計算機１０００は任意の計算機である。例えば計算機１０００は、Personal Computer（PC）やサーバマシンなどの据え置き型の計算機である。その他にも例えば、計算機１０００は、スマートフォンやタブレット端末などの可搬型の計算機である。計算機１０００は、警告装置２０００を実現するために設計された専用の計算機であってもよいし、汎用の計算機であってもよい。

【００３１】

計算機１０００は、バス１０２０、プロセッサ１０４０、メモリ１０６０、ストレージデバイス１０８０、入出力インタフェース１１００、及びネットワークインタフェース１１２０を有する。バス１０２０は、プロセッサ１０４０、メモリ１０６０、ストレージデバイス１０８０、入出力インタフェース１１００、及びネットワークインタフェース１１２０が、相互にデータを送受信するためのデータ伝送路である。ただし、プロセッサ１０４０などを互いに接続する方法は、バス接続に限定されない。

【００３２】

プロセッサ１０４０は、CPU（Central Processing Unit）、GPU（Graphics Processing Unit）、FPGA（Field－Programmable Gate Array）などの種々のプロセッサである。メモリ１０６０は、RAM（Random Access Memory）などを用いて実現される主記憶装置である。ストレージデバイス１０８０は、ハードディスク、SSD（Solid State Drive）、メモリカード、又は ROM（Read Only Memory）などを用いて実現される補助記憶装置である。

【００３３】

入出力インタフェース１１００は、計算機１０００と入出力デバイスとを接続するためのインタフェースである。例えば入出力インタフェース１１００には、キーボードなどの入力装置や、ディスプレイ装置などの出力装置が接続される。

【００３４】

ネットワークインタフェース１１２０は、計算機１０００を通信網に接続するためのインタフェースである。この通信網は、例えば LAN（Local Area Network）や WAN（Wide Area Network）である。ネットワークインタフェース１１２０が通信網に接続する方法は、無線接続であってもよいし、有線接続であってもよい。

【００３５】

ストレージデバイス１０８０は、警告装置２０００の各機能構成部を実現するプログラムモジュールを記憶している。プロセッサ１０４０は、これら各プログラムモジュールをメモリ１０６０に読み出して実行することで、各プログラムモジュールに対応する機能を実現する。

【００３６】

＜処理の流れ＞

図４は、実施形態１の警告装置２０００によって実行される処理の流れを例示するフローチャートである。第１生成部２０２０は、第１検出イベント情報１０を取得する（Ｓ１

０２）。第１生成部２０２０は、第１検出イベント情報１０を用いて第２検出イベント情報２０を生成する（Ｓ１０４）。特定部２０４０は、複数の脅威情報３０の中から、検出イベント情報との関連度が高い（第１検出イベント情報１０及び第２検出イベント情報２０のうちの少なくとも一方との関連度が高い）脅威情報３０を特定する（Ｓ１０６）。第２生成部２０６０は、特定された脅威情報３０及びその合致レベルに基づいて、警告情報４０を生成する（Ｓ１０８）。出力部２０８０は、生成された警告情報４０を出力する（Ｓ１１０）。

【００３７】

なお、警告装置２０００によって実行される処理の流れは、図４に示すものに限定されない。例えば警告装置２０００は、第２検出イベント情報２０を生成する前に、各脅威情報３０に含まれる第１脅威イベント情報３２を第１検出イベント情報１０と比較し、第１検出イベント情報１０との関連度が高い第１脅威イベント情報３２を含む脅威情報３０が存在しなかった場合に、第２検出イベント情報２０を生成してもよい。そして、警告装置２０００は、生成した第２検出イベント情報２０と各脅威情報３０に含まれる第２脅威イベント情報３４とを比較することで、第２検出イベント情報２０との関連度が高い第２脅威イベント情報３４を含む脅威情報３０を特定する。

【００３８】

この点については、後述するように第２の抽象レベル以上の抽象度の情報を扱う場合についても同様である。すなわち、警告装置２０００は、第 n の抽象レベルの検出イベント情報と第 n の抽象レベルの脅威イベント情報との間に関連度の高いものが見つからなかった場合に、第 (n+1) の抽象レベルの検出イベント情報を生成するようにする。

【００３９】

＜イベントについて＞

イベントは、対象システム上で発生する種々の事象である。例えばイベントは、対象システム上で（対象システムに含まれるいずれかの端末上で）動作するプロセスの活動を表す。例えばプロセスの活動は、システムコール単位で記録される。なお、対象システムを構成する端末は、物理マシンであってもよいし、仮想マシンであってもよい。

【００４０】

イベントは、例えば、イベントが発生した端末の識別情報、イベントの主体、イベントの客体、主体が客体について行った活動の内容、及び発生時刻という５つの要素を示す情報によって表される。そこで例えば、イベントを表す情報は、大別して、端末の識別情報、主体を表す主体情報、客体を表す客体情報、活動の内容を表す内容情報、及び発生時刻という５つの項目で構成される。

【００４１】

端末の識別情報は、端末を識別できる任意の情報である。例えば、端末のネットワークアドレス（IP アドレスや MAC アドレス）や UUID（Universally Unique Identifier）などを端末の識別情報として利用できる。

【００４２】

主体情報は、主体であるプロセスを識別できる任意の識別情報である。以下、プロセスを識別する情報をプロセス識別情報と呼ぶ。具体的には、プロセス識別情報は、プロセスＩＤ（Identifier）を含む。ただし、複数のスレッドが動作するプロセスについてのプロセス識別情報は、プロセスＩＤに加え、スレッドＩＤをさらに含む。

【００４３】

また、プロセス識別情報は、プロセスの実行ファイルに関する情報をさらに含む。プロセスの実行ファイルに関する情報とは、例えば、実行ファイルの名称やパス、実行ファイルのハッシュ値、実行ファイルのデジタル署名、又は実行ファイルで実現されるアプリケーションの名称などである。

【００４４】

客体情報は、例えば、その客体の種類及び識別情報である。客体の種類は、例えば、プロセス、ファイル、又はソケットなどである。客体がプロセスである場合、客体情報には

そのプロセスのプロセス識別情報が含まれる。
【００４５】
客体がファイルである場合、客体情報には、そのファイルを識別する情報（以下、ファイル識別情報）が含まれる。ファイル識別情報は、例えばファイルの名称やパスなどである。また、客体がファイルである場合、客体情報には、そのファイルのハッシュ値や、ファイルシステムの識別子とファイルシステム上でのファイルを構成するディスクブロックの識別子（inode 番号やオブジェクトID）の組み合わせなどが含まれていてもよい。
【００４６】
客体がソケットである場合、例えば客体情報には、ソケットに割り当てられた識別子が含まれる。
【００４７】
内容情報は、例えば、種々ある活動内容に割り当てられた識別情報である。例えば、「起動する」、「停止する」、「オープンする」、「データを読み込む」、及び「データを書き込む」などといった活動の内容に、互いに異なる識別子を割り当てておく。なお、ソケットに対するアクセスは、そのソケットに対応づけられた他の装置へのアクセスを意味する。
【００４８】
図５は、イベントを表す情報の構造をテーブル形式で例示する図である。以下、図５のテーブルをイベントテーブル２００と呼ぶ。イベントテーブル２００の各レコードは、１つのイベントを表す。イベントテーブル２００は、大別して、端末識別情報２０１、主体情報２０２、客体情報２０４、内容情報２０６、及び発生時刻２０７という５つの項目を含む。主体情報２０２は、プロセスＩＤ２０８、スレッドＩＤ２０９、及びパス２１０という３つの項目を含む。客体情報２０４は、種類２１２及び識別情報２１４という２つの項目を含む。発生時刻２０７は、イベントが発生した時刻を示す。
【００４９】
ここで、各イベントは、対象システム上におけるプロセスの活動を記録することで生成される。プロセスの活動を記録する技術には、既存の技術を利用することができる。
【００５０】
＜イベント集合について＞
イベント集合は、互いに関連する１つ以上のイベントのまとまりである。例えば、「或るイベントの客体が別のイベントにおいて主体となっている場合に、これらのイベントを連結する」という操作によって連結される複数のイベントを、同一のイベント集合に含めるようにする。
【００５１】
ここで、システム上で発生したイベントを連結してグラフで表現することがある。イベント集合は、このようにイベントを連結してグラフで表現する場合に１つのグラフを構成する複数のイベントで構成することができる。例えば図１では、１つのグラフを構成するイベント群をイベント集合として扱っている。
【００５２】
なお、或るイベントの客体が別のイベントにおいて主体となっていたとしても、これらのイベントが関連していないと考えられることもある。例えば、これらのイベントの発生時刻が大きく異なる場合には、これらのイベントは関連していない蓋然性が高い。そこで、イベント同士を連結する条件として、これらのイベントの発生時刻の差が所定値以下であるという条件をさらに設けてもよい。なお、このようにイベントの連結について設ける具体的な条件については、イベント同士を連結してグラフを生成する既存手法において利用されている種々の条件を利用することができる。
【００５３】
ここで、イベント集合を構成する方法（複数のイベントを同一のイベント集合に含める方法）は、連結されるイベントを同一のイベント集合に含めるという方法だけに限定されない。すなわち、イベントのつながりをグラフで表現した場合において互いに連結されな

