

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2017-167695

(P2017-167695A)

(43) 公開日 平成29年9月21日(2017.9.21)

(51) Int.Cl.

G06F 21/57 (2013.01)

F I

G06F 21/57

テーマコード (参考)

審査請求 未請求 請求項の数 17 O L (全 39 頁)

(21) 出願番号 特願2016-50471 (P2016-50471)
 (22) 出願日 平成28年3月15日 (2016.3.15)

(71) 出願人 000006013
 三菱電機株式会社
 東京都千代田区丸の内二丁目7番3号
 394013002
 三菱電機インフォメーションシステムズ株式会社
 東京都港区芝浦四丁目13番23号
 (74) 代理人 100099461
 弁理士 溝井 章司
 (74) 代理人 100187300
 弁理士 長谷川 靖子
 (72) 発明者 榊原 裕之
 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内

最終頁に続く

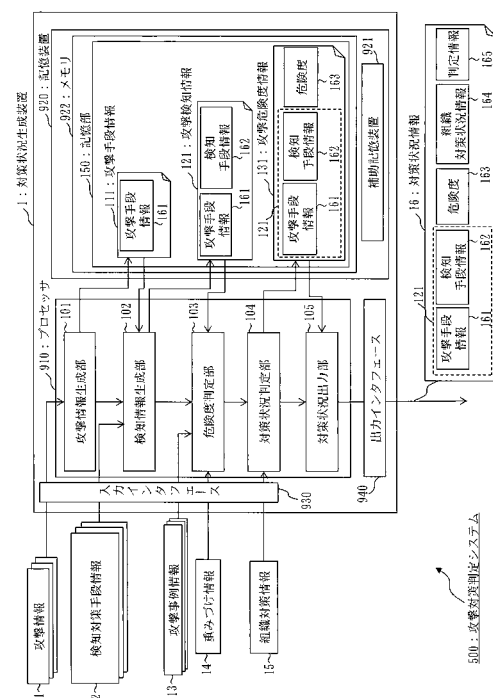
(54) 【発明の名称】 攻撃対策判定システム、攻撃対策判定方法及び攻撃対策判定プログラム

(57) 【要約】

【課題】 攻撃手段に対する組織の対策をよりの確に判定することができる攻撃対策判定システムを提供することを目的とする。

【解決手段】 サイバー攻撃の攻撃手段と、攻撃手段を検知する検知手段と、攻撃手段に対する検知手段の検知精度を含む攻撃検知情報121を生成する検知情報生成部102と、攻撃検知情報121と、サイバー攻撃の対象となる組織において攻撃手段に対する対策として実施されている検知手段を組織検知手段として含む組織対策情報15とを取得し、攻撃検知情報121に含まれる検知精度と組織対策情報15とに基づいて、組織における対策の効果の程度を表す効果度を判定する対策状況判定部104とを備えた。

【選択図】 図2



【特許請求の範囲】

【請求項 1】

サイバー攻撃の攻撃手段と、前記攻撃手段を検知する検知手段と、前記攻撃手段に対する前記検知手段の検知精度とを含む攻撃検知情報を生成する検知情報生成部と、

前記攻撃検知情報と、前記サイバー攻撃の対象となる組織において前記攻撃手段に対する対策として実施されている検知手段を組織検知手段として含む組織対策情報とを取得し、前記攻撃検知情報に含まれる前記検知精度と前記組織対策情報とに基づいて、前記組織における前記対策の効果の程度を表す効果度を判定する対策状況判定部とを備えた攻撃対策判定システム。

【請求項 2】

10

前記攻撃対策判定システムは、さらに、

前記攻撃手段と前記効果度とを対策状況情報として出力する対策状況出力部を備えた請求項 1 に記載の攻撃対策判定システム。

【請求項 3】

前記対策状況出力部は、

前記攻撃手段を検知する前記検知手段と、前記検知手段の前記検知精度とを前記対策状況情報に含める請求項 2 に記載の攻撃対策判定システム。

【請求項 4】

前記対策状況判定部は、

前記検知精度と前記組織対策情報とに基づいて、前記検知手段が前記組織において実施されているか否かを示す組織対策状況情報を生成し、前記組織対策状況情報に基づいて前記効果度を判定する請求項 2 又は 3 に記載の攻撃対策判定システム。

20

【請求項 5】

前記対策状況出力部は、

前記組織対策状況情報を前記対策状況情報に含める請求項 4 に記載の攻撃対策判定システム。

【請求項 6】

前記攻撃対策判定システムは、さらに、

前記検知手段の前記検知精度に基づいて、前記攻撃手段の危険度を判定する危険度判定部を備え、

30

前記対策状況出力部は、

前記攻撃手段の危険度を前記対策状況情報に含める請求項 2 から 5 のいずれか 1 項に記載の攻撃対策判定システム。

【請求項 7】

前記危険度判定部は、

前記検知手段の前記検知精度と前記攻撃手段が実施される前記サイバー攻撃における攻撃フェーズとに基づいて、前記危険度を判定する請求項 6 に記載の攻撃対策判定システム。

【請求項 8】

前記検知情報生成部は、

40

前記攻撃手段を説明する説明文を含む攻撃手段情報と、前記検知手段が検知する攻撃手段を前記検知精度に応じて取得するためのキーワードを含む検知対策手段情報とを取得し、前記キーワードを用いて前記攻撃手段情報に含まれる前記説明文を検索し、前記検知手段が検知する攻撃手段を前記検知精度に応じて検出する請求項 1 から 7 のいずれか 1 項に記載の攻撃対策判定システム。

【請求項 9】

前記検知情報生成部は、

前記検知手段により検知される攻撃手段であって前記検知手段の前記検知精度に応じた攻撃手段を含む検知対策手段情報を取得し、前記検知対策手段情報に基づいて、前記検知手段が検知する攻撃手段を前記検知精度に応じて検出する請求項 1 から 7 のいずれか 1 項

50

に記載の攻撃対策判定システム。

【請求項 10】

前記検知情報生成部は、

前記検知精度として、前記検知手段が前記攻撃手段を検知できない第1検知精度と、前記検知手段による前記攻撃手段の検知漏れの場合がある第2検知精度と、前記検知手段が前記攻撃手段を誤検知する場合がある第3検知精度と、前記検知手段が前記攻撃手段を誤検知せず、かつ、前記検知手段による前記攻撃手段の検知漏れがない第4検知精度と、前記検知手段が前記攻撃手段を検知できる場合と、前記検知手段が前記攻撃手段を検知できない場合と、前記検知手段が前記攻撃手段を誤検知する場合とがある第5検知精度との少なくともいずれかを有する請求項1から9のいずれか1項に記載の攻撃対策判定システム。

10

【請求項 11】

前記攻撃対策判定システムは、さらに、

前記攻撃手段の危険度を含む攻撃手段情報を取得する危険度判定部を備え、

前記対策状況出力部は、

前記攻撃手段の危険度を前記対策状況情報に含める請求項2から7のいずれか1項に記載の攻撃対策判定システム。

【請求項 12】

前記攻撃対策判定システムは、さらに、

前記サイバー攻撃の攻撃フェーズと前記攻撃フェーズにおいて実施される攻撃手段とを含む攻撃事例情報と、前記対策状況情報とを取得し、前記対策状況情報を用いて、前記攻撃事例情報について前記攻撃フェーズの攻撃手段ごとに前記組織の対策状況を判定する攻撃事例判定部を備えた請求項2から7のいずれか1項に記載の攻撃対策判定システム。

20

【請求項 13】

前記攻撃事例判定部は、

前記攻撃事例情報と前記組織の対策状況とを攻撃事例対応情報として出力する請求項12に記載の攻撃対策判定システム。

【請求項 14】

前記攻撃対策判定システムは、さらに、

前記組織の対策状況に基づいて選択された選択攻撃手段と前記選択攻撃手段以外の攻撃手段とを含む前記攻撃事例情報を取得し、前記選択攻撃手段と組み合わせて使用される攻撃手段を前記攻撃事例情報から判定する対策候補抽出部を備えた請求項12または13に記載の攻撃対策判定システム。

30

【請求項 15】

前記対策候補抽出部は、

前記選択攻撃手段と組み合わせて使用される攻撃手段を強化対策情報として出力する請求項14に記載の攻撃対策判定システム。

【請求項 16】

検知情報生成部が、サイバー攻撃の攻撃手段と、前記攻撃手段を検知する検知手段と、前記攻撃手段に対する前記検知手段の検知精度とを含む攻撃検知情報を生成し、

40

対策状況判定部が、前記攻撃検知情報と、前記サイバー攻撃の対象となる組織において前記攻撃手段に対する対策として実施されている検知手段を組織検知手段として含む組織対策情報とを取得し、前記攻撃検知情報に含まれる前記検知精度と前記組織対策情報とに基づいて、前記組織における前記対策の効果の程度を表す効果度を判定する攻撃対策判定方法。

【請求項 17】

サイバー攻撃の攻撃手段と、前記攻撃手段を検知する検知手段と、前記攻撃手段に対する前記検知手段の検知精度とを含む攻撃検知情報を生成する検知情報生成処理と、

前記攻撃検知情報と、前記サイバー攻撃の対象となる組織において前記攻撃手段に対する対策として実施されている検知手段を組織検知手段として含む組織対策情報とを取得し

50

、前記攻撃検知情報に含まれる前記検知精度と前記組織対策情報とに基づいて、前記組織における前記対策の効果の程度を表す効果度を判定する対策状況判定処理とをコンピュータに実行させる攻撃対策判定プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、組織の情報システムに対するサイバー攻撃対策における不足や補強を判定する攻撃対策判定システム、攻撃対策判定方法及び攻撃対策判定プログラムに関する。

【背景技術】

【0002】

近年、マルウェアが機密情報を組織外に漏洩させる事故が問題となっている。マルウェアを用いたサイバー攻撃は高度化されつつあり、具体例として、非特許文献1に示されるAPT（高度かつ継続的な脅威：Advanced・Persistent・Threat）と呼ばれる攻撃等がある。

【0003】

APTでは、添付メールなどで組織に侵入したマルウェアが、計算機に感染し、さらに、攻撃者が運用するインターネット上のC&C（Command&Control）サーバと通信し、新しいマルウェアや攻撃ツールをダウンロードしたり自身をアップデートする。そして、マルウェアはC&Cサーバから命令を受信して、組織内を偵察し、ファイルサーバを見つけ、機密ファイルをC&Cサーバへ通信で漏洩する。これらの各活動を、攻撃とみなした場合、各攻撃は、長時間かけて段階的に行われる。具体例として、計算機に感染したマルウェアは、感染後、1ヶ月は活動せず身を潜め、1ヵ月後にC&Cサーバと通信を開始する。

【0004】

APT対策の既存技術として、不審なHTTP（Hypertext・Transfer・Protocol）通信を検知する技術、パターンファイルによるウィルス検知技術など様々なものがある。この様なAPT対策の例として非特許文献1がある。

【0005】

また、サイバー攻撃対策を行うにあたり、対策する攻撃手段は多数あり、情報システムを安全に守るためには、網羅的な攻撃手段の情報に対して、どの攻撃手段を対策すべきか調べた上で、攻撃を検知・対策するセキュリティ施策を行う必要がある。網羅的な攻撃手段の情報の例として非特許文献2がある。この文献に示される攻撃手段のリストには、攻撃手段の概要、攻撃方法、影響、検知や対策の方法が示されている。

【0006】

また、サイバー攻撃について、どの様な攻撃が発生したかを情報共有するためのフォーマットとして、非特許文献3がある。

【0007】

また、特許文献1には、セキュリティ監視サービスにおいて、サービス利用者が契約しているセキュリティサービスメニューや対策を変更することにより、現在起きている攻撃手段を回避可能か表示する機能が開示されている。

【先行技術文献】

【特許文献】

【0008】

【特許文献1】特開2015-026182号公報

【非特許文献】

【0009】

【非特許文献1】「新しいタイプの攻撃」の対策に向けた設計・運用ガイド改訂第2版、IPA、2011年11月、<https://www.ipa.go.jp/files/000017308.pdf>

【非特許文献2】攻撃手段のリストの例、CAPEC：Common Attack P

10

20

30

40

50

attern Enumeration and Classification, <https://capec.mitre.org/>

【非特許文献3】攻撃手段のリストの例、STIX:Structured Threat Information Expression, <https://stix.mitre.org/>

【発明の概要】

【発明が解決しようとする課題】

【0010】

サイバー攻撃は様々な攻撃手段を用いて行われるため、情報システムにおけるサイバー攻撃対策を確実に行うためには、CAPEC(Common・Attack・Pattern・Enumeration・and・Classification:共通攻撃パターン一覧)などで示される網羅的な攻撃手段のリストを参照し、1つ1つの攻撃手段についてどの様な検知・対策を行うか検討する必要がある。

10

ここで、検知と対策について説明する。

検知は攻撃手段を見つけることである。具体例として、攻撃パケットをIDS(Intrusion・Detection・System)で検知することが該当する。

対策は、実施することでその攻撃手段が実行されても被害を受けない施策である。具体例として、ソフトウェアの脆弱性修正パッチを適用することで、その脆弱性への攻撃が発生しても影響を受けないような、パッチ適用が該当する。

また、マルウェアについては、アンチマルウェアソフトで検知して駆除する場合がある。この施策は検知と対策の両方を含んだものである。

20

以後、検知、対策という文言は、上記の様な意味で使用するものとする。

【0011】

また、検知・対策の導入に伴う費用や運用負荷の増加などの理由で、全ての攻撃手段について検知・対策を行うことができない場合があり、優先的に対策する攻撃手段を抽出する必要がある。

さらに、ある攻撃手段について、その攻撃手段を検知する機能があるセキュリティ製品や検知技術を検知・対策として適用したとしても、その方法によっては、検知漏れが発生する場合がある。具体例として、プログラムの不審な振る舞いを検知することでウィルスなどの不正プログラムを検知する製品があったとしても、不正プログラムが正常なプログラムに似た振る舞いの範囲で不正な活動をすれば検知漏れすることがある。また、誤検知が多い製品の場合は、一定時間内に同じ検知アラートが閾値回数以上発生した場合にのみ、攻撃を検知したと判断する運用があり、この条件を満たさない攻撃は検知漏れすることになる。従って、攻撃手段について、検知・対策を実施していても、検知漏れする場合があるため、検知を強化する必要がある。

30

【0012】

しかし、従来は、攻撃手段に対し実施済の検知・対策について、他の検知・対策による強化をすべきか、強化する場合はどの様に実施したらよいかを示す技術が無かった。

特許文献1では、現在発生している攻撃手段について、契約している検知・対策サービスメニューを、予め用意された別の検知・対策サービスメニューの中から適切なものに変更することで、対応することが示されている。しかし、用意している検知・対策サービスメニューについて、検知漏れや誤検知を考慮したうえでこれらを強化する方式については示されていない。

40

【0013】

本発明は、検知手段の検知漏れや誤検知を考慮した検知精度に基づいて、攻撃手段に対する組織の対策をよりの確に判定することができる攻撃対策判定システムを提供することを目的とする。

【課題を解決するための手段】

【0014】

本発明に係る攻撃対策判定システムは、

50

サイバー攻撃の攻撃手段と、前記攻撃手段を検知する検知手段と、前記攻撃手段に対する前記検知手段の検知精度とを含む攻撃検知情報を生成する検知情報生成部と、

前記攻撃検知情報と、前記サイバー攻撃の対象となる組織において前記攻撃手段に対する対策として実施されている検知手段を組織検知手段として含む組織対策情報とを取得し、前記攻撃検知情報に含まれる前記検知精度と前記組織対策情報とに基づいて、前記組織における前記対策の効果の程度を表す効果度を判定する対策状況判定部とを備えた。

【発明の効果】

【0015】

本発明に係る攻撃対策判定システムでは、検知情報生成部が、攻撃手段に対する検知手段の検知精度を含む攻撃検知情報を生成し、対策状況判定部が、攻撃検知情報と、組織において攻撃手段に対する対策として実施されている検知手段を組織検知手段として含む組織対策情報とを取得し、検知精度と組織対策情報とに基づいて、組織における対策の効果の程度を表す効果度を判定する。このように、本発明に係る攻撃対策判定システムによれば、検知精度に基づいて攻撃手段に対する組織の対策を判定することができ、よりの確に組織の対策を判定することができるという効果を奏する。

【図面の簡単な説明】

【0016】

【図1】実施の形態1に係る対策状況生成装置1、攻撃事例判定装置2、対策候補抽出装置3の関係を示す図。

【図2】実施の形態1に係る対策状況生成装置1の構成図。

【図3】実施の形態1に係る攻撃対策判定方法510及び攻撃対策判定プログラム520の攻撃対策判定処理S100のフロー図。

【図4】実施の形態1に係る攻撃情報生成処理S110の入出力の構成図。

【図5】実施の形態1に係る攻撃情報生成処理S110のフロー図。

【図6】実施の形態1に係る検知情報生成処理S120の入出力の構成図。

【図7】実施の形態1に係る検知対策手段情報12の例を示す図。

【図8】実施の形態1に係る検知対策手段情報12の別例を示す図。

【図9】実施の形態1に係るキーワード変換表の例を示す図。

【図10】実施の形態1に係る検知情報生成処理S120のフロー図。

【図11】実施の形態1に係る検知情報生成処理S120で用いる判定表1201を示す図。

【図12】実施の形態1に係る危険度判定処理S130の入出力の構成図。

【図13】実施の形態1に係る攻撃事例情報13の一例を示す図。

【図14】実施の形態1に係る重みづけ情報14の一例を示す図。

【図15】実施の形態1に係る危険度判定処理S130のフロー図。

【図16】実施の形態1に係る攻撃対策状況判定処理S140の入出力の構成図。

【図17】実施の形態1に係る組織対策情報15の一例を示す図。

【図18】実施の形態1に係る攻撃対策状況判定処理S140のフロー図。

【図19】実施の形態1の変形例に係る対策状況生成装置1の構成図。

【図20】実施の形態2に係る攻撃事例判定装置2の構成及び入出力を示す図。

【図21】実施の形態2に係る攻撃事例判定部201による攻撃事例判定処理S200のフロー図。

【図22】実施の形態3に係る対策候補抽出装置3の構成及び入出力を示す図。

【図23】実施の形態3に係る対策候補抽出装置3の構成及び入出力の別例を示す図。

【図24】実施の形態3に係る対策候補抽出処理S300のフロー図。

【図25】実施の形態4に係る対策候補抽出装置3の構成及び入出力を示す図。

【図26】実施の形態10に係る組織対策情報15aの構成図。

【発明を実施するための形態】

【0017】

10

20

30

40

50

実施の形態 1.

