(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2019年2月7日(07.02.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/026310 A1

(51) 国際特許分類:
G06F 21/55 (2013.01)

(21) 国際出願番号： PCT/JP2017/043869

(22) 国際出願日： 2017年12月6日(06.12.2017)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(30) 優先権データ：
特願 2017-150179 2017年8月2日(02.08.2017) JP

(71) 出願人:三菱電機株式会社(**MITSUBISHI ELECTRIC CORPORATION**) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 Tokyo (JP).

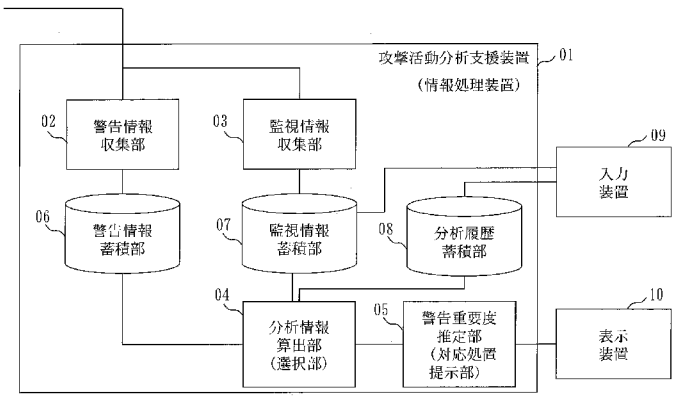
(72) 発明者:大野 一広(**ONO, Kazuhiro**); 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 伊藤 久繁(**ITO, Hisashige**); 〒1080023 東京都港区芝浦四丁目6番8号 三菱電機インフォメーションネットワーク株式会社内 Tokyo (JP). 高橋 雅香(**TAKAHASHI, Motoka**); 〒1080023 東京都港区芝浦四丁目6番8号 三菱電機インフォメーションネットワーク株式会社内 Tokyo (JP).

(74) 代理人: 溝井国際特許業務法人(**MIZOI INTERNATIONAL PATENT FIRM**); 〒2470056 神奈川県鎌倉市大船二丁目17番10号3階 Kanagawa (JP).

(54) **Title:** INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING METHOD, AND INFORMATION PROCESSING PROGRAM

(54) 発明の名称： 情報処理装置、情報処理方法及び情報処理プログラム

[図2]



01 Attack activity analysis assistance device (information processing device)
02 Alert information collection unit
03 Monitoring information collection unit
04 Analysis information computation unit (selection unit)
05 Alert importance estimation unit (response measure presentation unit)
06 Alert information accumulation unit
07 Monitoring information accumulation unit
08 Analysis information accumulation unit
09 Input device
10 Display device

(57) **Abstract:** Upon sensing an attack activity using a sensing rule, an analysis information computation unit (04) analyzes: the circumstances at the time of the detection of the present attack activity, this being the sensed attack activity; the circumstances at the time of the detection of a plurality of previous attack activities, these being a plurality of attack activities previously sensed using the sensing rule; and the circumstances whereon the sensing rule is premised. On the basis of the results of the analyses, the analysis information computation unit (04) selects an optional number of attack

WO 2019/026310 A1

[続葉有]

(81) 指定国（表示のない限り、全ての種類の国内保護が可能）：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国（表示のない限り、全ての種類の広域保護が可能）：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

— 国際調査報告（条約第21条(3)）

activities from the plurality of previous attack activities. An alert importance estimation unit (05) presents response measures carried out in response to the attack activities selected by the analysis information computation unit (04).