い複数のグラフに含まれる各イベントが、同一のイベント集合に含まれるようにしてもよい。

【００５４】

例えば、「着目するプロセスから派生したプロセスやファイルに関係したイベントを、まとめて１つのイベント集合に含める」という方法を採用することができる。図６から図８は、イベント集合を構成する方法を例示する図である。図６では、スケジュールタスクの生成に関連する複数のイベント、及びそのスケジュールタスクの実行に関連する複数のイベントが、１つのイベント集合に含められている。すなわち、スケジュールタスクを生成するプロセス（ドット柄で表したプロセス）が「着目するプロセス」として扱われ、スケジュールタスクを実行するプロセス、及びそのスケジュールタスクの実行によって生成されるプロセスが、「着目するプロセスから派生したプロセス」として扱われている。図６のように表されるイベント集合によって実現される脅威としては、例えば、「マルウエアを生成した後、所定の時間後にそのマルウエアの実行を行う」という脅威が考えられる。

【００５５】

図７では、端末Ａから端末Ｂへファイルをアップロードするイベント、及びそのファイルに対するアクセスするイベントが、同一のイベント集合に含められている。すなわち、ファイルを他の端末にアップロードするプロセス（ドット柄で表したプロセス）が「着目するプロセス」として扱われ、そのプロセスによってアップロードされたファイル（斜線で表したファイル）が「着目するプロセスから派生したファイル」として扱われている。

【００５６】

図８では、外部記憶装置にファイルを格納するイベント、及びその外部記憶装置からそのファイルを読み出して利用するイベントが、同一のイベント集合に含められている。すなわち、外部記憶装置にファイルを格納するプロセス（ドット柄で表したプロセス）が「着目するプロセス」として扱われ、その外部記憶装置に格納されたファイル（斜線で表したファイル）が「着目するプロセスから派生したファイル」として扱われている。なお、外部記憶装置に格納されたファイルを読み出すプロセスと、読み出したファイルを利用するプロセスとは、異なっていてもよいし（図８上段の例）、同一であってもよい（図８下段の例）。

【００５７】

ここで、外部記憶装置は、USB メモリや SD カードなどといった可搬型の記憶装置であってもよいし、NAS（Network Attached Storage）などの据え置き型の記憶装置であってもよい（図８の例では USB メモリ）。

【００５８】

なお、「着目するプロセス」には、様々なものを採用できる。例えば、警告装置２０００の内部又は外部に設けられた異常検知システムによって何らかの異常が検知されたイベントの主体又は客体のプロセスを、着目するプロセスとして扱う。この異常検知システムには、既存のシステムを利用することができる。例えば、「通常では発生しないプロセスの活動をルールとして定めておき、そのようなルールに合致するイベントを異常なイベントとして検知する」という動作を行う異常検知システムを利用する。

【００５９】

＜第１検出イベント情報１０と第２検出イベント情報２０について＞

第１検出イベント情報１０は、第１の抽象度でイベント集合を表現した情報である。例えば第１検出イベント情報１０は、イベントの主体及び客体それぞれについて、それらを一意に特定可能な識別情報を示す。例えばプロセスの識別情報は、プロセスＩＤやそのプロセスを実現するプログラムの実行ファイルの名前やパスなどである。また、ファイルの識別情報は、例えば、ファイルの名前やパスである。

【００６０】

第２検出イベント情報２０は、第１検出イベント情報１０によって表されているイベント集合を、第１検出イベント情報１０よりも高い抽象度で表現する情報である。例えば、第２検出イベント情報２０は、イベントの主体や客体の識別情報の代わりに、それらの種

類を表す情報を示す。例えばプロセスの種類は、そのプロセスとして実行されているプログラムの種類（ブラウザ、文書作成ソフト、又は表計算ソフトなど）で表すことができる。ファイルの種類は、例えば、HTML ファイル、PDF ファイル、又は表計算ファイルなどがある。

【００６１】

また、第１検出イベント情報１０と第２検出イベント情報２０において、活動内容が異なる抽象度で表されていてもよい。例えば、活動内容がネットワークを介したデータの書き込み（送信）である場合において、第１検出イベント情報１０では特定の通信プロトコルを利用した書き込みであることを示す一方、第２検出イベント情報２０では通信プロトコルを示さずに単に書き込みであることのみを示すという方法を採用しうる。

【００６２】

なお、第２検出イベント情報２０は、イベントの主体、客体、及び活動内容の少なくとも１つが第１検出イベント情報１０よりも高い抽象度で表されていればよい。

【００６３】

＜第１検出イベント情報１０の取得：Ｓ１０２＞

第１生成部２０２０は、第１検出イベント情報１０を取得する（Ｓ１０２）。第１生成部２０２０が第１検出イベント情報１０を取得する方法は様々である。例えば第１生成部２０２０は、他の装置から送信される第１検出イベント情報１０を取得する。その他にも例えば、第１生成部２０２０は、記憶装置から第１検出イベント情報１０を読み出すことで、第１検出イベント情報１０を取得してもよい。

【００６４】

さらに第１生成部２０２０は、対象システムで発生した各イベントを示す情報（例えば図５に示すイベントテーブル２００）を取得してイベントをグルーピングすることにより、１つ以上の第１検出イベント情報１０を生成してもよい。なお、システムで発生したイベントを記録する方法、及びその記録された情報を取得する方法には、既存の方法を利用することができる。また、対象システムで発生したイベントをグルーピングしてイベント集合にまとめる（複数のイベントを１つのイベント集合にまとめる）方法については、前述した通りである。

【００６５】

第１生成部２０２０は、対象システムで発生した全てのイベントを対象として第１検出イベント情報１０の生成を行ってもよいし、特定のイベントに着目して第１検出イベント情報１０の生成を行ってもよい。例えば前述した異常検知システムを導入して異常なイベントの検知を行い、異常なイベントについてのみイベント集合を生成するようにしてもよい。すなわち、異常なイベントと関連を持たないイベントについては、第１検出イベント情報１０の生成が行われない。

【００６６】

その他にも例えば、着目するイベントは、予め定義されたイベントであってもよい。着目するイベントを定義した情報は、第１生成部２０２０からアクセス可能な記憶装置に記憶させておく。

【００６７】

＜第２検出イベント情報２０の生成：Ｓ１０４＞

第１生成部２０２０は、第１検出イベント情報１０から第２検出イベント情報２０を生成する（Ｓ１０４）。ここで、第１検出イベント情報１０から第２検出イベント情報２０を生成するルール（すなわち、イベント集合の表現を第１の抽象度から第２の抽象度に変換するルール）は、予め定めておく。

【００６８】

例えば、第１検出イベント情報１０においてはイベントの主体を識別情報で表し、第２検出イベント情報２０においてはイベントの主体をその種類を表す種類情報で表すとする。この場合、変換ルールには、主体の識別情報を種類情報に変換すること、及びその変換方法を定めておく。例えば、主体の識別情報をプロセスの実行ファイル名で表し、主体の