構成の説明

図 1 を用いて、本実施の形態に係る対策状況生成装置 1、攻撃事例判定装置 2、対策候補抽出装置 3 の関係について説明する。

対策状況生成装置 1 は、攻撃情報 1 1 に対して、検知対策手段情報 1 2、組織対策情報 1 5、攻撃事例情報 1 3、及び重みづけ情報 1 4 を用いて、対策状況情報 1 6 を出力する。攻撃情報 1 1 は、攻撃手段に関する情報である。検知対策手段情報 1 2 は、検知漏れ、誤検知可能性の情報を含む検知・対策の情報である。組織対策情報 1 5 は、対策状況生成装置 1 により攻撃への対策状況を調査する対象の組織における実施済の対策情報である。攻撃事例情報 1 3 は、サイバー攻撃の事例情報である。重みづけ情報 1 4 は、危険度を判定するための情報である。対策状況情報 1 6 は、攻撃情報 1 1 に含まれる攻撃手段に対する組織の対策状況に対する評価判定を含む情報である。

【0018】

攻撃事例判定装置 2 は、対策状況情報 1 6 を用いて、ある攻撃事例情報 1 3 a に対して対策できているかを判定し、攻撃事例対応情報 1 7 を出力する。

【0019】

対策候補抽出装置 3 は、攻撃事例対応情報 1 7 において、誤検知あり、あるいは回避可能として判定された攻撃手段について対策を強化するための情報である強化対策情報 1 8 を出力する。

【0020】

図 2 を用いて、本実施の形態に係る対策状況生成装置 1 の構成について説明する。

本実施の形態において、対策状況生成装置 1 は、コンピュータである。対策状況生成装置 1 は、プロセッサ 9 1 0、記憶装置 9 2 0、入力インタフェース 9 3 0、出力インタフェース 9 4 0 といったハードウェアを備える。

また、対策状況生成装置 1 は、機能構成として、攻撃情報生成部 1 0 1 と、検知情報生成部 1 0 2 と、危険度判定部 1 0 3 と、対策状況判定部 1 0 4 と、対策状況出力部 1 0 5、記憶部 1 5 0 とを備える。以下の説明では、対策状況生成装置 1 における攻撃情報生成部 1 0 1 と、検知情報生成部 1 0 2 と、危険度判定部 1 0 3 と、対策状況判定部 1 0 4 と、対策状況出力部 1 0 5 との機能を、対策状況生成装置 1 の「部」の機能という。対策状況生成装置 1 の「部」の機能は、ソフトウェアで実現される。

また、記憶部 1 5 0 は、記憶装置 9 2 0 で実現される。記憶部 1 5 0 には、攻撃手段情報 1 1 1 と、攻撃検知情報 1 2 1 と、攻撃検知危険度情報 1 3 1 とが記憶される。対策状況出力部 1 0 5 により出力される対策状況情報 1 6 が記憶されていてもよい。

【0021】

プロセッサ 9 1 0 は、信号線を介して他のハードウェアと接続され、これら他のハードウェアを制御する。

プロセッサ 9 1 0 は、プロセッシングを行う IC (Integrated・Circuit) である。プロセッサ 9 1 0 は、具体的には、CPU (Central・Processing・Unit) である。

【0022】

記憶装置 9 2 0 は、補助記憶装置 9 2 1 及びメモリ 9 2 2 を含む。補助記憶装置 9 2 1 は、具体的には、ROM (Read・Only・Memory)、フラッシュメモリ、又は、HDD (Hard・Disk・Drive) である。メモリ 9 2 2 は、具体的には、RAM (Random・Access・Memory) である。記憶部 1 5 0 は、メモリ 9 2 2 により実現される。なお、記憶部 1 5 0 は、補助記憶装置 9 2 1 により実現されていてもよいし、補助記憶装置 9 2 1 とメモリ 9 2 2 の両方により実現されてもよい。

【0023】

入力インタフェース 9 3 0 は、マウス、キーボード、タッチパネルといった入力装置と接続されるポートである。入力インタフェース 9 3 0 は、攻撃情報 1 1、検知対策手段情報 1 2、攻撃事例情報 1 3、重みづけ情報 1 4、組織対策情報 1 5 を対策状況生成装置 1

に取り込む。入力インタフェース 930 は、具体的には、USB (Universal・Serial・Bus) 端子、RS-232C といったシリアルインタフェースである。なお、入力インタフェース 930 は、LAN (Local・Area・Network) と接続されるポートであってもよい。

【0024】

出力インタフェース 940 は、ディスプレイといった表示機器のケーブルが接続されるポートである。出力インタフェース 940 は、具体例として、USB 端子、HDMI (登録商標) (High・Definition・Multimedia・Interface) 端子、RS-232C といったシリアルインタフェースである。ディスプレイは、具体的には、LCD (Liquid・Crystal・Display) である。

10

【0025】

補助記憶装置 921 には、「部」の機能を実現するプログラムが記憶されている。このプログラムは、メモリ 922 にロードされ、プロセッサ 910 に読み込まれ、プロセッサ 910 によって実行される。補助記憶装置 921 には、OS (Operating・System) も記憶されている。OS の少なくとも一部がメモリ 922 にロードされ、プロセッサ 910 は OS を実行しながら、「部」の機能を実現するプログラムを実行する。

【0026】

対策状況生成装置 1 は、1 つのプロセッサ 910 のみを備えていてもよいし、複数のプロセッサ 910 を備えていてもよい。複数のプロセッサ 910 が「部」の機能を実現するプログラムを連携して実行してもよい。

20

【0027】

「部」の機能による処理の結果を示す情報、データ、信号値、及び、変数値は、補助記憶装置 921、メモリ 922、又は、プロセッサ 910 内のレジスタ又はキャッシュメモリに記憶される。なお、図 2 において、「部」の各部と記憶部 150 とを結ぶ矢印は、各部による処理の結果を記憶部 150 に記憶する、あるいは、記憶部 150 から情報を各部が読み出すことを表している。また、各部同士を結ぶ矢印は、制御の流れを表している。なお、情報が各部同士でメモリ 922 を介して授受されることを表すメモリ 922 と各部間の矢印については省略する。

【0028】

「部」の機能を実現するプログラムは、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ブルーレイ (登録商標) ディスク、DVD (Digital・Versatile・Disc) といった可搬記録媒体に記憶されてもよい。

30

なお、「部」の機能を実現するプログラムを攻撃対策判定プログラム 520 ともいう。攻撃対策判定プログラムは、「部」として説明している機能を実現するプログラムである。また、攻撃対策判定プログラムプロダクトと称されるものは、攻撃対策判定プログラムが記録された記憶媒体及び記憶装置であり、見た目の形式に関わらず、コンピュータ読み取り可能なプログラムをロードしているものである。

【0029】

動作の説明

図 3 は、本実施の形態に係る攻撃対策判定方法 510 及び攻撃対策判定プログラム 520 の攻撃対策判定処理 S100 のフロー図である。

40

図 3 に示すように、攻撃対策判定処理 S100 は、攻撃情報生成処理 S110 と、検知情報生成処理 S120 と、危険度判定処理 S130 と、対策状況判定処理 S140 と、対策状況出力処理 S150 とを有する。

【0030】

<攻撃情報生成処理 S110>

図 4 を用いて、本実施の形態に係る攻撃情報生成処理 S110 の入出力の構成について説明する。

攻撃情報生成部 101 は、サイバー攻撃の攻撃手段を表現した CAPEC などの複数の攻撃情報 11 を入力とし、攻撃手段情報 111 を出力する。攻撃情報 11 は、攻撃手段 I

50

D、攻撃名称、説明文、重大度、検知・対策、影響を受けるソフトウェア名の情報などで構成される。本実施の形態では、攻撃情報生成部101は、1つの攻撃情報11から、攻撃手段ID、攻撃名称、説明文を抽出して、攻撃手段情報111において1行の情報として記録する。1行の情報をエントリともいう。この処理を全ての攻撃情報11について行う。この結果、攻撃情報生成部101は図4に示す攻撃手段情報111を出力する。図4では、攻撃手段情報111を表として表現している。なお、少なくとも攻撃手段ID或いは攻撃名称のいずれかからサイバー攻撃の攻撃手段21が特定されるものとする。説明文は単に説明ともいう。

【0031】

次に、図5を用いて、本実施の形態に係る攻撃情報生成処理S110の流れについて説明する。

ステップS111において、攻撃情報生成部101は、aという変数に攻撃情報11の数、すなわち幾つの攻撃情報11が存在するかを設定する。さらに、攻撃情報生成部101は、攻撃情報11から、攻撃情報iを選択する。ここで、iは1から攻撃情報11の数までの自然数をとる。

ステップS112において、攻撃情報生成部101は、 $i > a$ である場合は、処理を終わる。 $i > a$ で無い場合は、ステップS113へ進む。

ステップS113において、攻撃情報生成部101は、攻撃情報iから、攻撃手段ID、攻撃名称、説明文を抽出して、攻撃手段情報111に1行の情報として加える。

ステップS114において、攻撃情報生成部101は、iをインクリメントする。

【0032】

以上で、攻撃情報生成処理S110についての説明を終わる。

【0033】

<検知情報生成処理S120>

図6を用いて、本実施の形態に係る検知情報生成処理S120の入出力の構成について説明する。

検知情報生成部102は、サイバー攻撃の攻撃手段21と、攻撃手段21を検知する検知手段22と、攻撃手段21に対する検知手段22の検知精度23とを含む攻撃検知情報121を生成する。

【0034】

具体的には、検知情報生成部102は、攻撃手段21を含む攻撃手段情報111と、検知・対策の技術・製品に関する検知対策手段情報12とを入力し、攻撃検知情報121を出力する。ここで、検知・対策の技術・製品を攻撃手段21に対して検知・対策する検知手段22とする。検知手段22は、検知・対策、あるいは検知・対策手段ともいう。攻撃検知情報121は、攻撃手段情報111における、攻撃手段IDで識別される攻撃手段21について、検知手段22の情報をマッピングしたものである。また、攻撃検知情報121には、検知手段22が攻撃手段21に対し、どの程度有効であるかを示す検知精度23が設定される。攻撃検知情報121は、攻撃手段・検知対策手段情報ともいう。

【0035】

具体例として、検知対策手段情報12は、IDS/FW(FireWall)/メールフィルタなどの検知・対策の技術や製品の情報と、プロキシログを分析/FWログを分析などのログ分析の情報との検知手段22から構成される。この場合、検知精度23とは、どの検知・対策の技術や製品/ログ分析が、攻撃手段21への対策として有効かを、○：検知可能、×：検知不可能、△：誤検知の可能性あり、□：検知漏れの可能性あり、◇：検知可能・検知不可能・誤検知ありという表現で表したものである。すなわち、検知精度23は、検知手段22が攻撃手段21を検知できない第1検知精度(×：検知不可能)と、検知手段22による攻撃手段21の検知漏れの場合がある第2検知精度(□：検知漏れの可能性あり)と、検知手段22が攻撃手段21を誤検知する場合がある第3検知精度(△：誤検知の可能性あり)と、検知手段22が攻撃手段21を誤検知せず、かつ、検知手段22による攻撃手段21の検知漏れがない第4検知精度(○：検知可能)と、検知手段

10

20

30

40

50

2 2 が攻撃手段 2 1 を検知できる場合と、検知手段 2 2 が攻撃手段 2 1 を検知できない場合と、検知手段 2 2 が攻撃手段 2 1 を誤検知する場合とがある第 5 検知精度（◇：検知可能・検知不可能・誤検知あり）とを有する。なお、検知精度 2 3 は、第 1 検知精度（×：検知不可能）と、第 2 検知精度（□：検知漏れの可能性あり）と、第 3 検知精度（△：誤検知の可能性あり）と、第 4 検知精度（○：検知可能）と、第 5 検知精度（◇：検知可能・検知不可能・誤検知あり）との少なくともいずれかを有していてもよい。

ここで、「検知手段 2 2 が、攻撃手段 2 1 を誤検知する」とは、検知手段 2 2 が攻撃手段 2 1 以外の正常な通信／処理、攻撃手段 2 1 以外の攻撃を誤って攻撃手段 2 1 として検知してしまうことを意味する。

【0036】

図 7 は、本実施の形態に係る検知対策手段情報 1 2 の例を示す図である。図 7 では、検知対策手段情報 1 2 にセキュリティ製品が示される例を示している。また、図 7 では、検知対策手段情報 1 2 を表として表現する。以下に、表のカラムの意味を説明する。

「CM__ID」は、1 つの検知・対策情報を区別するための ID である。

「製品カテゴリ」は、FW、振る舞い検知などの、セキュリティ製品のカテゴリを示す。ここで、製品カテゴリには、ハードウェア、ソフトウェア、システムなどの製品のカテゴリ、無償で公開されているハードウェア、ソフトウェア、システムなどのカテゴリ、セキュリティ技術のカテゴリなどが含まれる。

「検知可能」は、当製品で検知できる攻撃手段を示す。

「検知不可能」は、当製品で検知できない攻撃手段を示す。

「誤検知」は、当製品で誤って検知する処理や通信を示す。

【0037】

具体例として、図 7 の検知対策手段情報 1 2 の 1 行目を用いて説明する。

「CM__ID」が CM__ID__1 のセキュリティ製品である。

「製品カテゴリ」は次世代 FW であり、「製品カテゴリ」を示す名称“次世代 FW”と、この「製品カテゴリ」を示すキーワードとして、[NGFW] (Next・Generation・Fire・Wall) が設定される。当製品は、レピュテーション機能と、大量の HTTP 通信量が発生した場合に不審な HTTP 通信として検知する製品である。ここで、レピュテーション機能とは、様々な Web サイトについて悪性か否かを判定した情報を蓄積したデータベースを用いて、HTTP 通信している Web サイトが不正か否かを判断し、不正であると判断した場合は、不審な HTTP 通信が行われていると検知する機能である。

「検知可能」は、“不審な HTTP 通信”であり、当製品に備わっているレピュテーション機能や大量の HTTP 通信の検知機能により不審な HTTP 通信として検知可能、という意味である。“不審な HTTP 通信”を示すキーワードとして [URL, Suspicious, HTTP] が設定される。

「検知不可能」は、“改ざんされた正規サイトとの HTTP 通信”である。レピュテーション機能は、改ざんされた正規サイトについて、改ざんされてすぐの場合は、データベースに「改ざんされており悪性の Web サイトである」という情報が反映されない場合があり、その場合この Web サイトとの通信を不審として検知しない。“改ざんされた正規サイトとの HTTP 通信”を示すキーワードとして [URL, legitimate, HTTP] が設定される。

「誤検知」は、“正規の大量の HTTP 通信”である。正規 Web サイトとの通信が、偶然に大量に発生した場合に、不審な通信として誤検知する。“正規の大量の HTTP 通信”を示すキーワードとして [URL, legitimate, HTTP] が設定される。

なお、2 行目の CM__ID__2 は振る舞い検知 (AP: Appliance)、3 行目の CM__ID__3 は IDS (シグネチャ型) についての例である。なお、CM__ID__3 の誤検知の様に該当する事項が無い場合は無と記述している。

また、キーワードについては、後で使い方を詳しく説明する。

10

20

30

40

50

以上のように、図7の検知対策手段情報12では、セキュリティ製品の種類ごとに、検知可能、検知不可能、誤検知可能性の情報を格納する。

【0038】

図8は、本実施の形態に係る検知対策手段情報12の別例を示す図である。図8では、検知対策手段情報12に、ログ分析が示される例を示している。以下に図8の表のカラムの意味を説明する。