(57) 要約：検知ルールを用いて攻撃活動が検知された場合に、分析情報算出部（０４）は、検知された攻撃活動である現在の攻撃活動が検知された際の状況と、検知ルールを用いて過去に検知された複数の攻撃活動である複数の過去の攻撃活動のそれぞれが検知された際の状況と、検知ルールが前提としている状況とを分析し、分析結果に基づき、複数の過去の攻撃活動の中から任意数の攻撃活動を選択する。警告重要度推定部（０５）は、分析情報算出部（０４）により選択された攻撃活動に対して行われた対応処置を提示する。

明　細　書

発明の名称 ：

情報処理装置、情報処理方法及び情報処理プログラム

技術分野

[0001] 本発明は、情報システムに対する攻撃活動を検知する技術に関する。

背景技術

[0002] 本発明に関連する技術として、特許文献１～３に開示の技術がある。

[0003] 特許文献１では、サーバーが送信するＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）の宛先又は変数値から特徴量が算出され、監視装置が持つシグネチャに類似するＵＲＬであるかが判定される。これにより、監視装置が持つシグネチャに完全に一致しないＵＲＬの宛先又は変数値を用いた攻撃の通信を検知し、端末やサーバーへの未知の攻撃を検知することが可能である。特許文献１のシグネチャの類似を判定する機能の目的は新たな攻撃パターンを追加することである。

[0004] 特許文献２では、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）利用率に代表される計算機のリソース情報がセキュリティ侵害行為で変動することが多いことに着眼し、現在のＣＰＵ使用率と過去のＣＰＵ使用率の特徴量が算出される。そして、算出結果がリソース情報の条件を記載したルールと合致した場合に、異常と判定される。これにより、大量の様々なログ情報を分析することなく計算機システムへのセキュリティ侵害行為に対処することが可能である。

[0005] 遠隔からメンテナンス指示を出す際に、監視画像ではメンテナンス箇所を誤りなく指示することが困難であるという課題がある。これに対して特許文献３では、監視対象設備の画像情報と監視対象設備のＣＡＤ（Ｃｏｍｐｕｔｅｒ－Ａｉｄｅｄ　Ｄｅｓｉｇｎ）情報を組み合わせて座標情報が作成され、座標情報を用いてメンテナンス箇所が指示される。

先行技術文献

特許文献

[0006] 特許文献1：特開２０１３－０１１９４９号公報

特許文献2：特開２０１６－１８４３５８号公報

特許文献3：特許４６６１５１２号

発明の概要

発明が解決しようとする課題

[0007] 攻撃活動を監視するセキュリティ監視センターでは、アナリストが、検知された攻撃活動への対応処置を決定する。より具体的には、アナリストはセキュリティ監視センターに保管されている過去の攻撃活動の履歴をもとに、検知された攻撃活動に対する対応処置を決定する。ただし、同じ攻撃活動であっても、監視先のネットワークの構成及び対処したアナリストの経験等により異なる対応処置が選択される。このため、同じ攻撃活動に対して対応処置が異なる履歴が複数存在することになる。

経験の浅いアナリストが対応にあたった場合に、対応処置が異なる複数の履歴のうちのどの履歴を参考にすべきかを適切に判断することが困難であるという課題がある。また、複数の履歴から現在の攻撃活動に適した履歴を選択できないと、誤った対応処置がとられ、攻撃活動に有効に対処できないという課題がある。

特許文献１～３では、これらの課題を解決することはできない。

[0008] 本発明は、上記の課題を解決することを主な目的とする。具体的には、検知された攻撃活動に対して適切な対応処置がとられるようにすることを主な目的する。

課題を解決するための手段

[0009] 本発明に係る情報処理装置は、

検知ルールを用いて攻撃活動が検知された場合に、検知された攻撃活動である現在の攻撃活動が検知された際の状況と、前記検知ルールを用いて過去に検知された複数の攻撃活動である複数の過去の攻撃活動のそれぞれが検知

された際の状況と、前記検知ルールが前提としている状況とを分析し、分析結果に基づき、前記複数の過去の攻撃活動の中から任意数の攻撃活動を選択する選択部と、

前記選択部により選択された攻撃活動に対して行われた対応処置を提示する対応処置提示部とを有する。

発明の効果

[0010] 本発明では、現在の攻撃活動が検知された際の状況と、複数の過去の攻撃活動のそれぞれが検知された際の状況と、検知ルールが前提とする状況とを分析する。そして、本発明では、複数の過去の攻撃活動の中から現在の攻撃活動に適した過去の攻撃活動が選択され、選択された過去の攻撃活動に対する対応処置が提示される。