種類を拡張子で表すとする。この場合、実行ファイル名から拡張子部分を抽出するという変換方法により、主体の識別情報を主体の種類情報に変換できる。

【００６９】

＜＜第２の抽象レベルよりも高い抽象度のイベント情報の生成＞＞

第１生成部２０２０は、第２検出イベント情報２０に加え、第１検出イベント情報１０によって表されるイベント集合を第２の抽象レベルよりもさらに高い抽象度で表現した検出イベント情報を生成してもよい。例えば第１生成部２０２０は、第１検出イベント情報１０によって表されるイベント集合を、第２の抽象レベルよりも高い第３の抽象レベルで表現した第３検出イベント情報を生成する。同様に、第４の抽象レベルや第５の抽象レベルでの抽象化を行ってもよい。すなわち、第１生成部２０２０は、第１検出イベント情報１０を用い、第１検出イベント情報１０によって表されるイベント集合をそれぞれ異なる抽象レベルで表現した第２検出イベント情報から第 n 検出イベント情報（n は２以上の整数）を生成する。ここで、n の値が大きいほど抽象度が高くなるものとする。

【００７０】

図９は、３つ以上の抽象レベルを利用するケースを例示する図である。第１検出イベント情報１０では、プロセス、ファイル、及び通信先の端末がいずれも一意に可能な識別情報で表されている。これに対し、第２検出イベント情報２０では、客体がプロセス又はファイルである場合に、識別情報の代わりに種類情報が用いられている。さらに、第３検出イベント情報では、通信を表すイベントにおいて、客体として、通信先の識別情報の代わりに通信プロトコルを表す情報が示されている。そして、第４検出イベント情報では、主体を表す情報が省略される。すなわち、主体が特定されなくなる。

【００７１】

なお、図９に例示する第３の抽象レベルにおいて、通信プロトコルは、トランスポート層の通信プロトコルだけでなく、他の層のプロトコル（例えば、IP などのネットワーク層のプロトコルや、HTTP などのアプリケーション層等のプロトコルなど）であってもよい。

【００７２】

また、図９に示すように、抽象化の内容によっては、抽象化の前後でその内容が変化しないこともある。例えば「通信先を通信プロトコルで表す」という抽象化を行う場合、イベント集合の中に通信を表すイベントが含まれていなければ、抽象化の前後でイベント集合が変化しない。

【００７３】

＜脅威情報３０について＞

脅威情報３０は、コンピュータシステムにとって脅威となる活動である脅威活動を表すイベント集合を示す情報である。例えば脅威情報３０は、特定のマルウエアの活動や、特定のセキュリティホールを突いた侵入活動などを、それらの活動を構成するイベント集合で表現した情報である。例えば脅威情報３０は、実際に或るコンピュータシステムで発見された脅威活動や原理的に発生しうることが研究者等によって発見された脅威活動に関する情報をソースとして生成することができる。このように脅威情報３０のソースとなる情報（以下、ソース情報）としては、例えば、論文、セキュリティに関する研究活動のレポート、セキュリティ関連企業等のWeb ページ、又は SNS（Social Networking Service）に投稿された記事などといった様々な形態の情報を利用することができる。なお、ソース情報は、脅威情報３０を生成する人によって手動で収集されてもよいし、クローラなどを使ってネットワーク上から自動で収集されてもよい。

【００７４】

或る脅威活動を表す脅威情報３０は、その脅威活動を構成するイベント集合（以下、脅威イベント集合）をそれぞれ異なる抽象レベルで表現した複数の脅威イベント情報で構成される。脅威情報３０は、少なくとも、対応する脅威イベント集合を第１の抽象レベルで表現した第１脅威イベント情報３２、及びその脅威イベント集合を第２の抽象レベルで表現した第２脅威イベント情報を含む。さらに、検出イベント情報と同様に、第２の抽象レベルよりも高い抽象度の脅威イベント情報が含まれてもよい。具体的には、脅威イベント

集合を第３の抽象レベルで表した第３脅威イベント情報や、脅威イベント集合を第４の抽象レベルで表した第４脅威イベント情報などが含まれてもよい。すなわち、１つの脅威活動に対応する脅威情報３０は、その脅威活動を表すイベント集合がそれぞれ異なる抽象レベルで表現された第１脅威イベント情報から第 n 脅威イベント情報を含むことができる（n は２以上の任意の整数）。

【００７５】

脅威情報３０は、脅威イベント情報以外の情報を含んでもよい。例えば、脅威情報３０は、その脅威情報３０が表す脅威活動に関する説明を含む。脅威活動に関する説明は、例えば、攻撃の内容、攻撃の対象、及び攻撃が突くシステムの脆弱性などに関する情報を含む。さらに脅威情報３０は、IOC（Indicator of Compromise）を含んでもよい。IOC とは、マルウエア等の被害を受けたシステムから取得された、マルウエア等の活動の痕跡を表すデータである。例えば IOC には、マルウエア等のハッシュ値や、マルウエア等が行った通信の通信先の IP アドレスやドメイン名などが含まれる。

【００７６】

ここで、ソース情報を用いた脅威情報３０の生成は、人手で行われてもよいし、コンピュータ（例えば警告装置２０００）によって自動で行われてもよい。以下、後者の場合について、説明を容易にするために脅威情報３０が警告装置２０００によって生成されるものとして説明を行う。

【００７７】

例えば、警告装置２０００は、ソース情報を構成する文章から所定のルールに従ってイベントを抽出することで、イベント集合を生成する。そして、警告装置２０００は、抽出されたイベント集合について、第１脅威情報から第 n 脅威情報を生成する。例えば、警告装置２０００は、ソース情報に表されている抽象レベルでイベント集合を表した情報を、第１脅威イベント情報として生成する。そして、生成した第１脅威イベント情報から、他の抽象レベルの脅威イベント情報を生成する。

【００７８】

ここで、ソース情報を構成する文章から所定のルールに従ってイベントを抽出する技術には、自然言語処理の分野などで利用されている既存の技術を利用することができる。例えば、単語の集合や文章と、それらによって表されるイベントとを対応づけたイベント抽出ルールを定めておく。そして警告装置２０００は、この抽出ルールを用いてソース情報から１つ以上のイベントを抽出し、抽出されたイベントの集合を脅威イベント集合として定義する。

【００７９】

なお、第１脅威イベント情報を第２脅威イベント情報に変換するルールなど、より高い脅威イベント情報への変換を行うルールには、検出イベント情報をより高い抽象度の検出イベント情報に変換するルールと同様のルールを利用することができる。

【００８０】

さらに、警告装置２０００は、ソース情報から、脅威活動に関する説明や IOC などの抽出も行う。これらの抽出を実現するルールも、ソース情報からイベントを抽出するルールと同様に予め定めておく。

【００８１】

＜検出イベント情報と脅威情報３０の比較：Ｓ１０６＞

特定部２０４０は、検出イベント情報との関連度が高い脅威情報３０を特定する（Ｓ１０６）。そのために、特定部２０４０は、検出イベント情報によって表されているイベント集合と、脅威情報３０によって表されている脅威イベント集合との間の関連度を算出する。具体的には、特定部２０４０は、同一の抽象レベルの検出イベント情報と脅威イベント情報との間で関連度を算出する。

【００８２】

例えば、或る脅威情報３０を検出イベント情報と比較する場合、特定部２０４０は、第 n 検出イベント情報とその脅威情報３０に含まれる第 n 脅威イベント情報とを、各 n に

ついてそれぞれ比較する。すなわち、第１検出イベント情報１０については、その脅威情報３０に含まれる第１脅威イベント情報３２との関連度が算出され、第２検出イベント情報２０については、その脅威情報３０に含まれる第２脅威イベント情報３４との関連度が算出される。以下、脅威情報３０に含まれる第 n 脅威イベント情報と第 n 検出イベント情報との関連度を、第 n 関連度と表記する。

【００８３】

特定部２０４０は、脅威情報３０の中から、その脅威情報３０について算出された各第 n 関連度のいずれか一つ以上が高い（所定の閾値以上である）脅威情報３０を、検出イベント情報との関連度が高い脅威情報３０として特定する。

【００８４】

＜＜関連度の算出方法＞＞

以下、検出イベント情報と脅威イベント情報との間で関連度を算出する方法について説明する。例えば、検出イベント情報と脅威イベント情報との関連度は、以下のようにして算出することができる。

【００８５】

まず、検出イベント情報と脅威イベント情報において各イベントを表すデータを、イベントデータと呼ぶ。例えばイベントデータは、イベントの主体を表す文字列、イベントの客体を表す文字列、及び活動内容を表す文字列を連結したデータである。ここで、文字列 x と文字列 y を連結した文字列を x+y と表記する場合、主体が s1 であり、客体が o1 であり、活動内容が d1 であるイベント１のイベントデータ e1 は、e1=s1+o1+d1 で表される。