「CM_ID」は、1つの検知・対策を区別するためのIDである。

「ログ種類」は、攻撃手段を検知するために分析するログの種類を示す。

「検知可能」は、当ログ分析で検知できる攻撃手段を示す。

「検知不可能」は、当ログ分析で検知できない攻撃手段を示す。

「誤検知」は、当ログ分析で誤って検知する処理や通信を示す。

10

【0039】

具体例として、図8の検知対策手段情報12の1行目を用いて説明する。

「CM_ID」がCM_ID_11のログ分析である。

「ログ種類」はプロキシログであり、「ログ種類」を示す名称“プロキシログ”と、この「製品カテゴリ」を示すキーワードとして、[PROXY]が設定される。

当ログ分析は、1つのWebサイトと1つの端末が、単位時間あたりに通信する回数が閾値以上である場合にあって定期的(Periodic)に通信している場合に攻撃(不審な通信)として検知する。

「検知可能」は、“定期的なC&C通信”であり、1つのWebサイト(C&Cサーバ)と1つの端末が、単位時間あたりに通信する回数が閾値以上である場合、C&Cサーバと通信していると検知する。“定期的なC&C通信”を示すキーワードとして[HTTP, Periodic]が設定される。

20

「検知不可能」は、“不定期なC&C通信”である。具体例として、1つのWebサイト(C&Cサーバ)と1つの端末がランダムな間隔で通信した場合、1つのWebサイトと1つの端末が、単位時間あたりに通信する回数が閾値以上にならないことがあり、この場合は検知できない。“不定期なC&C通信”を示すキーワードとして[HTTP, unperiodic]が設定される。

「誤検知」は、“正規のHTTP通信”である。1つの正規Webサイトと1つの端末が、単位時間あたりに通信する回数が閾値以上であった場合に誤検知する。“正規のHTTP通信”を示すキーワードとして[HTTP, unintentional, periodic]が設定される。

30

なお、2行目のCM_ID_12はOSなどの監査ログで認証エラーなどのイベントが記録されるものであり、3行目のCM_ID_13はFW(Fire・Wall)で、ポリシー違反の通信などが記録される例である。

以上のように、図8の検知対策手段情報12では、分析するログと分析内容ごとに、検知可能、検知不可能、誤検知可能性の情報を格納する。

【0040】

上記のようなキーワードは、予め、攻撃情報11、攻撃事例情報13において共通に現れる文言を使用する。攻撃情報11、攻撃事例情報13について、公開情報を利用する場合、これらの間で、攻撃手段を表現する文言や、検知手段(製品カテゴリ、ログ種類などの検知・対策)を示す文言は同じになる可能性が高いので、まず、これらに共通の文言を抽出する。次に、検知対策手段情報12を生成する際に、抽出した文言をキーワードとして設定することで、攻撃情報11、検知対策手段情報12、攻撃事例情報13において攻撃手段、検知手段(検知・対策)を表す文言を共有できる。

40

検知対策手段情報12は、製品カテゴリ、技術カテゴリから、上記のような手法を用いて、対策状況生成装置1の外で予め作成される。なお、検知対策手段情報12は、製品カテゴリ、技術カテゴリから、上記のような手法を用いて予め手動で作成されてもよい。

【0041】

図9は、本実施の形態に係るキーワード変換表の例を示す図である。

50

もし、攻撃情報 1 1、攻撃事例情報 1 3、検知対策手段情報 1 2において、攻撃手段を表現する文言、検知手段（製品カテゴリ、ログ種類などの検知・対策）を共通化できない場合は、これらの文言間でキーワード変換表を作成し、対策状況生成装置 1 に保存する。

図 9 のキーワード変換表の例では、No 1 の行において、検知対策手段情報 1 2 における“Virus”というキーワードは、攻撃情報 1 1 における「説明文」内の該当する文言である“Malware”と同一とみなす。攻撃情報 1 1 は複数の攻撃情報 1 1 を含むが、これらの「説明文」においては一般的に用語が統一されているため、この様な 1 つの変換を定義すればよい。同様に No 2 において、検知対策手段情報 1 2 における“Web”は、攻撃事例情報 1 3 における「説明文」では“URL”、又は、“Website”と変換される。No 3 では、“Malicious”は“Suspicious”に変換される。No 4 では、“HTTP”は同一の“HTTP”に変換される。No 5 では、攻撃情報 1 1 における「説明文」内の該当する文言には存在する“HTTPS”は、検知対策手段情報 1 2 では該当するキーワードは無いため斜線で表している。

【0042】

同じようなキーワード変換表を、攻撃情報 1 1 と攻撃事例情報 1 3 間、検知対策手段情報 1 2 と攻撃事例情報 1 3 間で作成しても良い。

この様なキーワード変換表の作成は、対策状況生成装置 1 の外で行う。

【0043】

次に、図 10 を用いて、本実施の形態に係る検知情報生成処理 S 1 2 0 の流れについて説明する。

まず、以下に、検知情報生成処理 S 1 2 0 の概要について説明する。

検知情報生成部 1 0 2 は、サイバー攻撃の攻撃手段 2 1 と、攻撃手段 2 1 を検知する検知手段 2 2 と、攻撃手段 2 1 に対する検知手段 2 2 の検知精度 2 3 とを含む攻撃検知情報 1 2 1 を生成する。検知情報生成部 1 0 2 は、攻撃手段 2 1 を説明する説明文を含む攻撃手段情報 1 1 1 と、検知手段 2 2 が検知する攻撃手段 2 1 を検知精度 2 3 に応じて取得するためのキーワードを含む検知対策手段情報 1 2 とを取得する。そして、検知情報生成部 1 0 2 は、キーワードを用いて攻撃手段情報 1 1 1 に含まれる説明文を検索し、検知手段 2 2 が検知する攻撃手段 2 1 を検知精度 2 3 に応じて検出する。そして、検知情報生成部 1 0 2 は、検知精度 2 3 に応じて検出した攻撃手段 2 1 の情報を用いて攻撃検知情報 1 2 1 を生成する。

【0044】

以下に、図 10 を用いて検知情報生成処理 S 1 2 0 について詳しく説明する。

検知情報生成部 1 0 2 は、入力された攻撃手段情報 1 1 1 の 1 つの行を抽出する。抽出した行に対応する攻撃手段 ID を攻撃手段 ID_j で示す。ここで、j は 1 から攻撃手段 ID の数（すなわち攻撃手段情報 1 1 1 の行の数）までの自然数をとる。検知対策手段情報 1 2 は、CM_{ID_i} で構成されたとする。ここで、i は 1 から検知対策手段情報 1 2 の行の数までの自然数をとる。ここで、検知対策手段情報 1 2 の行の数を n とする。

【0045】

ステップ S 1 2 1 において、検知情報生成部 1 0 2 は、変数に、初期値を設定する。検知情報生成部 1 0 2 は、 $i = 1$ 、 $detect_flag = False$ 、 $undetected_flag = False$ 、 $falsedetected_flag = False$ を設定する。

ステップ S 1 2 2 において、検知情報生成部 1 0 2 は、攻撃手段 ID_j に該当する、攻撃手段情報 1 1 1 のエントリにおける「説明文」を抽出する。具体例として、「説明文」が「A malware maliciously accesses data files on an infected computer, then leaks them to a C&C server by HTTP. URLs of the C&C server could be suspicious.」という記述であったとする。

ステップ S 1 2 3 において、検知情報生成部 1 0 2 は、 $i > n$ か否かを判定する。「は

い」の場合、処理を終了する。「いいえ」の場合、ステップS 1 2 4に進む。

ステップS 1 2 4において、検知情報生成部1 0 2は、検知対策手段情報1 2から、CM__ID__iのエントリを取り出す。

【0046】

ステップS 1 2 5において、検知情報生成部1 0 2は、CM__ID__iのエントリにおける「検知可能」のキーワードが、攻撃手段ID__jに該当する「説明文」に含まれるか検索する。「説明文」＝「A malware maliciously accesses data files on an infected computer, then leaks them to a C&C server by HTTP. URLs of the C&C server could be suspicious.」である。図7のCM__ID__1が現在参照しているCM__ID__i (i=1)であったとすると、「検知可能」のキーワードは、“URL”、“suspicious”、“HTTP”であり、これらは、「説明文」に含まれる。

また、検知対策手段情報1 2のキーワードと、攻撃情報1 1の「説明文」における文言を共通にできない場合は、キーワード変換表を用いる。この場合、CM__ID__iのエントリにおける「検知可能」のキーワードについて、キーワード変換表を用いて文言を変換して、変換した文言が、「説明文」に含まれるか検索する。

また、キーワード変換表を用いない場合は、「検知可能」のキーワードと「説明文」に含まれる文言間の類似度を、既存の技術を使用して調べ、類似している場合に、「検知可能」のキーワードが含まれると判定することで、「検知可能」のキーワードが含まれるかの検索処理としても良い。ここで、文言間の類似度を調べる既存の技術とは、文字列の類似度、長さなどから同じ意味を持つキーワードを特定してマッピングする技術である。具体例としては、レーベンシュタイン距離を利用する技術がある。

【0047】

ステップS 1 2 6において、検知情報生成部1 0 2は、ステップS 1 2 5における検索結果が、「含まれる」の場合は、ステップS 1 2 7に進み、「含まれる」でない場合は、ステップS 1 2 8に進む。

ステップS 1 2 7において、検知情報生成部1 0 2は、攻撃手段ID__jで識別される攻撃手段について、CM__ID__iで検知可能と判定し、detect__flag=Trueに設定する。

【0048】

ステップS 1 2 8において、検知情報生成部1 0 2は、CM__ID__iのエントリにおける「検知不可能」を参照する。

ステップS 1 2 9において、検知情報生成部1 0 2は、「検知不可能」が空の場合、ステップS 1 2 11に進む。ステップS 1 2 9において、検知情報生成部1 0 2は、「検知不可能」が空ではない場合、「検知不可能」となることがあるので、ステップS 1 2 10において、undetected__flag=Trueに設定する。

なお、図7において、「検知不可能」にもキーワードが設定されているが、本実施の形態では、このキーワードが「説明文」に有るかを調べずに、フラグをTrueに設定している。これは、「検知不可能」がある、と製品カテゴリやログ分析の機能の制限が図7で示されているためである。一方、ステップS 1 2 5における「検知可能」については、攻撃手段に対し、検知対策手段情報1 2に列挙された検知対策の手段が該当するかは必ず調べなくてはならないため、キーワードによる検索は必須となる。つまり、「検知可能」のキーワードが「説明文」に含まれるかを調べて、検知対策の手段が攻撃手段への検知・対策として該当するか判断する。その後、場合によって検知不可能であったり（誤検知であったり）の制限があるかを調べる。

【0049】

ステップS 1 2 11において、検知情報生成部1 0 2は、CM__ID__iのエントリにおける「誤検知」を参照する。

ステップS 1 2 12において、検知情報生成部1 0 2は、「誤検知」が空の場合、ステ

ップ S 1 2 1 4 に進む。ステップ S 1 2 1 2 において、検知情報生成部 1 0 2 は、「誤検知」が空ではない場合、「誤検知」となることがあるので、ステップ S 1 2 1 3 において、検知情報生成部 1 0 2 は、`false detect _ flag = True` に設定する。

なお、図 7 において、「誤検知」にもキーワードが設定されているが、本実施の形態では、このキーワードが「説明文」に有るかを調べずに、フラグを `True` に設定している。これは、「誤検知」がある、と製品カテゴリやログ分析の機能の制限が図 7 で示されているためである。

【0050】

図 1 1 は、本実施の形態に係る検知情報生成処理 S 1 2 0 で用いる判定表 1 2 0 1 を示す図である。

ステップ S 1 2 1 4 において、検知情報生成部 1 0 2 は、図 1 1 の判定表 1 2 0 1 を参照し、`detect _ flag`、`undetected _ flag`、`false detect _ flag` の値から、`CM _ ID _ i` で識別される検知・対策の効果において、○、△、□、◇、×を判定する。これらの記号は以下の意味である。

○：検知可能

×：検知不可能

△：誤検知の可能性あり

□：検知漏れの可能性あり

◇：検知可能・検知不可能・誤検知あり

検知漏れについては、`CM _ ID _ i` で識別される検知・対策を用いた場合、この攻撃手段を検知可能であるが、その検知・対策の方法の機能や性能の制限により検知・対策を回避されてしまい、検知漏れが生じる可能性があることを示す。

【0051】

ステップ S 1 2 1 5 において、検知情報生成部 1 0 2 は、攻撃手段 `ID _ j` に対して、`CM _ ID _ i` による対策の可否について、ステップ S 1 2 1 4 で取得した判定結果を割り当てる。この結果、図 6 における、攻撃検知情報 1 2 1 における、1 つの攻撃手段 `ID` に対する 1 つの検知・対策手段情報について、対応の可否が割り当てられる。具体的には、攻撃手段 `ID _ j` が `Add _ 0001`、`CM _ ID _ i` が製品カテゴリ = `IDS` であれば、攻撃手段 `ID` が `Add _ 0001` の行における、列が `IDS` の検知手段情報 1 6 2 のマスにおいて、ステップ S 1 2 1 4 の判定結果が割り当てられる。図 6 においては×が割り当てられている。

ステップ S 1 2 1 6 において、検知情報生成部 1 0 2 は、`i` をインクリメントし、S 1 2 3 に戻る。

【0052】

検知対策手段情報 1 2 が、図 8 のようなログ分析であった場合も、図 1 0 と同じ処理を行うことで、図 6 の検知手段情報 1 6 2 のログ分析の列の様に検知・対策の効果について、○、△、□、◇、×の判定結果を設定できる。

【0053】

図 4 に示す攻撃手段情報 1 1 1 について、全ての攻撃手段 `ID` ごとに、図 7、図 8 に示すような 1 つ以上の検知対策手段情報 1 2 の対策の可否を、図 1 0 に従い判定することで図 6 の攻撃検知情報 1 2 1 の様な情報を作成できる。図 6 における攻撃検知情報 1 2 1 は、攻撃手段情報 1 1 1 に対し、図 1 0 による検知対策手段情報 1 2 の対策可否の判定を対応づけ表として表現したものである。すなわち、攻撃検知情報 1 2 1 は、サイバー攻撃の攻撃手段 2 1 と、攻撃手段を検知する検知手段 2 2 と、攻撃手段 2 1 に対する検知手段 2 2 の検知精度 2 3 とを含む情報である。攻撃検知情報 1 2 1 において、攻撃手段情報 1 1 1 は攻撃手段情報 1 6 1 として、検知対策手段情報 1 2 は検知手段情報 1 6 2 として表現される。

また、図 6 には図示していないが、攻撃検知情報 1 2 1 における検知手段情報 1 6 2 の要素（`IDS` や `FW` など）には、該当する `CM _ ID _ i` が紐づけられている。

【0054】

<危険度判定処理 S 1 3 0>

図 1 2 を用いて、本実施の形態に係る危険度判定処理 S 1 3 0 の入出力の構成について説明する。

危険度判定部 1 0 3 は、攻撃検知情報 1 2 1 と、攻撃事例情報 1 3 と、重みづけ情報 1 4 とを入力とし、攻撃検知危険度情報 1 3 1 を出力する。危険度判定部 1 0 3 は、検知手段 2 2 の検知精度 2 3 に基づいて、攻撃手段 2 1 の危険度 1 6 3 を判定する。また、危険度判定部 1 0 3 は、検知手段 2 2 の検知精度 2 3 と、攻撃手段 2 1 が実施されるサイバー攻撃における攻撃フェーズとに基づいて、危険度 1 6 3 を判定する。

図 1 2 において、攻撃事例情報 1 3 は、サイバー攻撃の事例を表現したデータであり、どの様な攻撃手段がどの様な順番で、すなわち、どの攻撃フェーズで活動したかを示した情報である。

10

【0055】

図 1 3 は、本実施の形態に係る攻撃事例情報 1 3 の一例を示す図である。

サイバー攻撃は複数の攻撃フェーズで行われるが、一般的には、攻撃相手を調査してメールアドレスを入手するなどの“事前調査”フェーズ、マルウェアを添付したメールなどで侵入する“侵入”フェーズ、攻撃者がマルウェアと通信しながら攻撃を送受信して活動を行う“バックドア通信”フェーズ、侵入した組織内にどの様なサーバが存在するかを調べる“内部偵察”フェーズ、情報漏えいを行う“情報漏えい”フェーズで構成される。この様な複数の攻撃フェーズ 3 1 で構成された一連の流れをキルチェーンという。また、各々の攻撃フェーズを実現するために、各攻撃フェーズにおいて 1 つ以上の攻撃手段を用いて攻撃が行われる。攻撃事例情報 1 3 は、エントリを識別する No と、キルチェーンにおける攻撃フェーズと、各攻撃フェーズで実施される攻撃手段の攻撃手段 ID 及び攻撃名称で構成される。

20

【0056】

具体的には、図 1 3 において、“事前調査”フェーズでは、攻撃手段 ID = 4 0 5 ・ 攻撃名称 = S o c i a l I n f o r m a t i o n G a t h e r i n g v i a R e s e a r c h で識別される攻撃が行われる。“侵入”フェーズでは、攻撃手段 ID = 1 6 3 ・ 攻撃名称 = S p e a r P h i s h i n g、攻撃手段 ID = 5 4 2 ・ 攻撃名称 = T a r g e t e d M a l w a r e で攻撃される。この場合、S p e a r P h i s i n g は狙った相手に絞ったメール送付などの詐欺行為を意味し、T a r g e t e d M a l w a r e は標的に特化したマルウェアを用いることを意味する。つまり、標的に特化したマルウェアを、標的のみに添付メール（詐欺メール）で送付したり、Web アクセス（詐欺で誘導）により標的のみにダウンロードさせることを意味する。

30

図 1 3 における以降の攻撃フェーズについては、同様の情報構成なので説明を省略する。

【0057】

図 1 2 において、重みづけ情報 1 4 は、危険度判定を行うための情報である。

図 1 4 は、本実施の形態に係る重みづけ情報 1 4 の一例を示す図である。

上述したように、危険度判定部 1 0 3 は、検知手段 2 2 の検知精度 2 3 と、攻撃手段 2 1 が実施されるサイバー攻撃における攻撃フェーズとに基づいて、危険度 1 6 3 を判定する。本実施の形態における重みづけ情報 1 4 は、攻撃手段 2 1 がどの攻撃フェーズで使用されるかにより、重みを定義したものである。図 1 4 は、事前調査に用いられる攻撃手段の場合、事前調査自体は未だ攻撃が始まっていないため、重みは 5 と低い、情報漏えいは最も被害が大きくなるため 1 0 0 と高くなっており、攻撃フェーズが進むにつれて重みが大きくなる例である。図 1 4 における重みの値の設定は一例であり、侵入やバックドア通信などの攻撃フェーズの初期から中期について重みを大きくしてもよい。各々のエントリには通し番号が No として付与される。

40

【0058】

次に、図 1 5 を用いて、本実施の形態に係る危険度判定処理 S 1 3 0 の流れについて説明する。

50

ステップ S 1 3 1 において、危険度判定部 1 0 3 は、攻撃検知情報 1 2 1 の攻撃手段情報 1 6 1 における攻撃手段 I D を 1 つ選択し攻撃手段 I D $_i$ とする。ここで、 i は 1 から攻撃手段情報 1 6 1 における攻撃手段 I D の数までの自然数をとる。

ステップ S 1 3 2 において、危険度判定部 1 0 3 は、攻撃事例情報 1 3 における N o を j として参照するため、 $j = 1$ とする。ここで、 j は 1 から n までの自然数をとる。 n は、攻撃事例情報 1 3 における N o の最大値とする。

【0059】

ステップ S 1 3 3 において、危険度判定部 1 0 3 は、 $j > n$ か調べる。 $j > n$ であれば、処理を終わる。 $j > n$ でなければ、ステップ S 1 3 4 に進む。

ステップ S 1 3 4 において、危険度判定部 1 0 3 は、攻撃事例情報 1 3 から N o = j に該当するエントリを取り出す。

ステップ S 1 3 5 において、危険度判定部 1 0 3 は、攻撃事例情報 1 3 の N o = j のエントリにおける攻撃手段 I D、すなわち攻撃手段 I D $_j$ を取り出す。

ステップ S 1 3 6 において、危険度判定部 1 0 3 は、攻撃手段 I D $_i$ と攻撃手段 I D $_j$ とが同じか調べる。同じであれば、ステップ S 1 3 7 に進み、同じでなければ、ステップ S 1 3 1 3 に進む。

【0060】

ステップ S 1 3 7 において、危険度判定部 1 0 3 は、重みづけ情報 1 4 における N o を k として参照するため $k = 1$ とする。ここで、 k は 1 から m までの自然数をとる。 m は、重みづけ情報 1 4 における N o の最大値とする。

ステップ S 1 3 8 において、危険度判定部 1 0 3 は、 $k > m$ か調べる。 $k > m$ であれば、ステップ S 1 3 1 3 に進み、 $k > m$ でなければ、ステップ S 1 3 9 に進む。

ステップ S 1 3 9 において、危険度判定部 1 0 3 は、攻撃事例情報 1 3 の N o = j のエントリにおける「攻撃フェーズ」が、重みづけ情報 1 4 の N o = k のエントリにおける「攻撃手段が用いられるキルチェーンの攻撃フェーズ」と同じかを調べる。ステップ S 1 3 1 0 において、危険度判定部 1 0 3 は、同じであれば S 1 3 1 1 に進み、同じでなければ S 1 3 1 4 に進む。

【0061】

ステップ S 1 3 1 1 において、危険度判定部 1 0 3 は、重みづけ情報 1 4 の N o = k のエントリにおける「重み」を取得する。

ステップ S 1 3 1 2 において、危険度判定部 1 0 3 は、攻撃手段 I D $_i$ の危険度を、取得した「重み」に設定し、ステップ S 1 3 1 3 に進む。

ステップ S 1 3 1 3 において、危険度判定部 1 0 3 は、 j をインクリメントし、ステップ S 1 3 3 へ進む。

ステップ S 1 3 1 4 において、危険度判定部 1 0 3 は、 k をインクリメントし、ステップ S 1 3 8 へ進む。

【0062】

以上のように、ステップ S 1 3 1 2 において、攻撃手段 I D $_i$ に危険度 1 6 3 が付与される。攻撃手段情報 1 6 1 の攻撃手段 I D 全てについて、図 1 5 の危険度判定処理 S 1 3 0 を行うことで、攻撃手段情報 1 6 1 に危険度 1 6 3 を付与する。この結果、図 1 2 に示す攻撃検知危険度情報 1 3 1 が生成される。

【0063】

< 攻撃対策状況判定処理 S 1 4 0 >

図 1 6 を用いて、本実施の形態に係る攻撃対策状況判定処理 S 1 4 0 の入出力の構成について説明する。

図 1 6 に示すように、対策状況判定部 1 0 4 は、危険度判定部 1 0 3 により生成された攻撃検知危険度情報 1 3 1 と組織対策情報 1 5 とを入力とし、攻撃手段に対する組織の対策の効果度を含む対策状況情報 1 6 を出力する。

【0064】

図 1 7 は、本実施の形態に係る組織対策情報 1 5 の一例を示す図である。

組織対策情報15では、各エントリ（各行）を識別するIDとしてCMA__IDが付与され、各エントリにおける検知手段のIDに該当する情報を「対応するCM__ID」とする。さらに、各エントリに対して「運用上の制限」の情報が付与される。「運用上の制限」は、「閾値抑制（回数）」と、「閾値抑制（重大度）」と、「ホワイトリスト」とにより構成される。「閾値抑制（回数）」は、同じ検知が閾値回数以上発生した場合に検知として通報する運用を示す。「閾値抑制（重大度）」は、一定の重大度以上の検知のみを通報する運用を示す。「ホワイトリスト」は、検知が発生してもホワイトリストに記載されたプログラムの処理であれば通報しない運用を示す。或いは、「ホワイトリスト」は、ホワイトリストに記載された端末からの通信は検知しても通報しないなどの運用でもよい。組織対策情報15において、組織において対応する運用を適用している場合は「適用」、組織において対応する運用を適用していない場合は「未適用」が設定される。

10

【0065】

次に、図18を用いて、本実施の形態に係る攻撃対策状況判定処理S140の流れについて説明する。攻撃検知危険度情報131を、表で表現された情報として処理を説明する。

【0066】

ステップS141において、対策状況判定部104は、攻撃検知危険度情報131において、検知手段情報162と同様の表を危険度163の列の隣に追加する。対策状況判定部104は、追加した表において、検知手段22以外の内容、すなわち検知精度23の欄をクリアにすると共に、検知精度23の情報はメモリに一時記憶しておく。ここで、メモリに記憶する検知精度23の情報には、攻撃手段21と検知手段22とが紐付けられているものとする。この追加した表を組織対策状況情報164とする。図16に示すように、組織対策状況情報164は、検知手段情報162の表と同様に、IDS、FW、メールフィルタ、・・・、振る舞い検知（端末）、振る舞い検知（AP）、各種ログ分析などの検知手段22から構成される。

20

ステップS142において、対策状況判定部104は、攻撃検知危険度情報131のエントリ、すなわち行を1つ選択し、該当する攻撃手段情報161の攻撃手段ID__iと、組織対策状況情報164__iを取得する。ここで、iは1から攻撃手段情報161の攻撃手段IDの数までの自然数をとる。

ステップS143において、対策状況判定部104は、組織対策情報15におけるCMA__IDを1つ選択し、CMA__ID__jとする。また、CMA__ID__jに「対応するCM__ID」を、CM__ID__jとする。ここで、jは、1からpまでの自然数をとる。pは、組織対策情報15におけるCMA__IDの数、すなわち組織対策情報15のエントリ数である。

30

ステップS144において、対策状況判定部104は、 $j > p$ か確認し、 $j > p$ である場合、処理を終了する。また、 $j > p$ でない場合、S145に進む。

【0067】

ステップS145において、対策状況判定部104は、 $k = 1$ とする。

ステップS146において、対策状況判定部104は、組織対策状況情報164__iを構成する要素に紐づけられたCM__IDを、CM__ID__i__kとする。組織対策状況情報164はステップS141において、検知手段情報162のコピーとして生成されており、検知手段情報162に紐づいているCM__IDも同様にコピーされている。具体的には、組織対策状況情報164__iは、図16においてはIDS（ $k = 1$ ）やFW（ $k = 2$ ）などの要素で構成されており、各々に識別子であるCM__IDが付与されている。なお、iが変化しても、kが同じであれば同じCM__IDである。つまり、組織対策状況情報164の1つの列（kで参照）を見た場合、攻撃手段ID（iで参照）が何であっても、同じCM__IDである。具体的には、図16の組織対策状況情報164の $k = 1$ はIDSであり、攻撃手段IDが何であっても、列として見るのでIDSのCM__IDが参照される。また、上述したように、組織対策状況情報164では、検知手段情報162の攻撃手段IDごとの○△□◇×の判定、すなわち検知精度23は、メモリに記憶されている。し

40

50

たがって、検知手段情報 162 の攻撃手段 ID ごとの○△□◇×の判定は、メモリに記憶されている情報から取得するものとする。

【0068】

ステップ S147 において、対策状況判定部 104 は、組織対策状況情報 164 __ i の構成要素数 (IDS や FW などの要素数) を q とし、 $k > q$ か確認する。 $k > q$ である場合、対策状況判定部 104 は、ステップ S1411 へ進む。 $k > q$ でない場合、対策状況判定部 104 は、ステップ S148 へ進む。

ステップ S148 において、対策状況判定部 104 は、CM __ ID __ i __ k は CM __ ID __ j と同じかを調べる。同じ場合、対策状況判定部 104 は、ステップ S149 に進み、CM __ ID __ i __ k に該当する組織対策状況情報 164 __ i のマスに値を設定する。同じでない場合、対策状況判定部 104 は、ステップ S1410 に進む。

10

【0069】

ステップ S149 において、対策状況判定部 104 は、CM __ ID __ i __ k に該当する検知手段情報 162 の要素が、○△□◇であれば CM __ ID __ i __ k に該当する組織対策状況情報 164 __ i の欄に「済」を設定する。×の場合は「- (ハイフン)」を設定する。具体的には、攻撃手段 ID = 542 の行において、組織対策状況情報 164 の IDS は「済」である。これは、該当する検知手段情報 162 の IDS が □ だからである。同様に、同行の組織対策状況情報 164 の FW は、「-」であるが、これは、該当する検知手段情報 162 の FW が × だからである。

ステップ S1410 において、対策状況判定部 104 は、k をインクリメントして S147 へ進む。

20

【0070】

ステップ S1411 において、対策状況判定部 104 は、組織対策状況情報 164 __ i において、「済」か「-」に設定されていないマスを「未」に設定する。これは、検知対策手段情報 12 においては、○△□◇の何れかであるが、組織において実施されていない検知手段 22 であることを示す。対策状況判定部 104 は、j をインクリメントしてステップ S144 に進む。

【0071】

以上のように、対策状況判定部 104 は、攻撃手段 ID __ i の全てについて図 18 の処理を実行することで、図 16 の組織対策状況情報 164 に示すように、組織における対策について「済」「未」「-」を設定する。この結果、各攻撃手段 ID に対する組織の対策状況がどのような状態であるかを図 16 に示す対策状況情報 16 の様に示すことができる。

30

【0072】

対策状況判定部 104 は、図 16 に示す対策状況情報 16 の組織対策状況情報 164 の設定が完了すると、対策状況情報 16 の判定情報 165 に判定結果を設定する。判定情報 165 は、効果度 1651 と優先的対策項目 1652 とから構成される。

以上のように、対策状況判定部 104 は、攻撃検知情報 121 と、サイバー攻撃の対象となる組織においてサイバー攻撃に対する対策として実施されている検知手段 22 を組織検知手段として含む組織対策情報 15 とを取得し、攻撃検知情報 121 に含まれる検知精度 23 と組織対策情報 15 とに基づいて、組織における対策の効果の程度を表す効果度 1651 を判定する。また、対策状況判定部 104 は、検知手段 22 の検知精度 23 と、検知手段 22 が組織において実施されているか否かを示す情報 (組織対策状況情報 164) とに基づいて、効果度 1651 を判定する。

40

【0073】

以下に、対策状況判定部 104 による効果度 1651 を設定する処理について説明する。

対策状況判定部 104 は、図 16 の対策状況情報 16 における 1 つの攻撃手段 ID について、組織対策状況情報 164 が「済」である構成要素に該当する検知手段情報 162 の値を全て抽出する。対策状況判定部 104 は、抽出した値に基づいて以下 (a1) から (a5) のように「効果度 1651」を設定する。

50

(a 1) 抽出した値の中に○が含まれていれば効果度 1 6 5 1 に○を設定する。

(a 2) (a 1) に当てはまらない場合、抽出した値の中に△が含まれていれば△を効果度 1 6 5 1 に設定する。

(a 3) (a 2) に当てはまらない場合、抽出した値の中に□が含まれていれば□を効果度 1 6 5 1 に設定する。

(a 4) (a 3) に当てはまらない場合、抽出した値の中に◇が含まれていれば◇を効果度 1 6 5 1 に設定する。

(a 5) (a 4) に当てはまらない場合、×を効果度 1 6 5 1 に設定する。

図 1 6 の対策状況情報 1 6 では、組織対策状況情報 1 6 4 が「済」である構成要素が複数ある場合は、該当する検知手段情報 1 6 2 も複数になる。従って、複数の検知手段情報 1 6 2 において、全て○であったり、○、△、□、◇が混在することがありうるが、上記の処理 (a 1) から (a 5) に従えば、「効果度 1 6 5 1」は 1 つに決定される。

具体例として、図 1 6 の攻撃手段 ID = 5 4 2 においては、IDS、メールフィルタ、振る舞い検知 (端末) が「済」であり、上記の処理に従えば、振る舞い検知 (端末) が△なので、効果度 1 6 5 1 は△が設定される。

【0074】

次に、対策状況判定部 1 0 4 による「優先的対策項目 1 6 5 2」を設定する処理について説明する。

図 1 6 の対策状況情報 1 6 における 1 つの攻撃手段 ID について、「効果度 1 6 5 1」が○以外の項目を、「優先的対策項目 1 6 5 2」として判定し、「該当」を設定する。

【0075】

<対策状況出力処理 S 1 5 0>

対策状況出力処理 S 1 5 0 において、対策状況出力部 1 0 5 は、攻撃検知情報 1 2 1 (攻撃手段情報 1 6 1 及び検知手段情報 1 6 2) と効果度 1 6 5 1 とを含む対策状況情報 1 6 を出力する。対策状況情報 1 6 には、危険度 1 6 3 が含まれる。

対策状況出力部 1 0 5 は、出力インタフェース 9 4 0 を介して対策状況情報 1 6 を表示装置などに表示する。

【0076】

以上で、本実施の形態に係る攻撃対策判定処理 S 1 0 0 についての説明を終わる。

【0077】

他の構成

本実施の形態では、対策状況生成装置 1 は、入力インタフェース 9 3 0 を介して情報を取得し、出力インタフェース 9 4 0 を介して情報を出力する構成であった。しかし、対策状況生成装置 1 が通信装置を備え、通信装置を介して情報を受信してもよい。また、対策状況生成装置 1 は、通信装置を介して情報を送信してもよい。この場合、通信装置はレシーバとトランスミッタとを備える。具体的には、通信装置は通信チップまたは NIC (Network Interface Card) である。通信装置はデータを通信する通信部として機能する。レシーバはデータを受信する受信部として機能し、トランスミッタはデータを送信する送信部として機能する。

【0078】

本実施の形態では、対策状況出力部 1 0 5 は、図 1 6 に示す対策状況情報 1 6 を出力するものとしたが、その他の構成の対策状況情報 1 6 を出力してもよい。具体例を以下に示す。

第 1 に、対策状況出力部 1 0 5 は、攻撃手段 2 1 と効果度 1 6 3 とからなる対策状況情報 1 6 を出力する。すなわち、図 1 6 に示す攻撃手段情報 1 6 1 と効果度 1 6 5 1 とを対策状況情報 1 6 として出力してもよい。

第 2 に、対策状況出力部 1 0 5 は、攻撃手段 2 1 と効果度 1 6 3 とからなる対策状況情報 1 6 に、攻撃手段 2 1 を検知する検知手段 2 2 と、検知手段 2 2 の検知精度 2 3 とを含めて出力する。すなわち、図 1 6 に示す攻撃手段情報 1 6 1 と検知手段情報 1 6 2 と効果度 1 6 5 1 とを対策状況情報 1 6 として出力してもよい。