【００８６】

第１検出イベント情報１０と第２検出イベント情報２０とでは、これらによって表されるイベント集合は同じであっても、その表現の抽象度が異なる。そのため、これらの情報では、同一のイベントが互いに異なるイベントデータで表される。例えば、xyz.exe という実行ファイルのプロセスが主体であり、abc.txt というファイルが客体であり、活動内容が read であるイベント１があるとする。そして、第１検出イベント情報１０では客体を識別情報で表し、第２検出イベント情報２０では客体を種類情報で表すとする。この場合、第１検出イベント情報１０が示すイベントデータ e1 は 「"xyz.exe"+"abc.txt"+"read"」という文字列になる。一方、第２検出イベント情報２０が示すイベントデータ e2 は、「"xyz.exe"+"txt"+"read"」という文字列となる。

【００８７】

特定部２０４０は、検出イベント情報におけるイベントデータの集合と、脅威イベント情報におけるイベントデータの集合との重複度合い（合致度合い）に基づいて、検出イベント情報と脅威イベント情報との間の関連度を算出する。イベントの発生順序を考慮せずに関連度を算出する場合、例えば関連度は、以下の式（１）又は式（２）を用いて算出される。

【数１】

$$x = \frac{|S|}{|E|} \quad (1)$$

$$x = \frac{\sum_{i \in S} w_i}{\sum_{j \in E} w_j} \quad (2)$$

ここで、x は関連度を表す。E は、脅威イベント情報に示されているイベントデータの集合である。S は、脅威イベント情報と検出イベント情報とで互いに合致するイベントデータの集合である。｜｜ は、集合の要素数を表す。w はイベントデータに付されている重み

である。各イベントデータに付す重みは、脅威情報３０で予め定めておく。

【００８８】

式（１）では、脅威イベント情報と検出イベント情報との間で合致するイベントデータの数を、脅威イベント情報に示されているイベントの総数で割った値として、関連度が定められている。一方、式（２）では、脅威イベント情報と検出イベント情報との間で合致する各イベントデータに付された重みの総和を、脅威イベント情報に示されている各イベントデータに付された重みの総和で割った値として、関連度が定められている。ここで、イベントデータ同士の合致を判定する方法については後述する。

【００８９】

イベントの発生順序を考慮して関連度を算出する場合、例えば特定部２０４０は、脅威イベント情報と検出イベント情報との間で、順序が合致しているイベントデータの重複を１つ以上特定する。以下、説明を容易にするため、順序を考慮する必要があるイベント集合を、イベント順列とも呼ぶ。

【００９０】

例えば、検出イベント情報に {a,b,c,d} というイベント順列集合が示されており、脅威イベント情報に {b,d,c} というイベント順列が示されているとする。この場合、これらのイベント順列には、{b,d} 及び {b,c} という重複がある。いずれのイベント順列においても、d と c は b の後に発生しているためである。

【００９１】

特定部２０４０は、検出イベント情報と脅威イベント情報との間で重複するイベント順列（前述の例における {b,d} 及び {b,c}）に基づいて、これらの関連度を算出する。具体的には、以下の式（３）又は（４）を用いて関連度が算出される。

【数２】

$$x = \frac{\max_{P' \in P}(|P'|)}{|E|} \quad (3)$$

$$x = \frac{\max_{P' \in P} \sum_{i \in P'} w_i}{\sum_{j \in E} w_j} \quad (4)$$

ここで、P は検出イベント情報と脅威イベント情報との間で重複するイベント順列の集合（前述の例における {b,d} 及び {b,c} で構成される集合）である。その他の記号については、式（１）及び式（２）と同様である。

【００９２】

式（３）では、検出イベント情報と脅威イベント情報との間で重複する各イベント順列の要素数の最大値を、脅威イベント情報に示されているイベントの総数で割った値として、関連度が定められている。一方、式（４）では、検出イベント情報と脅威イベント情報との間で重複する各イベント順列についてその中に含まれるイベントデータの重みの総和が算出され、その総和の最大値を脅威イベント情報に示されている各イベントデータに付された重みの総和で割った値として、関連度が定められている。

【００９３】

イベントの発生順序を考慮するか否かは、脅威情報ごとに定められていてもよいし、脅威情報にかかわらず固定で定められていてもよい。例えば脅威情報に、イベントの発生順序を考慮するか否かを示すフラグを設けておく。また、イベントの発生順序を考慮するか否かは、脅威イベント情報ごとに定められていてもよい。

【００９４】

なお、脅威イベント情報において、全てのイベントの発生順序ではなく、一部のイベン

トの発生順序が定められていてもよい。すなわち、脅威イベント情報において、イベント集合の一部について順序が指定されている（イベント順列が示されている）ケースである。例えば、４つのイベント a, b, c, d が含まれる脅威イベント情報において、「a は必ず b の前に発生する」という発生順序のみを定めておくといったことが考えられる。

【００９５】

この場合、例えば特定部２０４０は、１）脅威イベント情報に示されているイベント集合と検出イベント情報に示されているイベント集合との間の関連度、及び２）脅威イベント情報に示されているイベント順列と検出イベント情報に示されているイベント順列との関連度という２つの関連度を算出する。前者はイベントの発生順序を考慮しないケースにおける関連度であり、後者はイベントの発生順序を考慮するケースにおける関連度である。そして特定部２０４０は、算出した２つの関連度の統計値（平均値、最大値、又は最小値など）を、脅威イベント情報と検出イベント情報との関連度として扱う。

【００９６】

＜＜イベントデータ同士の合致を判定する方法＞＞

イベントデータ同士が合致するかどうかの判定は、イベントデータをそのまま比較する（例えば文字列同士の合致判定を行う）ことで行われてもよいし、イベントデータを比較が容易な他のデータに変換した上で行われてもよい。後者の場合、例えば、特定部２０４０は、イベントデータを任意の規則で数値（イベント値）に変換する。例えばイベント値としては、ハッシュ値を用いることができる。

【００９７】

例えば特定部２０４０は、対比するイベント情報と脅威イベント情報それぞれに示されているイベントデータについてそのイベント値を算出し、イベント値の集合同士を比較することで、イベント情報と脅威イベント情報との間で一致しているイベントデータを特定する。ただし、脅威イベント情報に示されているイベントデータについては、予めイベント値に変換して脅威イベント情報に含めておくことが好適である。

【００９８】

＜＜付加情報をさらに利用した一致判定＞＞

脅威活動の種類によっては、イベントの集合だけではなく、その他の付加的な情報を用いることにより、対象システムにおいてその脅威活動が発生しているか否かをより正確に判定できるものがある。そこで、特定部２０４０は、イベント集合に加え、他の付加的な情報を利用して、検出イベント情報と脅威イベント情報とが合致するか否かを判定してもよい。

【００９９】

付加的な情報としては、例えば、読み書きされるデータのサイズを用いることができる。図１０は、イベント集合に加え、読み書きされるデータのサイズに基づいて、脅威活動を定めるケースを例示する図である。図１０の上段は、ファイルのダウンロードを表している。ファイルのダウンロードは、例えば、１）ネットワーク上の通信先から read する、２）read したデータを一時ファイルに write する、３）最後に一時ファイルの名前を本来の名称に変更するというイベント集合で表される。ここで、イベントだけを見ると、１）で read されたデータと、２）で write されるデータが同じものであるかが分からない。例えば、２）におけるファイルへの write が、１）におけるファイルの read とは無関係である可能性もある。

【０１００】

この例では、１）で read されるデータの内容と２）で write されるデータの内容が同じであれば、ファイルのダウンロードを表すイベント集合であると考えられる。ただし図１０では、このようにデータの内容を比較する代わりに、データのサイズを比較している。すなわち、上述した read のイベントと write のイベントがファイルのダウンロードを表すイベント集合を構成するか否かが、read されたデータのサイズと write されたデータのサイズとを比較することで判断される。

【０１０１】

具体的には、read されたデータのサイズが write されたデータのサイズより小さければ、read のイベントと write のイベントがファイルのダウンロードを表すイベント集合を構成しないと考えられる。一方で、read されたデータのサイズが write されたデータのサイズ以上であれば、read のイベントと write のイベントがファイルのダウンロードを表すイベント集合を構成すると考えられる。なお、データのアップロードについても同様のことがいえる。

【０１０２】

このように、データの内容の代わりにデータサイズを比較することには、比較処理に要する時間が短いというメリットや、比較のためにデータの内容を記録しておくという必要がないといったメリットがある。