第3に、対策状況出力部105は、攻撃手段21と効果度163と検知手段22と検知精度23とからなる対策状況情報16に、組織対策状況情報164を含めて出力する。すなわち、図16に示す攻撃手段情報161と検知手段情報162と組織対策状況情報164と効果度1651とを対策状況情報16として出力してもよい。

【0079】

また、本実施の形態では、対策状況生成装置1の「部」の機能がソフトウェアで実現されるが、変形例として、対策状況生成装置1の「部」の機能がハードウェアで実現されてもよい。

図19を用いて、本実施の形態の変形例に係る対策状況生成装置1の構成について説明する。

図19に示すように、変形例の対策状況生成装置1では、図2のプロセッサ910及び記憶装置920に替えて、処理回路909を備える。

【0080】

処理回路909は、前述した「部」の機能及び記憶部150を実現する専用の電子回路である。処理回路909は、具体的には、単回路、複合回路、プログラム化したプロセッサ、並列プログラム化したプロセッサ、ロジックIC、GA (Gate・Array)、ASIC (Application・Specific・Integrated・Circuit)、又は、FPGA (Field・Programmable・Gate・Array) である。

【0081】

「部」の機能は、1つの処理回路909で実現されてもよいし、複数の処理回路909に分散して実現されてもよい。

【0082】

別の変形例として、対策状況生成装置1の機能がソフトウェアとハードウェアとの組合せで実現されてもよい。すなわち、対策状況生成装置1の一部の機能が専用のハードウェアで実現され、残りの機能がソフトウェアで実現されてもよい。

【0083】

プロセッサ910、記憶装置920、及び、処理回路909を、総称して「プロセッシングサーキットリ」という。つまり、対策状況生成装置1の構成が図2及び図19のいずれに示した構成であっても、「部」の機能及び記憶部150は、プロセッシングサーキットリにより実現される。

【0084】

「部」を「工程」又は「手順」又は「処理」に読み替えてもよい。また、「部」の機能をファームウェアで実現してもよい。

【0085】

本実施の形態の効果の説明

以上の様にして、対策状況生成装置1の対策状況判定部104は、図16に示す対策状況情報16を生成し、表示装置に表示する。

本実施の形態における対策状況生成装置1は、攻撃情報に対して、検知・対策情報のマッピングを示し、さらに、攻撃事例情報から危険度を付与し、さらに、組織の攻撃対策実施の状況から攻撃情報への対策状況を図示できる効果がある。さらに、検知・対策手段情報から効果度1651を判定するとともに、優先的対策項目1652を図示できる効果がある。

本実施の形態における対策状況生成装置1の利用者は、自組織のセキュリティ対策が、様々な攻撃情報（手段）に対して有効であるか無効であるか効果度1651で確認でき、さらに、対策を強化すべき攻撃手段について優先的対策項目1652を確認できる。

【0086】

実施の形態2.

本実施の形態では、主に、実施の形態1に追加する部分あるいは実施の形態1と異なる部分について説明する。本実施の形態において、実施の形態1と同様の構成には同一の符

10

20

30

40

50

号を付し、その説明を省略する。また、実施の形態 1 と同様の機能についてもその説明を省略する。

本実施の形態では、図 1 に示す攻撃事例判定装置 2 が、個別の攻撃事例情報 1 3 a を用いて、組織の対策状況の判定を行う処理について説明する。

【0087】

構成の説明

図 20 を用いて、本実施の形態に係る攻撃事例判定装置 2 の構成及び入出力について説明する。

攻撃事例判定装置 2 は、コンピュータであり、図示はないが実施の形態 1 の図 1 で説明した対策状況生成装置 1 と同様のハードウェアを備える。また、攻撃事例判定装置 2 は、機能構成として攻撃事例判定部 201 を備える。すなわち、攻撃事例判定装置 2 の「部」の機能とは、攻撃事例判定部 201 の機能である。対策状況生成装置 1 と同様に、「部」の機能は、ソフトウェアで実現される。また、対策状況生成装置 1 と同様に、「部」の機能が処理回路 909 等のハードウェアで実現されていてもよい。

【0088】

攻撃事例判定装置 2 は、対策状況情報 1 6 と攻撃事例情報 1 3 a とを入力とし、攻撃事例対応情報 1 7 を出力する。

本実施の形態では、攻撃事例判定装置 2 は、対策状況情報 1 6 を用いて、攻撃事例情報 1 3 a への対策状況を攻撃事例対応情報 1 7 として出力する。本実施の形態では攻撃事例対応情報 17 を表で表現する。

【0089】

動作の説明

図 21 を用いて、本実施の形態に係る攻撃事例判定部 201 による攻撃事例判定処理 S200 について説明する。

攻撃事例判定処理 S200 において、攻撃事例判定部 201 は、対策状況情報 1 6 と、攻撃事例情報 1 3 a とを入力とし、図 21 に示す以下の処理を行う。攻撃事例情報 1 3 a は、図 13 の攻撃事例情報 13 の 1 つの例である。

攻撃事例判定部 201 は、サイバー攻撃の攻撃フェーズと攻撃フェーズにおいて実施される攻撃手段とを含む攻撃事例情報 1 3 a と、対策状況情報 1 6 とを取得し、対策状況情報 1 6 を用いて、攻撃事例情報 1 3 a について攻撃フェーズの攻撃手段ごとに組織の対策状況を判定する。また、攻撃事例判定部 201 は、攻撃事例情報 1 3 a と、判定した組織の対策状況を攻撃事例対応情報 1 7 として出力する。

【0090】

ステップ S211 において、攻撃事例判定部 201 は、攻撃事例情報 1 3 a における最初の攻撃手段 ID を参照する。この攻撃手段 ID は、攻撃事例情報 1 3 a において、一番初めの攻撃フェーズの先頭（一連の攻撃の最初の攻撃）を示すものである。

ステップ S212 において、攻撃事例判定部 201 は、攻撃事例情報 1 3 a の一連の攻撃における最後の攻撃手段 ID まで参照した場合は、S211 に進む。そうで無い場合は S213 に進む。

ステップ S213 において、攻撃事例判定部 201 は、攻撃事例情報 1 3 a における攻撃フェーズに含まれる攻撃手段 ID を抽出する。これを、参照攻撃手段 ID とする。

ステップ S214 において、攻撃事例判定部 201 は、参照攻撃手段 ID を、対策状況情報 1 6 から検索する。

ステップ S215 において、攻撃事例判定部 201 は、対策状況情報 1 6 における検索された攻撃手段 ID、すなわち参照攻撃手段 ID について、その行の情報を参照する。この行には、検知手段情報 162 の情報などが含まれる。

ステップ S216 において、攻撃事例判定部 201 は、対策状況情報 1 6 における、参照攻撃手段 ID に該当する検知手段情報 162 において、「×」が付いている構成要素（FW や IDS などの検知・対策）以外を選択し、名称を抽出する。つまり、攻撃事例判定部 201 は、何かしらの効果がある構成要素の名称を抽出する。

ステップ S 2 1 7 において、攻撃事例判定部 2 0 1 は、攻撃事例情報 1 3 a において、参照攻撃手段 I D に該当する行に「検知・対策の手段」（列）を追加し、ステップ S 2 1 6 で抽出した構成要素の名称を設定する。ステップ S 2 1 6 において複数抽出されている場合はそれらを全て設定する。

具体例を用いて説明する。図 2 0 に示すように、攻撃手段 I D = 1 6 3 であれば、メールフィルタが該当する。また、攻撃手段 I D = 5 4 2 であれば、I D S、メールフィルタ、振る舞い検知（端末）、振る舞い検知（A P）、ログ分析（端末）が該当する。検知手段情報 1 6 2 で「×」しかない場合は、「無」を設定する。

【0091】

ステップ S 2 1 8 において、攻撃事例判定部 2 0 1 は、対策状況情報 1 6 において、参照攻撃手段 I D の「効果度 1 6 5 1」を抽出する。

ステップ S 2 1 9 において、攻撃事例判定部 2 0 1 は、攻撃事例情報 1 3 a における参照攻撃手段 I D について「組織の対策状況」（列）を追加し、ステップ S 2 1 8 で抽出した「効果度 1 6 5 1」を設定する。具体例として、攻撃手段 I D = 5 4 2 であれば、図 1 6 及び図 2 0 に示すように△が該当する。上述したように、この「効果度 1 6 5 1」（□や△など）の意味は、図 1 1 の判定表 1 2 0 1 のとおりである。

ステップ S 2 1 1 0 において、攻撃事例判定部 2 0 1 は、攻撃事例情報 1 3 a における次の攻撃手段 I D を参照し、ステップ S 2 1 2 に戻る。

【0092】

ステップ S 2 1 1 1 において、攻撃事例判定部 2 0 1 は、攻撃事例情報 1 3 a について「総合判定」（列）を追加して、以下の様に値を設定する。

侵入など、初期の攻撃フェーズについて、組織の対策状況が○であれば、「優」とする

。

バックドア通信など、初期の次の攻撃フェーズについて組織の対策状況が○であれば、「良」とする。これは、侵入は許すが次の段階で検知できるためである。

さらに後続の攻撃フェーズについて組織の対策状況が○であれば、「可」とする。

初期や、初期の次の攻撃フェーズについて組織の対策状況が△であれば、「可」とする

。

これらに当てはまらなければ、「不可」とする。

なお、「総合判定」は、攻撃事例情報 1 3 a に付与するもので、攻撃手段 I D ごとに付与するものではない。

また、本実施の形態における総合判定の方法（優、良、可、不可の判定方法）は、上記に限らない。具体例として、初期と初期の次の攻撃フェーズの何れかに○が付かなければ全て不可、としても良いし、情報漏えいの攻撃フェーズに○が付いていれば、良、としても良い。

【0093】

以上で、本実施の形態に係る攻撃事例判定処理 S 2 0 0 についての説明を終わる。

この様に、攻撃事例判定部 2 0 1 は、攻撃事例情報 1 3 a に対して、対策状況情報 1 6 を用いて組織の対策状況を判定し、総合判定の情報を付与した攻撃事例対応情報 1 7 を出力する。

【0094】

本実施の形態の効果の説明

以上のように、本実施の形態に係る攻撃事例判定装置 2 によれば、攻撃事例対応情報 1 7 を参照することで、攻撃事例情報 1 3 a における攻撃手段 I D ごとの組織の対策状況を確認できる。具体例として、組織の対策状況が□や◇の攻撃手段 I D については、対策しているが検知漏れ（回避）が発生する場合があることを意味し、△や◇の攻撃手段 I D については、対策しているが誤検知が発生する場合があることを意味する。また、この攻撃事例情報に対する総合判定も確認できる。

また、本実施の形態に係る攻撃事例判定装置 2 によれば、攻撃事例情報 1 3 a に対して、対策状況情報 1 6 を用いて組織の対策状況を攻撃事例対応情報 1 7 として図示できる効

10

20

30

40

50

果がある。本実施の形態に係る攻撃事例判定装置 2 の利用者は、攻撃事例対応情報 1 7 の総合判定を確認することで、優・良であれば組織の対策はできていると判断し、可・不可であれば追加対策を検討する、といった判断が可能である。

【0095】

実施の形態 3.

本実施の形態では、主に、実施の形態 1 及び 2 に追加する部分あるいは実施の形態 1 及び 2 と異なる部分について説明する。本実施の形態において、実施の形態 1 及び 2 と同様の構成には同一の符号を付し、その説明を省略する。また、実施の形態 1 及び 2 と同様の機能についてその説明を省略する。

本実施の形態では、図 1 に示す対策候補抽出装置 3 が、追加対策を判定する処理について説明する。

【0096】

構成の説明

図 2 2 及び図 2 3 を用いて、本実施の形態に係る対策候補抽出装置 3 の構成及び入出力について説明する。

対策候補抽出装置 3 は、コンピュータであり、図示はないが実施の形態 1 の対策状況生成装置 1 及び実施の形態 2 の攻撃事例判定装置 2 と同様のハードウェアを備える。また、対策候補抽出装置 3 は、機能構成として対策候補抽出部 3 0 1 を備える。すなわち、対策候補抽出装置 3 の「部」の機能とは、対策候補抽出部 3 0 1 の機能である。対策状況生成装置 1 及び攻撃事例判定装置 2 と同様に、「部」の機能は、ソフトウェアで実現される。また、対策状況生成装置 1 及び攻撃事例判定装置 2 と同様に、「部」の機能が処理回路 9 0 9 等のハードウェアで実現されていてもよい。

【0097】

対策候補抽出部 3 0 1 は、組織の対策状況に基づいて選択された選択攻撃手段 1 7 1 と、選択攻撃手段 1 7 1 以外の攻撃手段と含む攻撃事例情報 1 3 3 を取得し、選択攻撃手段 1 7 1 と組み合わせて使用される攻撃手段を攻撃事例情報 1 3 3 から判定する。また、対策候補抽出部 3 0 1 は、選択攻撃手段 1 7 1 と組み合わせて使用される攻撃手段を強化対策情報 1 8 として出力する。このとき、攻撃事例情報 1 3 3 は、少なくとも選択攻撃手段 1 7 1 と、選択攻撃手段 1 7 1 以外の攻撃手段とを含む。また、攻撃事例情報 1 3 3 は 1 つでもよく、複数あってもよい。

【0098】

具体的には、対策候補抽出装置 3 は、1 つ又は複数の攻撃事例情報 1 3 3 と、攻撃事例対応情報 1 7 において組織の対策状況で△か◇がついた誤検知の多い攻撃手段 X（選択攻撃手段 1 7 1）とを入力とする。具体例としては、図 2 2 の（a）に示す攻撃手段 X である。攻撃手段 X は、攻撃事例対応情報 1 7 において組織の対策状況で誤検知の多いと判定された攻撃手段である。対策候補抽出装置 3 は、攻撃手段 X の誤検知を低減するために、併せて検知すべき攻撃手段 Y を抽出する。

なお、「誤検知の多い攻撃手段 X」とは、攻撃手段 X に対する組織の対策では、攻撃手段 X 以外を誤って攻撃手段 X として検知してしまうことが多い、という意味である。

【0099】

動作の説明

対策候補抽出装置 3 による対策候補抽出処理 S 3 0 0 を以下に説明する。

まず、対策候補抽出装置 3 は、攻撃手段 X の攻撃手段 ID __ X を抽出する。

次に、対策候補抽出装置 3 は、攻撃手段 ID __ X を含む攻撃事例情報 1 3 を、1 つ又は複数の攻撃事例情報 1 3 3 から抽出する。ここで、対策候補抽出装置 3 は、攻撃事例情報 1 3 を 1 つ以上抽出する。抽出結果を、攻撃事例情報 1 3 __ i とする。

【0100】

次に、対策候補抽出装置 3 は、攻撃事例情報 1 3 __ i において、攻撃手段 ID __ X 以外に、共通する攻撃手段 ID を抽出し、その数を数える。具体例として、攻撃事例情報 1 3 __ i が、以下であったとする。ここで、i = 1, 2, 3 とする。

攻撃事例情報 1 3 __ 1 = { 攻撃手段 I D __ X、攻撃手段 I D __ e、攻撃手段 I D __ f、
攻撃手段 I D __ g }

攻撃事例情報 1 3 __ 2 = { 攻撃手段 I D __ X、攻撃手段 I D __ e、攻撃手段 I D __ g、
攻撃手段 I D __ h }

攻撃事例情報 1 3 __ 3 = { 攻撃手段 I D __ X、攻撃手段 I D __ e、攻撃手段 I D __ i、
攻撃手段 I D __ j }

この時、攻撃手段 I D __ e は攻撃事例情報 1 3 __ 1、攻撃事例情報 1 3 __ 2、攻撃事例
情報 1 3 __ 3 の全てに含まれるため、出現数は 3 である。同様に、攻撃手段 I D __ g の出
現数は 2、攻撃手段 I D __ f、攻撃手段 I D __ h、攻撃手段 I D __ i、攻撃手段 I D __ j
の出現数は 1 である。

10

すなわち、攻撃手段 I D __ X が含まれる上記 3 つの攻撃事例情報 1 3 __ i では、攻撃手
段 I D __ X 以外に、攻撃手段 I D __ e が全てに含まれ、攻撃手段 I D __ g が 2 つに含まれ
ている。従って、これらの攻撃事例情報 1 3 においては、攻撃手段 I D __ X と攻撃手段 I
D __ e は常に併用されており、次に、攻撃手段 I D __ g が併用されていることが分かる。

対策候補抽出装置 3 は、この様に抽出した攻撃手段 I D __ e、攻撃手段 I D __ g を攻撃
手段 I D __ X と組み合わせて検知すべき攻撃手段 Y を強化対策情報 1 8 として出力する。

【 0 1 0 1 】

図 2 4 を用いて、本実施の形態に係る対策候補抽出処理 S 3 0 0 について説明する。

ステップ S 3 1 1 において、対策候補抽出部 3 0 1 は、攻撃事例情報 1 3 __ i から攻撃
手段 I D __ X を含むものを抽出する。ここで、i は 1 から r までの自然数とする。r は攻
撃事例情報 1 3 の数である。

20

ステップ S 3 1 2 において、対策候補抽出部 3 0 1 は、続く処理のために、抽出した攻
撃事例情報を、抽出攻撃事例情報 j とする。ここで、j は 1 から s までの自然数とする。
s は、ステップ S 3 1 1 において抽出された攻撃事例情報 1 3 の数である。

ステップ S 3 1 3 において、対策候補抽出部 3 0 1 は、変数 j を 1 に設定し、空の攻撃
手段 I D リストを用意する。

ステップ S 3 1 4 において、対策候補抽出部 3 0 1 は、j > s か調べ、j > s である場
合は処理を終了し、j > s でない場合はステップ S 3 1 5 へ進む。

【 0 1 0 2 】

ステップ S 3 1 5 において、対策候補抽出部 3 0 1 は、抽出攻撃事例情報 j に含まれる
攻撃手段 I D の数を t とする。

30

ステップ S 3 1 6 において、対策候補抽出部 3 0 1 は、変数 k を 1 に設定する。

ステップ S 3 1 7 において、対策候補抽出部 3 0 1 は、k > t か調べ、k > t である場
合はステップ S 3 1 1 3 へ進み、k > t でない場合はステップ S 3 1 8 へ進む。

【 0 1 0 3 】

ステップ S 3 1 8 において、対策候補抽出部 3 0 1 は、抽出攻撃事例情報 j に含まれる
攻撃手段 I D の 1 つである攻撃手段 I D __ k を取得する。

ステップ S 3 1 9 において、対策候補抽出部 3 0 1 は、攻撃手段 I D __ k が、攻撃手段
I D リストに存在するか調べ、存在すればステップ S 3 1 1 1 に進み、存在しなければ、
ステップ S 3 1 1 0 へ進む。

40

ステップ S 3 1 1 0 において、対策候補抽出部 3 0 1 は、攻撃手段 I D リストの末尾に
攻撃手段 I D __ k を追加し、その c o u n t を 1 に設定する。ここで、攻撃手段 I D リス
トは以下のような構造の情報である。

攻撃手段 I D リスト = { (攻撃手段 I D __ 1、c o u n t __ 1)、(攻撃手段 I D __ 2
、c o u n t __ 2)、… }

ここで、中カッコは情報の並びである。小カッコの中は攻撃手段 I D の値と、その攻撃
手段 I D が複数の攻撃事例情報に渡って出現した回数を表している。

【 0 1 0 4 】

ステップ S 3 1 1 1 において、対策候補抽出部 3 0 1 は、攻撃手段 I D リスト上の攻撃
手段 I D __ k の要素の c o u n t (c o u n t __ k) をインクリメントする。

50

ステップ S 3 1 1 2 において、対策候補抽出部 3 0 1 は、k をインクリメントする。

ステップ S 3 1 1 3 において、対策候補抽出部 3 0 1 は、j をインクリメントする。

【0105】

以上で、本実施の形態に係る対策候補抽出処理 S 3 0 0 についての説明を終わる。

【0106】

他の構成

また、図 2 2 の (b) に示すように、対策候補抽出装置 3 は、攻撃事例情報 1 3 3 と、攻撃事例対応情報 1 7 における組織の対策状況で□か◇のついた攻撃手段（攻撃手段 X 1）（選択攻撃手段 1 7 1）とを入力としてもよい。□か◇のついた攻撃手段（攻撃手段 X 1）とは、検知漏れ（回避）する可能性がある攻撃手段（攻撃手段 X 1）である。そして、対策候補抽出装置 3 は、攻撃手段 X 1 の検知漏れを低減するために、併せて検知すべき攻撃手段を抽出する。

ここで、対策候補抽出装置 3 の処理は、攻撃手段 X の場合（図 2 2 の (a)）と同じである。処理の結果、対策候補抽出装置 3 は、この様に抽出した攻撃手段 I D__e、攻撃手段 I D__g を攻撃手段 I D__X 1 と組み合わせて検知すべき攻撃手段攻 Y 1 として出力する。

【0107】

また、図 2 3 に示すように、対策候補抽出装置 3 は、攻撃事例情報 1 3 3 と、対策状況情報 1 6 における優先的対策項目 1 6 5 2 が「該当」である攻撃手段 U（選択攻撃手段 1 7 1）とを入力としてもよい。そして、対策候補抽出装置 3 は、攻撃手段 U と組み合わせて検知すべき攻撃手段を抽出し、攻撃手段 V として出力してもよい。この場合も対策候補抽出装置 3 の処理は攻撃手段 X の場合（図 2 2 の (a)）と同様の処理である。

【0108】

本実施の形態の効果の説明

本実施の形態に係る対策候補抽出装置 3 は、誤検知や検知漏れがある攻撃手段について、攻撃事例情報からの統計により、併用して使用される頻度の高い攻撃手段を抽出する。そして、抽出した攻撃手段を、誤検知や検知漏れがある攻撃手段と併せて検知を試みる候補となる攻撃手段として提示することができる。この結果、本実施の形態に係る対策候補抽出装置 3 によれば、提示された攻撃手段と、誤検知や検知漏れがある攻撃手段とを併せて検知することで、誤検知や検知漏れを低減することが可能となる効果がある。

【0109】

実施の形態 4.

本実施の形態では、主に、実施の形態 3 と異なる点について説明する。本実施の形態において、実施の形態 1 から 3 と同様の構成には同一の符号を付し、その説明を省略する。また、実施の形態 1 から 3 と同様の機能についてその説明を省略する。

本実施の形態では、実施の形態 3 で説明した対策候補抽出装置 3 による追加対策を提示する処理が実施の形態 3 と異なる。

【0110】

図 2 5 は、本実施の形態に係る対策候補抽出装置 3 の構成及び入出力を示す図である。

図 2 5 に示すように、対策候補抽出装置 3 は、1 つ又は複数の攻撃事例情報 1 3 3 と、攻撃事例対応情報 1 7 における組織の対策状況で△か◇のついた、誤検知の多い攻撃手段 X、又は、攻撃事例対応情報 1 7 における組織の対策状況で□か◇のついた、検知漏れする可能性がある攻撃手段 X 1、又は、対策状況情報 1 6 における優先的対策項目 1 6 5 2 が「該当」である攻撃手段 U を入力とする。さらに、対策状況情報 1 6 を入力する。

【0111】

誤検知の多い攻撃手段 X、又は、検知漏れする可能性がある攻撃手段 X 1、又は、対策状況情報 1 6 における優先的対策項目 1 6 5 2 が「該当」である攻撃手段 U に対して、組み合わせて検知すべき攻撃手段を抽出する方法は、実施の形態 3 と同じである。

本実施の形態では、組み合わせて検知すべき攻撃手段のうち、対策状況情報 1 6 を利用して既に組織で対策しているものに絞り提示する。

具体例として、組み合わせて検知すべき攻撃手段が、図 16 の対策状況情報 16 における攻撃手段 ID = 542 であった場合、組織対策状況情報 164 において「済」になっている IDS / メールフィルタ / 振る舞い検知 (端末) を抽出し、この攻撃手段 ID = 542 の情報に加えて攻撃手段 W を強化対策情報 18 として出力する。

もし、組み合わせて検知すべき攻撃手段について、対策状況情報 16 において、組織対策状況情報 164 に「済」が付くものが無い場合は、該当する攻撃手段 W は無い。よって、攻撃手段 W を出力しない、あるいは、強化対策情報 18 がないとの警告を出力してもよい。

【0112】

*** 本実施の形態の効果の説明 ***

本実施の形態における対策候補抽出装置 3 は、実施の形態 3 の、入力された攻撃手段と組み合わせて検知すべき攻撃手段について、組織対策状況情報 164 を参照して既に組織で対策済みの攻撃手段に限定して提示することで、組織で既に適用している対策を利用し、検知を強化することが可能となる効果がある。

【0113】

実施の形態 5 .

本実施の形態では、主に、実施の形態 1 と異なる点について説明する。本実施の形態において、実施の形態 1 から 4 と同様の構成には同一の符号を付し、その説明を省略する。また、実施の形態 1 から 4 と同様の機能についてその説明を省略する。

【0114】

実施の形態 1 では、検知情報生成部 102 は、図 10 の S125 において、攻撃手段 ID _ j の「説明文」に、検知対策手段情報 12 の CM _ ID _ i のエントリにおける「検知可能」のキーワードが含まれるかを調べることで、CM _ ID _ i の「検知可能」な攻撃を攻撃手段 ID _ j を紐づけていた。

本実施の形態では、検知対策手段情報 12 の CM _ ID _ i のエントリにおける「検知可能」において、キーワードの代わりに「検知可能」な攻撃手段 ID が含まれているものについて説明する。「検知不可能」「誤検知」の項目についても同様である。すなわち、検知情報生成部 102 は、検知手段により検知される攻撃手段であって検知手段の検知精度に応じた攻撃手段を含む検知対策手段情報 12 を取得し、この検知対策手段情報 12 に基づいて、検知手段が検知する攻撃手段を検知精度に応じて検出する。

【0115】

上記の検知対策手段情報 12 を用いる場合、ステップ S125 の処理を、「CM _ ID _ i のエントリにおける「検知可能」の攻撃手段 ID が、攻撃手段 ID _ j に一致するかを確認する」と置き換えればよい。ステップ S126 は、この確認が、一致する場合にステップ S127 へ進み、一致しない場合はステップ S128 へ進むように変更すればよい。

本実施の形態においては、上記の検知対策手段情報 12 を生成する際に、キーワードの代わりに攻撃手段 ID を設定することを前提としている。なお、実施の形態 1 で説明したように、キーワードの代わりに攻撃手段 ID を含む検知対策手段情報 12 の生成は、対策状況生成装置 1 の外で行う。

【0116】

*** 本実施の形態の効果の説明 ***

本実施の形態における対策状況生成装置 1 は、実施の形態 1 に係る検知対策手段情報 12 の「検知可能」において、キーワードを用いる代わりに、攻撃手段 ID を用いることにより、実施の形態 1 と同じ効果が得られる。

【0117】

実施の形態 6 .

本実施の形態では、主に、実施の形態 1 と異なる点について説明する。本実施の形態において、実施の形態 1 から 5 と同様の構成には同一の符号を付し、その説明を省略する。また、実施の形態 1 から 5 と同様の機能についてその説明を省略する。

【0118】

実施の形態1では、危険度判定部103は、攻撃事例情報13と重みづけ情報14とを用いて危険度163を攻撃手段IDに付与していた。攻撃情報11には、図3で図示していないが、危険度レベル=1、2、3、4、5（大きいほど危険）などの、危険度の情報が含まれる場合がある。その場合、本実施の形態では、危険度判定部103は、攻撃事例情報13と重みづけ情報14とを用いずに、攻撃情報11において攻撃手段IDごとに付与されている危険度レベルを参照し、その危険度レベルの値を、対策状況情報16における攻撃手段IDの危険度163に設定する。すなわち、危険度判定部103は、攻撃手段の危険度（危険度レベル）を含む攻撃手段情報111を取得し、対策状況出力部105は、攻撃手段の危険度（危険度レベル）を含む対策状況情報16を出力する。

10

【0119】

本実施の形態の効果の説明

本実施の形態における対策状況生成装置1は、攻撃情報11に危険度（危険度レベル）の情報が含まれる場合、これを、対策状況情報16における、危険度163に設定できる効果がある。

【0120】

実施の形態7.

本実施の形態では、主に、実施の形態1と異なる点について説明する。本実施の形態において、実施の形態1から6と同様の構成には同一の符号を付し、その説明を省略する。また、実施の形態1から6と同様の機能についてその説明を省略する。

20

【0121】

実施の形態1では、対策状況生成装置1は、対策状況情報16において、対策済の組織対策状況情報164の要素において、「済」「未」「-」の3種類しか設定しなかった。本実施の形態では、検知対策手段情報12に記載されている「検知不可能」「誤検知」の情報を、対策状況情報16における組織対策状況情報164の情報として、追加設定する。

【0122】

本実施の形態では、検知情報生成部102は、図10のステップS1210において、`undetected_flag=True`の設定に加えて、参照しているCM_ID_iの「検知不可能」の情報を、攻撃手段ID_jに紐づける。さらに、ステップS1213において、参照しているCM_ID_iの「誤検知」の情報を、攻撃手段ID_jに紐づける。さらに、ステップS1215において、攻撃手段ID_jに対して、CM_ID_iによる対策可否を設定することに加えて、攻撃手段ID_jに紐づけたCM_ID_iの「検知不可能」「誤検知」の情報を、追加設定する。

30

【0123】

さらに、本実施の形態では、対策状況判定部104の処理を示した図18のステップS149において、CM_ID_i_kに該当する組織対策状況情報164_iの欄に「済」を設定する処理に加えて、CM_ID_i_kのIDに上記の様に紐づけて設定された「検知不可能」「誤検知」を設定する。具体例として、同欄に「済」を設定することに加えて、以下の様に紐づいた「検知不可能」「誤検知」を設定する。

40

対策状況情報16の攻撃手段ID=Add_0001における組織対策状況情報164のログ分析・プロキシログのマスの設定例を以下に示す。

- ・済
- ・検知不可能：改ざんされた正規サイトとのHTTP通信
- ・誤検知：正規のHTTP通信

【0124】

本実施の形態の効果の説明

本実施の形態における対策状況生成装置1は、対策状況情報16において、攻撃手段の対策状況を確認できるとともに、対策済みであった場合の、検知不可能（検知漏れ）や誤検知の発生の可能性について含めることができる。このため、対策状況生成装置1の利用

50

者は、ある攻撃手段が対策済みであっても、検知不可能（検知漏れ）や誤検知のリスクについて把握することが可能となる。

【0125】

実施の形態 8.

本実施の形態では、主に、実施の形態 3 及び 4 と異なる点について説明する。本実施の形態において、実施の形態 1 から 7 と同様の構成には同一の符号を付し、その説明を省略する。また、実施の形態 1 から 7 と同様の機能についてその説明を省略する。

【0126】

本実施の形態では、対策候補抽出装置 3 は、追加対策の提示の処理において、実施の形態 3 及び 4 と異なる処理を行う。実施の形態 3 では、対策候補抽出装置 3 は、攻撃事例情報 13 において、攻撃手段 X や攻撃手段 X 1 や攻撃手段 U と併用される攻撃手段の統計を取り、例えば、攻撃手段 X と最も多く併用される攻撃手段 Y を抽出し、強化対策情報 18 として出力した。

【0127】

本実施の形態では、さらに、攻撃手段 X や攻撃手段 X 1 と併用される攻撃手段の統計を取り、さらに、対策状況情報 16 を参照して、併用されることが多い攻撃手段について有効な検知手段情報 162 を併せて出力する。

実施の形態 3 で説明した以下の 3 つの攻撃事例情報を用いて説明する。ここでは攻撃手段 X について併せて検知する他の攻撃手段を抽出する場合を挙げる。

攻撃事例情報 13 __ 1 = { 攻撃手段 I D __ X、攻撃手段 I D __ e、攻撃手段 I D __ f、
攻撃手段 I D __ g }

攻撃事例情報 13 __ 2 = { 攻撃手段 I D __ X、攻撃手段 I D __ e、攻撃手段 I D __ g、
攻撃手段 I D __ h }

攻撃事例情報 13 __ 3 = { 攻撃手段 I D __ X、攻撃手段 I D __ e、攻撃手段 I D __ i、
攻撃手段 I D __ j }

これらの攻撃事例情報に対して図 18 の処理を実行すると、攻撃手段 I D リスト = { (攻撃手段 I D __ e、count __ e = 3)、(攻撃手段 I D __ g、count __ g = 2) } となる。

【0128】

この結果、攻撃手段 I D __ e、又は攻撃手段 I D __ e と攻撃手段 I D __ g との両方を攻撃手段 Y として出力する。本実施の形態では、この出力において、以下の (b1) から (b3) の判定を行う。

(b1) 攻撃手段 I D リストに記録された攻撃手段 I D で、対策状況情報 16 の検知手段情報 162 において、○がつく検知・対策手段情報があるものを抽出し、この様に抽出された攻撃手段 I D を攻撃手段 Y として出力する。攻撃手段 I D リスト上にこの条件に該当する攻撃手段 I D が複数あれば、これらを攻撃手段 Y として出力する。具体例として、攻撃手段 I D __ e について、対策状況情報 16 の検知手段情報 162 において振る舞い検知（端末）に○が設定されていた場合は、攻撃手段 I D __ e を攻撃手段 Y として出力する。

(b2) (b1) の処理において○が付く攻撃手段が無い場合は、対策状況情報 16 の検知手段情報 162 において△がつく攻撃手段 I D を抽出する。抽出された攻撃手段 I D を攻撃手段 Y として出力する。

(b3) (b2) の処理において△が付く攻撃手段が無い場合は、対策状況情報 16 の検知手段情報 162 において□がつく攻撃手段 I D を抽出する。抽出された攻撃手段 I D を攻撃手段 Y として出力する。

なお、(b1) のみを処理しても良いし、(b1) と (b2) のみを処理しても良いし、(b1) と (b2) と (b3) とを処理してもよい。

さらに、(b1) の処理で抽出した攻撃手段 I D について、○が示される検知手段情報 162（具体例として、IDS）を、攻撃手段 I D と併せて攻撃手段 Y として出力しても良い。同様に (b2) では△である検知手段情報 162 を、(b3) では□である検知手段情報 162 を攻撃手段 I D と併せて攻撃手段 Y として出力しても良い。

【0129】

対策候補抽出装置3は、攻撃手段X1についても同様の処理で、同様の攻撃手段Y1を出力できる。

実施の形態4では、攻撃手段Xや攻撃手段X1や攻撃手段Uについて、組み合わせて検知すべき攻撃手段のうち、対策状況情報16を利用して既に組織で検知手段を実施しているものに絞り提示した。本実施の形態では、さらに、これらについて、(b1)(b2)(b3)の様に、○がつくもの、△がつくもの、□が付くものを抽出して、攻撃手段W1として出力する。

【0130】

本実施の形態の効果の説明

10

本実施の形態における対策候補抽出装置3は、実施の形態3及び4の効果に加えて、併せて対策すべき攻撃手段について、具体的にどのような検知手段を適用すればよいか判断できる効果がある。

【0131】

実施の形態9.