【０１０３】

図１０の下段は、中間者によるデータ転送を表している。具体的には、プロセスＢが、プロセスＡとＣの間におけるデータの送受信を仲介している。この例では、「プロセスＡがプロセスＢに対して write したデータが、プロセスＢがプロセスＣに対して write したデータと同じである」という条件を満たせば、プロセスＡからプロセスＣへのデータ送信をプロセスＢが仲介したことになる。逆の流れについても同様である。

【０１０４】

ただし実際には、ダウンロードの例と同様に、プロセスＢがデータの送信を仲介しているかどうかを判定する条件として、「プロセスＡがプロセスＢに対して write したデータのサイズが、プロセスＢがプロセスＣに対して write したデータのサイズとほぼ同じである」というデータサイズに関する条件を用いることが好適である。

【０１０５】

以上のように、図１０で例示したような脅威活動についての脅威情報３０では、イベント集合に加え、データの読み書きにおけるデータサイズについての条件を定めておく。さらに、第１検出イベント情報１０においても、読み書きされたデータのサイズが示されているようにする。そして、特定部２０４０は、前述した方法でイベント集合同士の合致度合いを算出することに加え、上述したデータサイズに関する条件が満たされているか否かを判定する。

【０１０６】

ここで、データサイズの条件に関する判定の結果を利用する方法は様々である。例えば特定部２０４０は、脅威情報３０と検出イベント情報とについて、前述したデータサイズに関する条件が満たされていなければ、イベント集合同士の合致度合いにかかわらず、その脅威情報３０を、検出イベント情報と関連度が高いものとして特定しないようにする。

【０１０７】

その他にも例えば、特定部２０４０は、データサイズに関する条件が満たされているか否かに応じて、イベント集合同士の合致度合いに基づいて算出された関連度の値を補正する。例えば、上述したデータサイズに関する条件が満たされていない場合、特定部２０４０は、イベント集合同士の合致度合いに基づいて算出された関連度に対し、０より大きく１より小さい所定の補正係数を掛けることで、その関連度をより小さい値に補正する。

【０１０８】

＜警告情報の生成：Ｓ１０８＞

第２生成部２０６０は、特定部２０４０によって特定された脅威情報３０及びその合致レベルに基づいて、警告情報４０を生成する（Ｓ１０８）。例えば、或る脅威情報３０に含まれる第１脅威イベント情報３２が第１検出イベント情報１０と高い関連度を持つと特定された場合、警告情報４０は、その脅威情報３０及び「第１の抽象レベル」という合致レベルに基づいて生成される。ここで、合致レベルの具体的な利用方法については後述する。

【０１０９】

例えば第２生成部２０６０は、脅威情報３０によって表される脅威に関する説明やその脅威に対する対応策を、警告情報４０に含める。脅威に関する説明や対応策は、予め脅威

情報３０に含めておく。

【０１１０】

ここで、脅威に関する説明のうち、検出イベント情報と脅威情報３０との間で合致したイベントについての記述を強調することが好ましい。強調の方法としては、例えば、他の記述とは異なる文字色にしたり、下線や枠線などを付したりする方法がある。

【０１１１】

その他にも例えば、第２生成部２０６０は、検出イベント情報と脅威情報３０との間で合致したイベントを表す情報を警告情報４０に含めてもよい。具体的には、検出イベント情報によって表されるイベント集合のグラフ表現を警告情報４０に含め、そのグラフにおいて、脅威情報３０と合致したイベントを強調表示するようにする。

【０１１２】

図１１は、警告情報４０を例示する図である。図１１の警告情報４０には、脅威情報３０の名称（概要）、合致レベル、第１検出イベント情報１０によって表されるイベントのグラフ表現、脅威に関する説明、及び対策手法の説明が含まれている。また、イベントのグラフにおいて、脅威情報３０と合致したイベントが、ドット柄で塗られた枠で囲まれている。

【０１１３】

合致レベルは、脅威に関する説明やイベントのグラフを強調する際において、その強調の態様を決定するために利用できる。すなわち、第２生成部２０６０は、合致レベルに応じて、強調の方法を異ならせる。例えば、合致レベルが低いほど、脅威に関する説明やイベントのグラフにおける強調が、より強く行われるようにする。強調の強さは、例えば、色をより目立つに色にしたり、下線や枠線などの太さをより太くしたりすることなどによって、強くすることができる。

【０１１４】

ここで、特定部２０４０によって特定される脅威情報３０は、１つではなく、複数である可能性もある。この場合、第２生成部２０６０は、特定された全ての脅威情報３０について警告情報４０を生成してもよいし、一部の脅威情報３０について警告情報４０を生成してもよい。

【０１１５】

後者の場合、まず第２生成部２０６０は、各脅威情報３０についての合致レベルを考慮する。すなわち、第２生成部２０６０は、検出イベント情報との関連度が高いと特定された脅威情報３０のうち、その合致レベルが低いものを優先して、警告情報４０を生成する。例えば第２生成部２０６０は、特定された脅威情報３０を合致レベルの昇順でソートした場合に所定の順位以内に入るものについてのみ、警告情報４０を生成する。

【０１１６】

また、第２生成部２０６０は、合致レベルに加え、関連度の高さを考慮してもよい。すなわち、第２生成部２０６０は、特定された脅威情報３０を合致レベルの昇順でソートし、さらに同一の合致レベルの脅威情報３０について関連度の降順でソートした場合において、所定の順位以内に入る脅威情報３０についてのみ、警告情報４０を生成する。なお、「所定の順位」については、特定部２０４０からアクセス可能な記憶装置に予め記憶させておく。

【０１１７】

＜警告情報４０の出力：Ｓ１１０＞

出力部２０８０は警告情報４０を出力する（Ｓ１１０）。ここで、警告情報４０の出力態様は任意である。例えば出力部２０８０は、警告装置２０００に接続されているディスプレイ装置に警告情報４０を表示させる。その他にも例えば、出力部２０８０は、任意の記憶装置に警告情報４０を格納してもよい。その他にも例えば、出力部２０８０は、警告装置２０００以外の装置に警告情報４０を送信してもよい。例えば警告情報４０は、対象システムの管理者等の端末に送信される。対象システムの管理者等は、その端末を操作することで、その端末に接続されているディスプレイ装置で、警告情報４０を閲覧する。

【０１１８】
＜ユーザからのフィードバック＞
警告装置２０００は、出力した警告情報４０について、ユーザからフィードバックを受け付けてもよい。具体的には、警告情報４０に、検出イベント情報と脅威情報３０との間で合致したイベントを表す情報（図１１におけるイベントのグラフなど）が含まれているとする。この場合において、ユーザが、検出されたイベントは脅威を表すものではないと判断したとする。この場合、ユーザは、検出されたイベントが脅威を表していない（すなわち、警告に誤りがある）ことを示す入力を、警告装置２０００に対して行う。警告装置２０００は、この入力に基づいて、検出されたイベントの重要度を下げる（例えば、そのイベントの重要度を、現在の値に１より小さい所定の係数を掛けた値に更新する）処理を行う。このようにすることで、ユーザの知識を活かして警告装置２０００がより正確な警告情報４０を生成できるようになる。
【０１１９】
同様に、警告装置２０００は、警告が正しいことを示す入力を、ユーザから受け付けてもよい。この場合、警告装置２０００は、警告情報４０に含めた検出イベント情報に含まれるイベントの重要度を上げる（例えば、そのイベントの重要度を、現在の値に１より大きい所定の係数を掛けた値に更新する）処理を行う。
【０１２０】
＜変形例＞
警告装置２０００は、対象システムの正常な活動を表す情報をさらに利用してもよい。この情報を正常情報と呼ぶ。正常情報は、対象システムの正常な活動をイベント集合で表す。より具体的には、正常情報は、同一のイベント集合をそれぞれ異なる抽象レベルで表す複数の正常イベント情報を有する。以下、正常情報に対応するイベント集合を第 n の抽象レベルで表現する正常イベント集合を、第 n 正常イベント集合と表記する。
【０１２１】
特定部２０４０は、検出イベント情報と脅威イベント情報との関連度を算出することに加え、検出イベント情報と正常イベント情報との関連度を算出する。具体的には、各正常情報について、その正常情報に含まれる第 n 正常イベント情報と、第 n 検出イベント情報との関連度を算出する。なお、検出イベント情報と正常イベント情報とについて関連度を算出する方法には、検出イベント情報と脅威イベント情報とについて関連度を算出する方法と同じ方法を利用できる。
【０１２２】
警告装置２０００は、検出イベント情報と正常情報との関連度に基づいて、警告情報４０の生成や出力を制御する。例えば第２生成部２０６０は、検出イベント情報との関連度が高い正常情報についての情報を警告情報に含める。ただし、警告情報に正常情報についての情報を含めるのは、検出イベント情報が脅威活動を表している蓋然性よりも、検出イベント情報が正常な活動を表している蓋然性の方が高いと考えられる場合のみであってもよい。その他にもたとえば、第２生成部２０６０は、検出イベント情報が脅威活動を表している蓋然性よりも、検出イベント情報が正常な活動を表している蓋然性の方が高いと考えられる場合には、警告情報４０を生成しないようにしてもよい。
【０１２３】
ここで、検出イベント情報が脅威活動を表している蓋然性よりも、検出イベント情報が正常な活動を表している蓋然性の方が高いか否かを判定する方法は様々である。例えば第２生成部２０６０は、検出イベント情報との関連度が所定値以上であると特定された正常イベント情報のうち、抽象レベルが最小であるものを特定する。同様に、第２生成部２０６０は、検出イベント情報との関連度が所定値以上であると特定された脅威イベント情報のうち、抽象レベルが最小であるものを特定する。こうすることで、最も低い抽象度で（最も具体的な表現で）検出イベント情報と合致する正常イベント情報、及び最も低い抽象度で（最も具体的な表現で）検出イベント情報と合致する脅威イベント情報が特定される。
【０１２４】