本実施の形態では、主に、実施の形態1と異なる点について説明する。本実施の形態において、実施の形態1から8と同様の構成には同一の符号を付し、その説明を省略する。また、実施の形態1から8と同様の機能についてもその説明を省略する。

【0132】

本実施の形態は、実施の形態1において、組織対策情報15における、運用上の制限を参照して、図18のステップS149の処理を変更したものである。

20

実施の形態1のステップS149のでは、実施の形態1においてCM__ID__i__kに該当する組織対策状況情報164__iの欄の設定について「済」と判定した場合、さらに、CM__ID__j(CM__ID__i__kに等しい)に該当する組織対策情報15のエントリを参照し、該当する運用上の制限を参照する。この運用上の制限において、閾値抑制(回数)、閾値抑制(重大度)、ホワイトリストにおいて適用がある場合は、組織対策状況情報164__iの欄に「済」の代わりに「済・回避」を設定する。

併せて、閾値抑制(回数)、閾値抑制(重大度)、ホワイトリストなど運用上の抑制措置について、その内容(組織対策情報15上の項目名)を追加情報として設定しても良い。対策状況生成装置1の利用者は、この追加情報を参照することで、検知手段は行っているが回避可能である理由を知ることができる(例:閾値抑制(回数))。

30

【0133】

対策状況判定部104が、対策状況情報16に効果度1651を付与する処理について説明する。図6の対策状況情報16における1つの攻撃手段IDについて、組織対策状況情報164が「済」の場合は、該当する検知手段情報162の構成要素の設定値(○△□◇×)をそのまま抽出して、実施検知手段情報1621として対策状況判定部104に保存する。

組織対策状況情報164が「済・回避」の場合は、該当する検知手段情報162の構成要素の設定値(○△□◇×)を抽出し、○は□に、△は□に変換して実施検知手段情報1621として対策状況判定部104に保存する。対策状況判定部104は、この様に抽出・変換した、実施検知手段情報1621について以下の様に処理する。

40

(c1) 実施検知手段情報1621に○が含まれていれば効果度1651に○を設定する。

(c2) (c1)に当てはまらない場合、△が含まれていれば△を効果度1651に設定する。

(c3) (c2)に当てはまらない場合、□が含まれていれば□を効果度1651に設定する。

(c4) (c3)に当てはまらない場合、◇が含まれていれば◇を効果度1651に設定する。

(c5) (c4)に当てはまらない場合、×を効果度1651に設定する。

50

具体例として、ある攻撃手段IDについて、組織対策状況情報164の振る舞い検知（AP）が「済・回避」であり、検知手段情報162の振る舞い検知（AP）が△であったとする。この場合は、振る舞い検知（AP）の検知手段情報162を△から□にして、実施検知手段情報1621に保存する。同じ攻撃手段IDについて、組織対策状況情報164のIDSが「済」であり、検知手段情報162のIDSが□であったとする。この場合は、IDSの検知手段情報162は変換せず□として実施検知手段情報1621に保存する。このとき、実施検知手段情報1621は□（振る舞い検知（AP））、□（IDS）であり、上記（c3）に該当するので、効果度1651に□を設定する。

【0134】

この様に、組織において検知・対策に運用制限をかけている場合、その検知・対策の製品やログ分析が攻撃手段を検知できるとしても、運用制限によってその検知能力が下がる可能性があるため、効果度1651については、検知漏れ（回避）の可能性がある評価を付与する。（c3）（c4）についてはもともと検知漏れ（回避）があるという評価であるが、（c3）については、□+、◇+として効果度1651に設定しても良い。この“+”は、通常の□、◇よりも検知漏れ（回避）が起こる可能性があるという意味である。

【0135】

本実施の形態の効果の説明

本実施の形態における対策状況生成装置1は、組織対策情報15を参照することで、攻撃手段への対策として実施している検知・対策が、運用上の制限により、検知漏れ（回避）を起こすことを、対策状況情報16に示すことが可能となり、利用者は、運用制限による検知漏れのリスクを認識できる。

【0136】

実施の形態10.

本実施の形態では、主に、実施の形態1と異なる点について説明する。本実施の形態において、実施の形態1から9と同様の構成には同一の符号を付し、その説明を省略する。また、実施の形態1から9と同様の機能についてもその説明を省略する。

【0137】

実施の形態1において、検知対策手段情報12と組織対策情報15を分けて処理したが、本実施の形態においては、組織対策情報15に検知対策手段情報12の該当する検知手段をマージして、組織対策情報15aとして使用する。

本実施の形態において、対策状況生成装置1における、攻撃情報生成部101の処理は、実施の形態1と同じである。

【0138】

本実施の形態において、検知情報生成部102における処理は、検知対策手段情報12の代わりに組織対策情報15aを使用する。それ以外の処理は、実施の形態1と同じである。この結果、攻撃検知情報121の検知手段情報162には、組織対策情報15aにおけるCM__IDで区別される検知手段が設定される。

【0139】

本実施の形態において、危険度判定部103の処理は、実施の形態1と同じである。

【0140】

本実施の形態において、対策状況判定部104の処理では、組織対策情報15の代わりに組織対策情報15aを参照する。本実施の形態では、まず、図18のS141の処理を実施する。次に、対策状況情報16において、攻撃手段IDごとに検知手段情報162を参照し、○△□◇が設定されている構成要素について、組織対策状況情報164の同じ構成要素について「済」を設定する。最後に、全ての攻撃手段IDごとに、組織対策状況情報164において「済」が設定されていない箇所は「-」を設定する。本実施の形態では、検知手段情報162は全て実施済みであり、攻撃手段について検知手段が可能な場合に○△□◇が付与される。それ以外の場合は付与されない。

その他の対策状況生成装置1の処理は実施の形態1と同じである。

図26は、本実施の形態に係る組織対策情報15aの構成の一例を示す図である。組織

10

20

30

40

50

対策情報 15 a の各行は、組織で実施済の検知手段の情報と、その運用上の制限で構成される。

【0141】

本実施の形態の効果の説明

本実施の形態における対策状況生成装置 1 は、検知対策手段情報 12 に代わりに、実施済の検知・対策手段情報と運用上の制限の情報を組み合わせた組織対策情報 15 a を参照することで、実施済の検知・対策について、効果の状況を出力することができる。

【0142】

以上、実施の形態 1 から 10 では、対策状況生成装置 1 と、攻撃事例判定装置 2 と、対策候補抽出装置 3 とを別装置として説明したが、1 つのコンピュータに対策状況生成装置 1 と、攻撃事例判定装置 2 と、対策候補抽出装置 3 との機能が搭載されていてもよい。また、攻撃対策判定システム 500 は、図 1 に示した装置構成でなくともよく、上述した機能を実現することができればどのような装置構成でも構わない。

【0143】

また、実施の形態 1 から 10 の説明において「部」として説明するもののうち、いずれか 1 つのみを採用してもよいし、いくつかの任意の組合せを採用してもよい。つまり、対策状況生成装置 1 と攻撃事例判定装置 2 と対策候補抽出装置 3 との各々の機能構成は、上記の実施の形態で説明した機能を実現することができれば、任意である。機能構成を、どのような組合せ、あるいは任意の機能構成で攻撃対策判定システム 500 を構成しても構わない。

【0144】

また、これらの実施の形態 1 から 10 のうち、複数を部分的に組合せて実施しても構わない。あるいは、これらの実施の形態のうち、1 つの実施の形態を部分的に実施しても構わない。その他、これらの実施の形態を、全体としてあるいは部分的に、どの様に組合せて実施しても構わない。

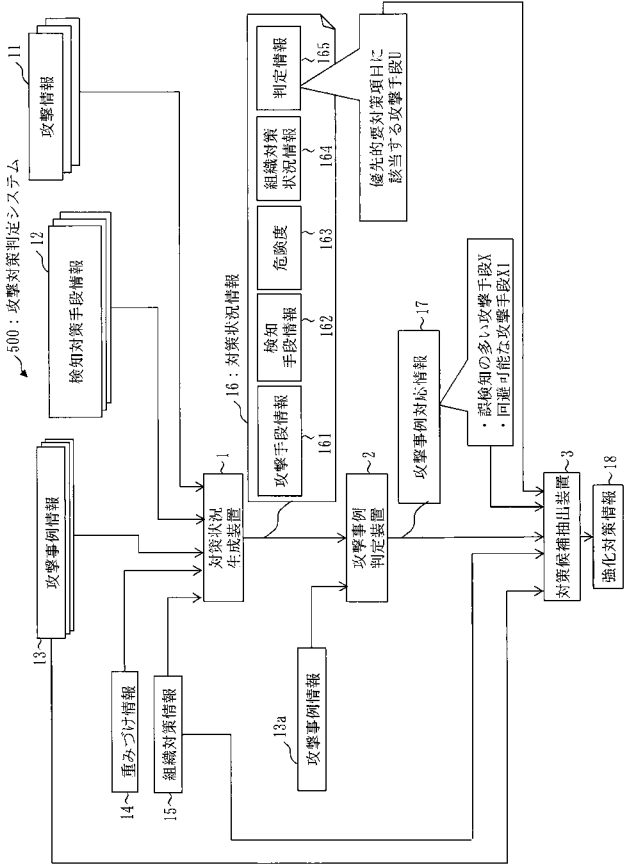
なお、上記の実施の形態は、本質的に好ましい例示であって、本発明、その適用物や用途の範囲を制限することを意図するものではなく、必要に応じて種々の変更が可能である。

【符号の説明】

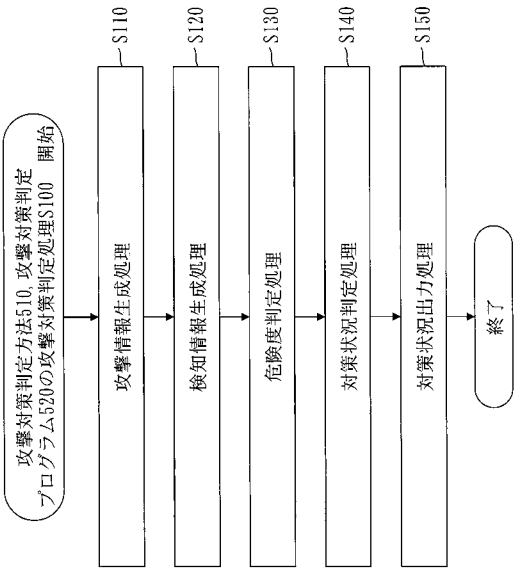
【0145】

1 対策状況生成装置、11 攻撃情報、12 検知対策手段情報、13, 13a 攻撃事例情報、14 重みづけ情報、15, 15a 組織対策情報、16 対策状況情報、17 攻撃事例対応情報、18 強化対策情報、21, X, X1, U 攻撃手段、22 検知手段、23 検知精度、24 説明文、31 攻撃フェーズ、101 攻撃情報生成部、102 検知情報生成部、103 危険度判定部、104 対策状況判定部、105 対策状況出力部、150 記憶部、111, 161 攻撃手段情報、121 攻撃検知情報、131 攻撃検知危険度情報、133 攻撃事例情報、162 検知手段情報、1621 実施検知手段情報、163 危険度、164 組織対策状況情報、165 判定情報、1651 効果度、1652 優先的対策項目、171 選択攻撃手段、2 攻撃事例判定装置、201 攻撃事例判定部、3 対策候補抽出装置、301 対策候補抽出部、500 攻撃対策判定システム、510 攻撃対策判定方法、520 攻撃対策判定プログラム、909 処理回路、910 プロセッサ、920 記憶装置、921 補助記憶装置、922 メモリ、930 入力インタフェース、940 出力インタフェース、S100 攻撃対策判定処理、S110 攻撃情報生成処理、S120 検知情報生成処理、S130 危険度判定処理、S140 対策状況判定処理、S150 対策状況出力処理。

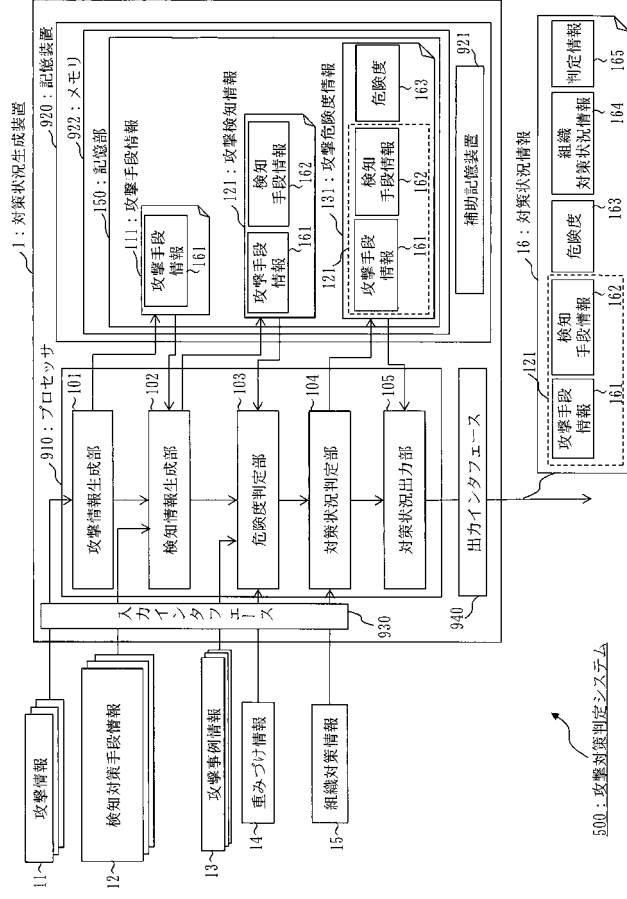
【図 1】



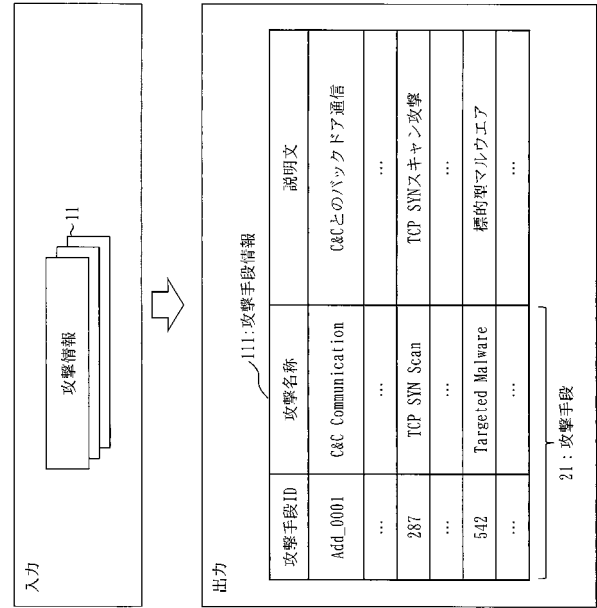
【図 3】



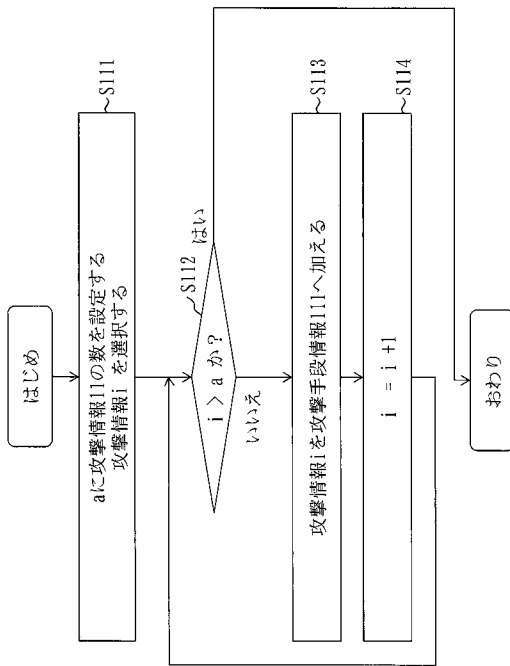
【図 2】



【図 4】



【図 5】

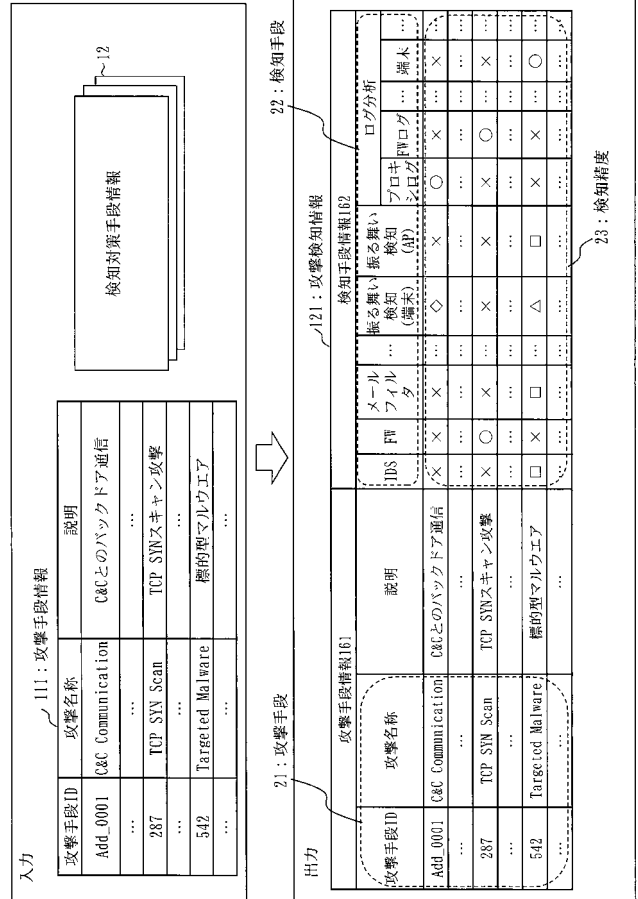


【図 7】

検知対策手段情報12の例

CM_ID	製品カテゴリ	検知可能	検知不可能	誤検知
	キーワード	キーワード	キーワード	キーワード
CM_ID_1	次世代FW	不審なHTTP通信	改ざんされた正規サイトとのHTTP通信	正規の大量のHTTP通信
	[NGFW]	[URL, suspicious, HTTP]	[URL, legitimate, HTTP]	[URL, Legitimate, HTTP]
CM_ID_2	振る舞い検知 (AP)	不審な挙動	特定の条件がそろわないと活動しない	プログラムの正規の挙動
	[behavior analysis, gateway]	[behavior, suspicious]	[condition, specific]	[Behavior, Legitimate]
CM_ID_3	IDS (シングネチャ型)	既知の攻撃	未知の攻撃	無
	[IDS, signature]	[attack, known]	[attack, unknown]	無