まず第２生成部２０６０は、特定された正常イベント情報と脅威イベント情報の抽象レベルを比較する。特定された正常イベント情報の抽象レベルが、特定された脅威イベント情報の抽象レベルよりも低ければ、第２生成部２０６０は、検出イベント情報が正常な活動を表している蓋然性の方が高いと判定する。一方、特定された正常イベント情報の抽象レベルが、特定された脅威イベント情報の抽象レベルよりも高ければ、第２生成部２０６０は、検出イベント情報が脅威活動を表している蓋然性の方が高いと判定する。

【０１２５】

特定された正常イベント情報の抽象レベルと、特定された脅威イベント情報の抽象レベルとが等しい場合、第２生成部２０６０は、これらについて算出された関連度を比較する。正常イベント情報について算出された関連度が脅威イベント情報について算出された関連度より大きい場合、第２生成部２０６０は、検出イベント情報が正常な活動を表している蓋然性の方が高いと判定する。一方、正常イベント情報について算出された関連度が脅威イベント情報について算出された関連度以下であれば、第２生成部２０６０は、検出イベント情報が脅威活動を表している蓋然性の方が高いと判定する。

【０１２６】

以上、図面を参照して本発明の実施形態について述べたが、これらは本発明の例示であり、上記各実施形態の組み合わせ、又は上記以外の様々な構成を採用することもできる。

【０１２７】

上記の実施形態の一部又は全部は、以下の付記のようにも記載されうるが、以下には限られない。

１．　対象システムにおいて発生したイベントの集合であるイベント集合を第１の抽象レベルで表す第１の検出イベント情報を取得し、前記取得した第１の検出イベント情報によって表される前記イベント集合を第２の抽象レベルで表す第２の検出イベント情報を生成する第１生成部と、

それぞれが脅威活動を表す複数の脅威情報の中から、第１の前記検出イベント情報及び第２の前記検出イベント情報のうちの少なくとも一方との関連度が高い前記脅威情報を特定する特定部と、

前記特定された脅威情報と、その脅威情報との関連度が高い前記検出イベント情報に対応する抽象レベルである合致レベルとに基づいて、前記対象システムで発生している脅威に関する警告情報を生成する第２生成部と、を有する警告装置。

２．　前記イベントは、前記対象システム上で動作するプロセスの活動を表す、１．に記載の警告装置。

３．　前記第１の抽象レベルで表されたイベント集合では、イベントの主体であるプロセスの実行ファイル又はイベントの客体であるファイルについて、その識別情報が示され、

前記第２の抽象レベルで表されたイベント集合では、イベントの主体であるプロセスの実行ファイル又はイベントの客体であるファイルについて、その種類が示される、１．又は２．に記載の警告装置。

４．　前記脅威情報は、その脅威情報が表すイベント集合を第１の抽象度で表す第１の脅威イベント情報と、その脅威情報が表すイベント集合を第２の抽象度で表す第２の脅威イベント情報とを含み、

前記特定部は、

第１の前記検出イベント情報と各前記脅威情報の第１の脅威イベント情報との間で第１関連度を算出し、

第２の前記検出イベント情報と各前記脅威情報の第２の脅威イベント情報との間で第２関連度を算出し、

第１関連度又は第２関連度の少なくとも一方が閾値以上である前記脅威情報を特定する、１．乃至３．いずれか一つに記載の警告装置。

５．　前記第１生成部は、前記第１関連度が閾値以上である前記脅威情報が存在しない場合に、前記第２の検出イベント情報の生成を行う、４．に記載の警告装置。

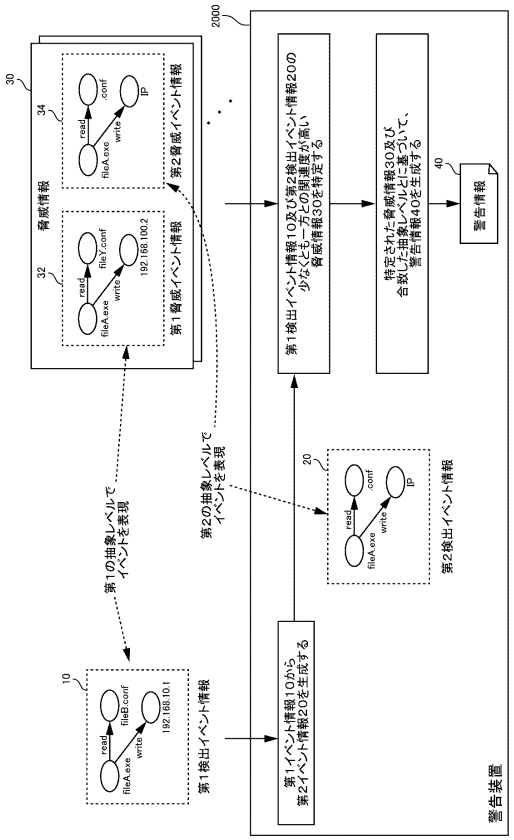
６．　前記特定部は、前記検出イベント情報に示されるイベント集合と前記脅威イベント