【図 6】



【図 8】

検知対策手段情報12の別例

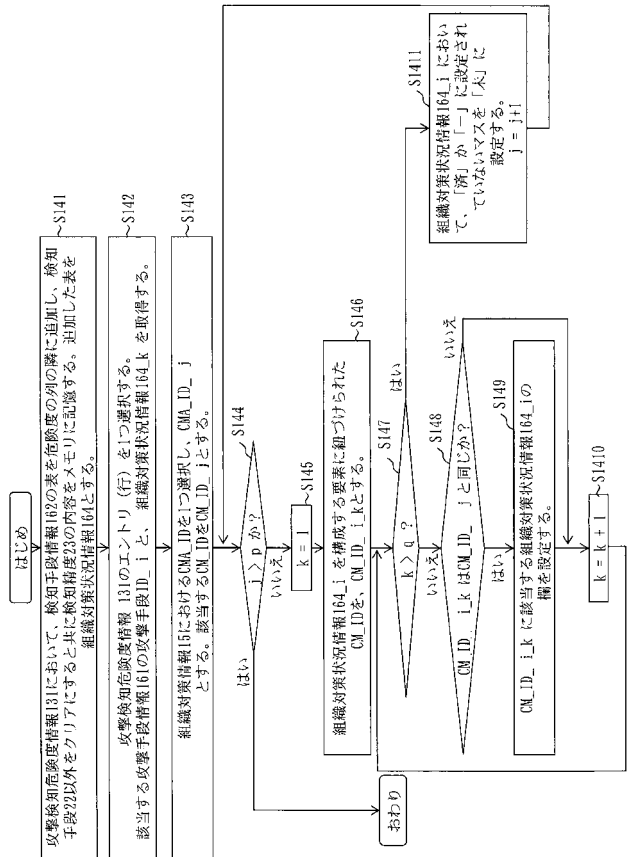
CM_ID	ログ種類	検知可能	検知不可能	誤検知
		キーワード	キーワード	キーワード
CM_ID_11	プロキシログ (PROXY)	定期的なC&C通信 [HTTP, periodic]	不定期的なC&C通信 [HTTP, unperiodic]	正規のHTTP通信 [HTTP, unintentional, periodic]
CM_ID_12	監査ログ (Audit)	認証試行の失敗 [login, fail]	無	正規ユーザの認証失敗 [login, UnintentionalFail]
CM_ID_13	FWログ (FW)	ポリシー違反の通信 [policy, violation]	ポリシー違反にならない不正通信	意図しないポリシー違反 (苦無し) [Policy, UnintentionalViolation]

【図 17】

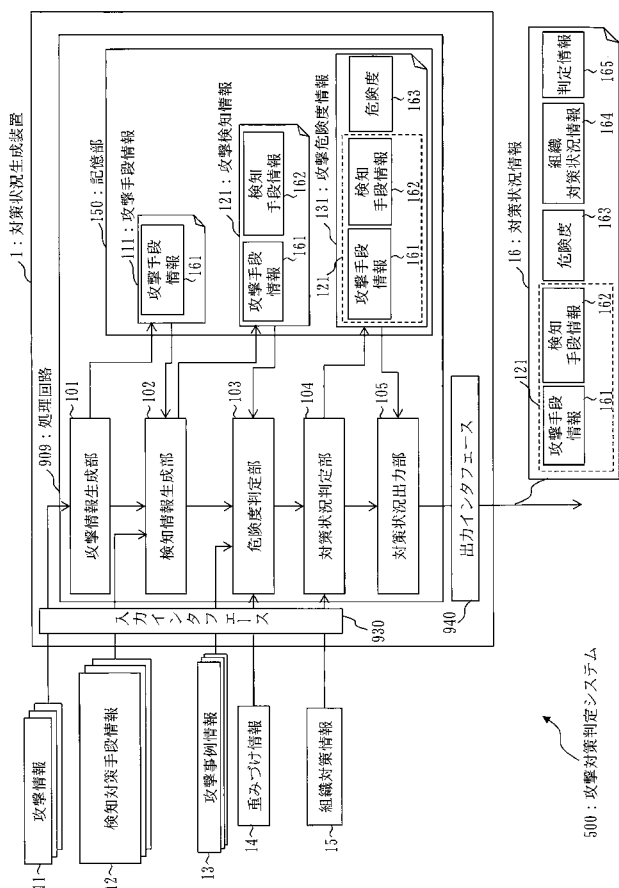
→組網対策情報15の例

CMA_ID	対応するCM_ID (検知手段のID)	運用上の制限		
		閾値抑制 (回 数)	閾値抑制 (重 大度)	ホワイトリス ト
CMA_ID_1	CM_ID_2	未適用	適用	未適用
CMA_ID_2	CM_ID_3	適用	適用	未適用
...	...	...	...	...

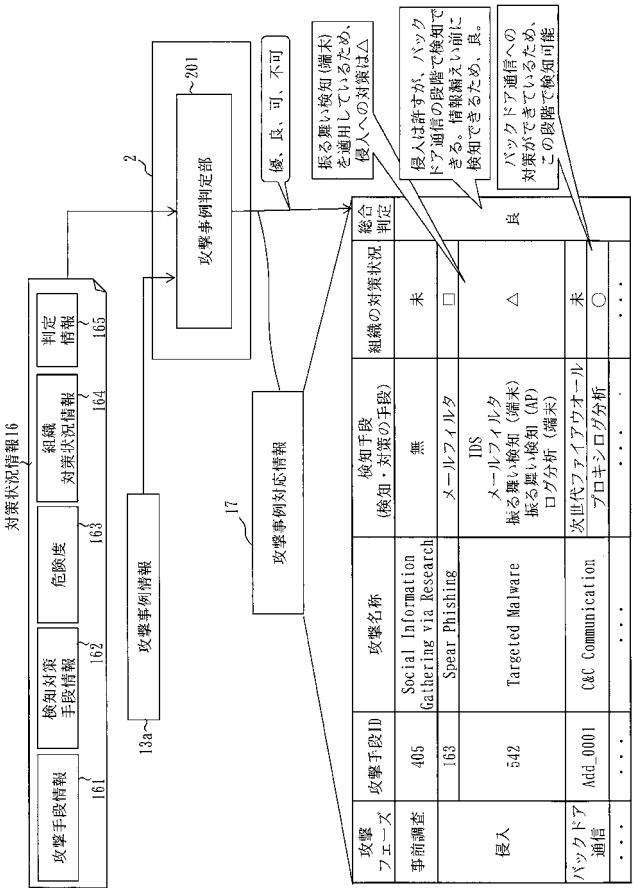
【 図 1 8 】



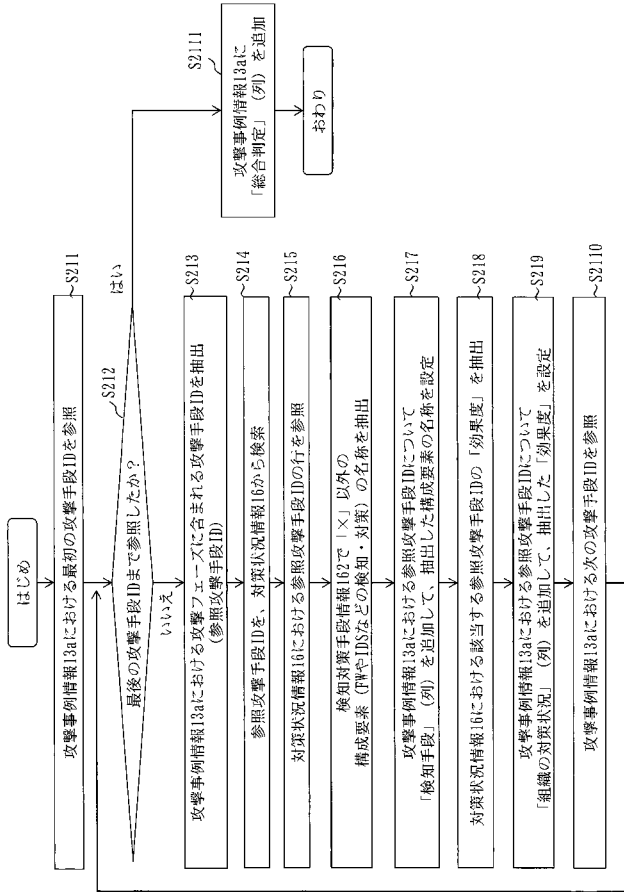
【图 19】



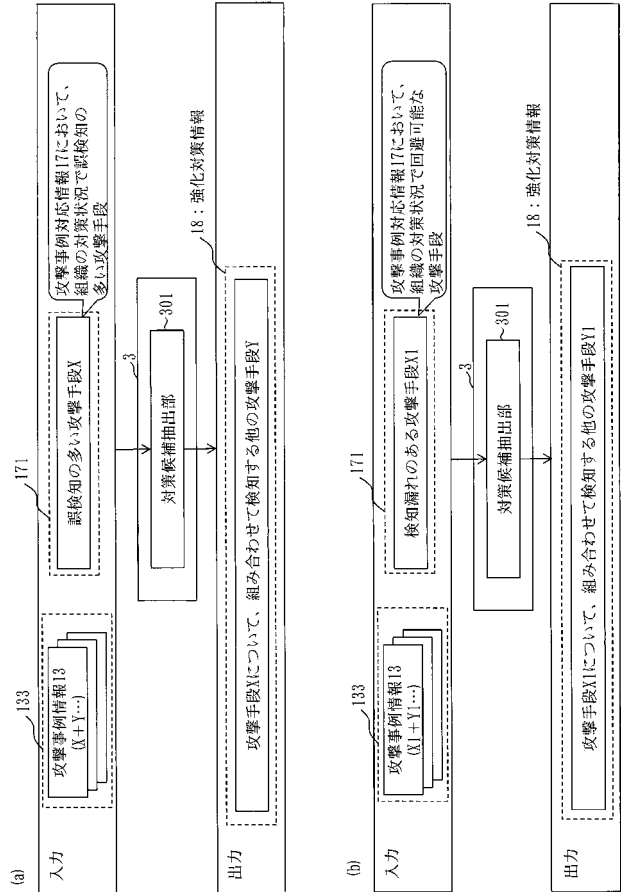
【 図 2 0 】



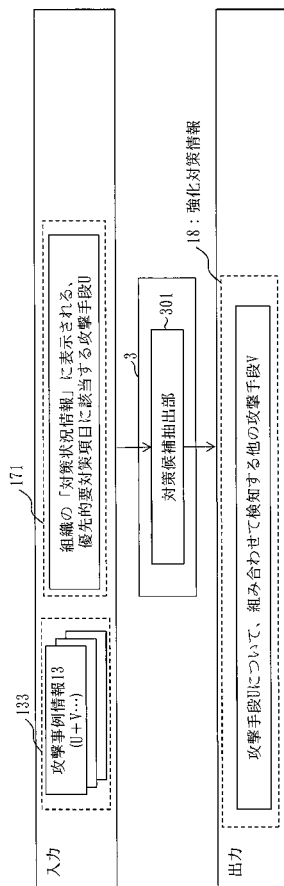
【図 2 1】



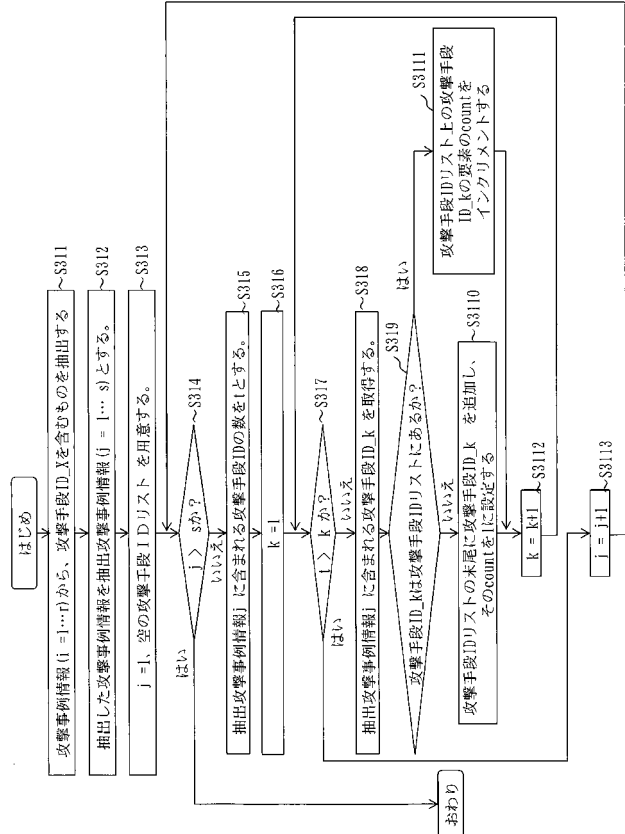
【図 2 2】



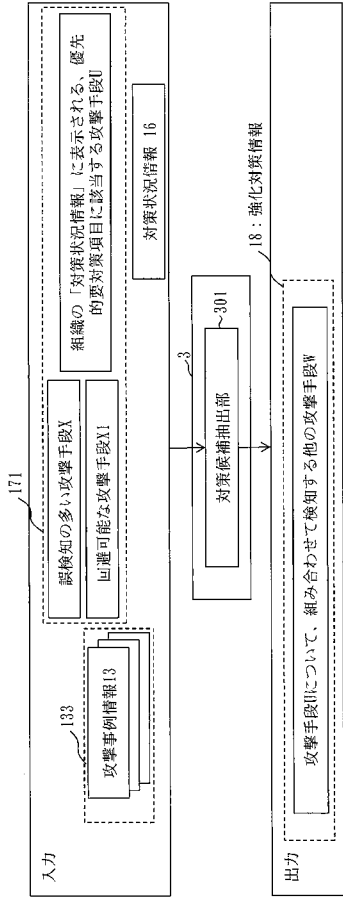
【図 2 3】



【図 2 4】



【図 25】



【図 26】

組織対策情報15aの例

CM_ID	製品カテゴリ	検知可能	検知不可能	誤検知	運用上の制限	
					閾値抑制 (回数)	ホワイトリスト
CM_ID_1	キーワード	キーワード	キーワード	キーワード	×	×
	次世代FW	不審なHTTP通信	改ざんされた正規サイトとのHTTP通信	止廻の大量のHTTP通信		
...	[NGFW]	[URL, suspicious, HTTP]	[URL, legitimate, HTTP]	[URL, Legitimate, HTTP]	○	...
	...	...	...	...		

フロントページの続き

- (72)発明者 森 滋男
東京都港区芝浦四丁目1 3 番2 3 号 三菱電機インフォメーションシステムズ株式会社内
- (72)発明者 福田 貢士
東京都港区芝浦四丁目1 3 番2 3 号 三菱電機インフォメーションシステムズ株式会社内
- (72)発明者 田中 学
東京都港区芝浦四丁目1 3 番2 3 号 三菱電機インフォメーションシステムズ株式会社内
- (72)発明者 伊串 亮二
東京都港区芝浦四丁目1 3 番2 3 号 三菱電機インフォメーションシステムズ株式会社内