情報に示されるイベント集合との間で合致するイベントの総数を、前記脅威イベント情報に示されるイベント集合に含まれるイベントの総数で割ることで、前記検出イベント情報と前記脅威イベント情報との間の関連度を算出する、４．又は５．に記載の警告装置。
７．　前記特定部は、前記検出イベント情報に示されるイベント集合と前記脅威イベント情報に示されるイベント集合との間で合致する各イベントに付された重みの総和を、前記脅威イベント情報に示されるイベント集合に含まれる各イベントに付された重みの総和で割ることで、前記検出イベント情報と前記脅威イベント情報との間の関連度を算出する、４．又は５．に記載の警告装置。
８．　前記脅威イベント情報は、各イベントについてそのイベントを数値で表したイベント値を示し、
　前記特定部は、
　　前記検出イベント情報に示されている各イベントについて、そのイベントを数値で表したイベント値を算出し、
　　前記検出イベント情報に示されている各イベント値と、前記脅威イベント情報に示されている各イベント値とを比較することで、前記検出イベント情報に示されているイベントと前記脅威イベント情報に示されているイベントとが合致するか否かを判定する、４．乃至７．いずれか一つに記載の警告装置。
９．　前記脅威イベント情報は、前記イベント集合に含まれるイベントで扱われるデータのサイズに関する条件を示し、
　前記特定部は、前記検出イベント情報と前記脅威イベント情報との間の関連度を、前記検出イベント情報に示されるイベント集合と前記脅威イベント情報に示されるイベント集合との間でイベントが合致する度合い、及び前記検出イベント情報によって示されるイベントにおいて前記脅威イベント情報に示される前記条件が満たされるか否かの判定の結果に基づいて算出する、４．乃至８．いずれか一つに記載の警告装置。
１０．　前記警告情報は、前記検出イベント情報と前記特定された脅威情報との間で合致するイベントが前記合致レベルに応じた度合いで強調されている情報を含む、１．乃至９．いずれか一つに記載の警告装置。
【０１２８】
１１．　コンピュータによって実行される制御方法であって、
　対象システムにおいて発生したイベントの集合であるイベント集合を第１の抽象レベルで表す第１の検出イベント情報を取得し、前記取得した第１の検出イベント情報によって表される前記イベント集合を第２の抽象レベルで表す第２の検出イベント情報を生成する第１生成ステップと、
　それぞれが脅威活動を表す複数の脅威情報の中から、第１の前記検出イベント情報及び第２の前記検出イベント情報のうちの少なくとも一方との関連度が高い前記脅威情報を特定する特定ステップと、
　前記特定された脅威情報と、その脅威情報との関連度が高い前記検出イベント情報に対応する抽象レベルである合致レベルとに基づいて、前記対象システムで発生している脅威に関する警告情報を生成する第２生成ステップと、を有する制御方法。
１２．　前記イベントは、前記対象システム上で動作するプロセスの活動を表す、１１．に記載の制御方法。
１３．　前記第１の抽象レベルで表されたイベント集合では、イベントの主体であるプロセスの実行ファイル又はイベントの客体であるファイルについて、その識別情報が示され、
　前記第２の抽象レベルで表されたイベント集合では、イベントの主体であるプロセスの実行ファイル又はイベントの客体であるファイルについて、その種類が示される、１１．又は１２．に記載の制御方法。
１４．　前記脅威情報は、その脅威情報が表すイベント集合を第１の抽象度で表す第１の脅威イベント情報と、その脅威情報が表すイベント集合を第２の抽象度で表す第２の脅威イベント情報とを含み、
　前記特定ステップにおいて、

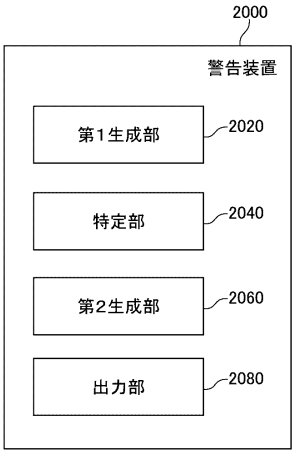
第１の前記検出イベント情報と各前記脅威情報の第１の脅威イベント情報との間で第１関連度を算出し、
第２の前記検出イベント情報と各前記脅威情報の第２の脅威イベント情報との間で第２関連度を算出し、
第１関連度又は第２関連度の少なくとも一方が閾値以上である前記脅威情報を特定する、１１．乃至１３．いずれか一つに記載の制御方法。
１５．　前記第１生成ステップにおいて、前記第１関連度が閾値以上である前記脅威情報が存在しない場合に、前記第２の検出イベント情報の生成を行う、１４．に記載の制御方法。
１６．　前記特定ステップにおいて、前記検出イベント情報に示されるイベント集合と前記脅威イベント情報に示されるイベント集合との間で合致するイベントの総数を、前記脅威イベント情報に示されるイベント集合に含まれるイベントの総数で割ることで、前記検出イベント情報と前記脅威イベント情報との間の関連度を算出する、１４．又は１５．に記載の制御方法。
１７．　前記特定ステップにおいて、前記検出イベント情報に示されるイベント集合と前記脅威イベント情報に示されるイベント集合との間で合致する各イベントに付された重みの総和を、前記脅威イベント情報に示されるイベント集合に含まれる各イベントに付された重みの総和で割ることで、前記検出イベント情報と前記脅威イベント情報との間の関連度を算出する、１４．又は１５．に記載の制御方法。
１８．　前記脅威イベント情報は、各イベントについてそのイベントを数値で表したイベント値を示し、
前記特定ステップにおいて、
前記検出イベント情報に示されている各イベントについて、そのイベントを数値で表したイベント値を算出し、
前記検出イベント情報に示されている各イベント値と、前記脅威イベント情報に示されている各イベント値とを比較することで、前記検出イベント情報に示されているイベントと前記脅威イベント情報に示されているイベントとが合致するか否かを判定する、１４．乃至１７．いずれか一つに記載の制御方法。
１９．　前記脅威イベント情報は、前記イベント集合に含まれるイベントで扱われるデータのサイズに関する条件を示し、
前記特定ステップにおいて、前記検出イベント情報と前記脅威イベント情報との間の関連度を、前記検出イベント情報に示されるイベント集合と前記脅威イベント情報に示されるイベント集合との間でイベントが合致する度合い、及び前記検出イベント情報によって示されるイベントにおいて前記脅威イベント情報に示される前記条件が満たされるか否かの判定の結果に基づいて算出する、１４．乃至１８．いずれか一つに記載の制御方法。
２０．　前記警告情報は、前記検出イベント情報と前記特定された脅威情報との間で合致するイベントが前記合致レベルに応じた度合いで強調されている情報を含む、１１．乃至１９．いずれか一つに記載の制御方法。
【０１２９】
２１．　１１．乃至２０．いずれか一つに記載の制御方法の各ステップをコンピュータに実行させるプログラム。

【図面】

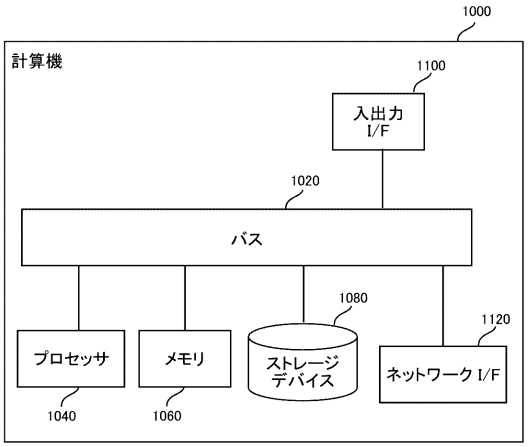
【図１】


2000
30
脅威情報
34
read
fileA.exe
write
.conf
IP
第2脅威イベント情報
32
read
fileA.exe
write
fileY.conf
192.168.100.2
第1脅威イベント情報
第1検出イベント情報10及び第2検出イベント情報20の
少なくとも一方との関連度が高い
脅威情報30を特定する
特定された脅威情報30及び
合致した抽象レベルに基づいて、
警告情報40を生成する
40
警告情報
第2の抽象レベルで
イベントを表現
20
read
fileA.exe
write
.conf
IP
第2検出イベント情報
第1の抽象レベルで
イベントを表現
10
read
fileA.exe
write
fileB.conf
192.168.10.1
第1検出イベント情報
第1イベント情報10から
第2イベント情報20を生成する
警告装置

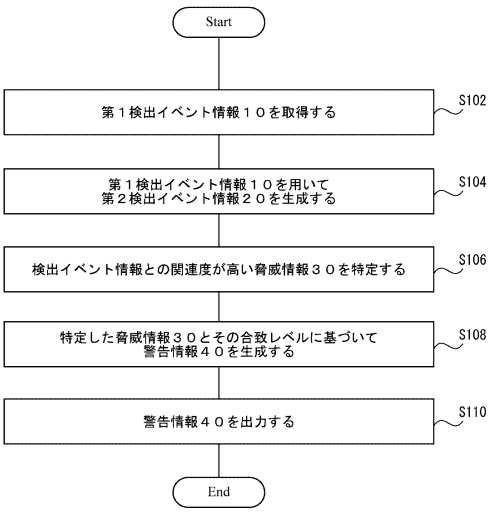
【図２】


2000
警告装置
第1生成部
2020
特定部
2040
第2生成部
2060
出力部
2080

【図３】


1000
計算機
1100
入出力
I/F
1020
バス
1080
1120
プロセッサ
メモリ
ストレージ
デバイス
ネットワーク I/F
1040
1060

【図４】


Start
第１検出イベント情報１０を取得する
S102
第１検出イベント情報１０を用いて
第２検出イベント情報２０を生成する
S104
検出イベント情報との関連度が高い脅威情報３０を特定する
S106
特定した脅威情報３０とその合致レベルに基づいて
警告情報４０を生成する
S108
警告情報４０を出力する
S110
End

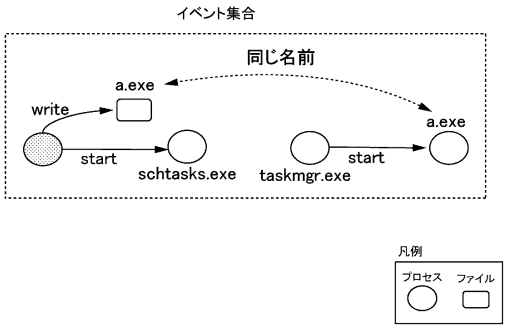
【図５】

200

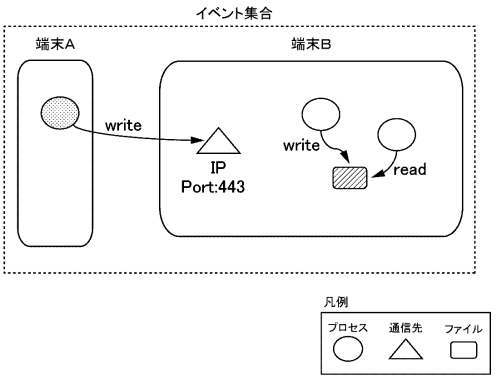
端末識別情報	主体情報 プロセスID	主体情報 スレッドID	主体情報 パス	客体情報 種類	客体情報 識別情報	内容情報	発生時刻
端末A	010	001	C¥:dir11/a1.exe	プロセス	D¥:dir21/dir22/a2.exe	起動	2018/1/10 10:05:24
端末A	010	002	C¥:dir11/a1.exe	ファイル	D¥:dir23/b2.conf	書き込み	2018/1/10 10:06:02
端末B	013	-	C¥:dir15/b1.exe	ソケット	socket1	読み込み	2018/1/11 9:06:02
…	…	…	…	…	…	…	…

201 202 204 206 207 208 209 210 212 214

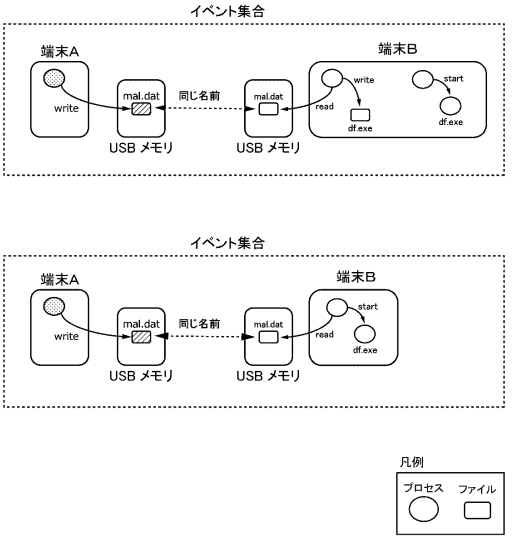
【図６】



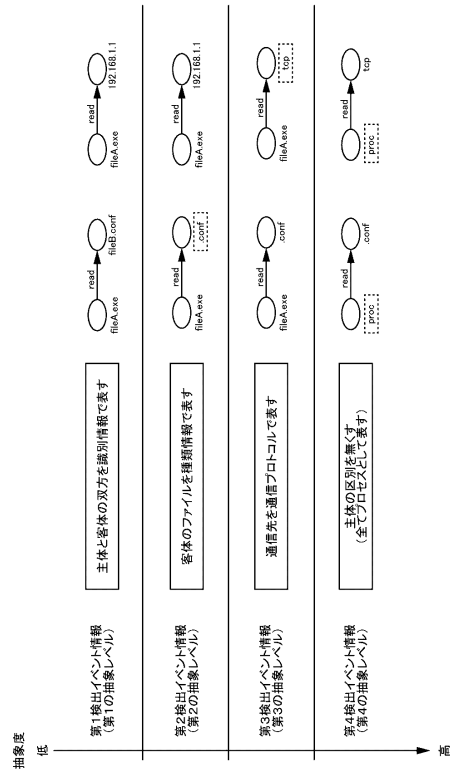
【図７】



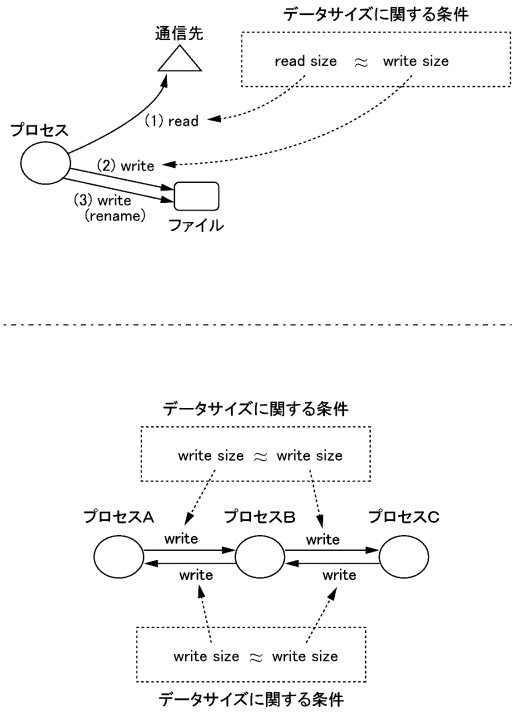
【図８】



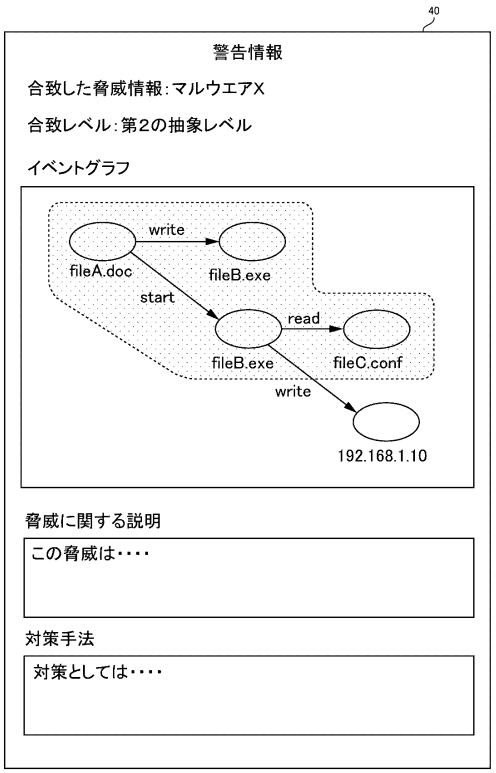
【図９】


抽象度
低
高
第1検出イベント情報
（第1の抽象レベル）
第2検出イベント情報
（第2の抽象レベル）
第3検出イベント情報
（第3の抽象レベル）
第4検出イベント情報
（第4の抽象レベル）
主体と客体の双方を識別情報で表す
客体のファイルを種類情報で表す
通信先を通信プロトコルで表す
主体の区別を無くす
（全てプロセスとして表す）
read
fileA.exe
192.168.1.1
fileB.conf
.conf
tcp
proc

【図１０】


データサイズに関する条件
通信先
read size ≈ write size
プロセス
(1) read
(2) write
(3) write
(rename)
ファイル
データサイズに関する条件
write size ≈ write size
プロセスA
プロセスB
プロセスC
write
write
write
write
write size ≈ write size
データサイズに関する条件

【図１１】


40
警告情報
合致した脅威情報：マルウエアX
合致レベル：第2の抽象レベル
イベントグラフ
write
fileA.doc
fileB.exe
start
read
fileB.exe
fileC.conf
write
192.168.1.10
脅威に関する説明
この脅威は・・・・
対策手法
対策としては・・・・

フロントページの続き

東京都港区芝五丁目７番１号 日本電気株式会社内

審査官　吉田 歩

(56)参考文献

特表２０１７－５２７９３１（ＪＰ，Ａ）
国際公開第２０１９／０４９２４３（WO，Ａ１）
国際公開第２０１８／０７０４０４（WO，Ａ１）
特開２０１３－０９８９１５（ＪＰ，Ａ）
芝田 文 ほか，マルウェア動的解析のネットワーク接続制御を支援するユーザインタフェースの提案，情報処理学会研究報告 IPSJ SIG Technical Reports，日本，社団法人情報処理学会 Information Processing Socie，2009年02月26日，Vol.2009, No.20，p.277-279

(58)調査した分野 (Int.Cl.，ＤＢ名)

Ｇ０６Ｆ　２１／５５