このため、本発明によれば、アナリストは、検知された攻撃活動に適した対応処置をとることができる。

図面の簡単な説明

[0011] [図1]実施の形態１に係るネットワーク構成例を示す図。

[図2]実施の形態１に係る攻撃活動分析支援装置の機能構成例を示す図。

[図3]実施の形態１に係る攻撃活動分析支援装置の処理の流れを示すフローチャート図。

[図4]実施の形態１に係る分析履歴テーブルの例を示す図。

[図5]実施の形態１に係る機器管理テーブルの例を示す図。

[図6]実施の形態１に係る類似履歴比較テーブルの例を示す図。

[図7]実施の形態１に係る選択された分析履歴の例を示す図。

[図8]実施の形態１に係るオペレーターへの提示例を示す図。

[図9]実施の形態１に係る検知ログの例を示す図。

[図10]実施の形態１に係る攻撃活動分析支援装置のハードウェア構成例を示す図。

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、図を用いて説明する。以下の実施の

形態の説明及び図面において、同一の符号を付したものは、同一の部分または相当する部分を示す。

[0013] 実施の形態１．

＊＊＊構成の説明＊＊＊

図１は、本実施の形態に係るネットワーク構成例を示す。

[0014] 本実施の形態では、ファイアウォール１１により、外部ネットワーク１６と内部ネットワーク１８とが区別されている。ファイアウォール１１は、外部ネットワーク１６とＤＭＺ（ＤｅＭｉｌｉｔａｒｉｚｅｄ　Ｚｏｎｅ）ネットワーク１７と内部ネットワーク１８とに接続されている。ファイアウォール１１及びＤＭＺネットワーク１７により、外部ネットワーク１６から内部ネットワーク１８への攻撃活動を防ぐことができる。

[0015] ＤＭＺネットワーク１７には、侵入検知装置１２、プロキシサーバー１３及び複数の監視対象１４が含まれる。

[0016] 侵入検知装置１２はファイアウォール１１と接続する。

侵入検知装置１２は、ファイアウォール１１を通過する外部ネットワーク１６とＤＭＺネットワーク１７との間の通信と、外部ネットワーク１６と内部ネットワーク１８との間の通信を検知ルールを用いて調査する。そして、侵入検知装置１２は、外部ネットワーク１６からの攻撃活動を検知した場合に、当該攻撃活動を検知した際の状況が示される検知ログを生成する。

[0017] プロキシサーバー１３は、ファイアウォール１１と接続する。

プロキシサーバー１３は、内部ネットワーク１８内の監視対象１５から外部ネットワーク１６への通信を中継する。さらに、プロキシサーバー１３は、外部ネットワーク１６から監視対象１５への通信を中継する。

[0018] 監視対象１４はファイアウォール１１と接続する。

監視対象１４にはメールサーバー、Ｗｅｂサーバー等が含まれる。

[0019] 内部ネットワーク１８には、複数の監視対象１５と攻撃活動分析支援装置０１が含まれる。

監視対象１５は、ファイアウォール１１と接続する。

監視対象１５には個人端末、ファイルサーバー、ＡＤ（Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙ）サーバー等が含まれる。

[0020] 攻撃活動分析支援装置０１は、内部ネットワーク１８に接続し、ＤＭＺネットワーク１７に接続された監視対象１４及び内部ネットワーク１８に接続された監視対象１５を監視する。

攻撃活動分析支援装置０１は、監視対象１４及び監視対象１５への攻撃活動が検知された際の状況及び対応処置が示される分析履歴を記憶している。分析履歴の詳細は後述する。

外部ネットワーク１６からＤＭＺネットワーク１７又は内部ネットワーク１８に対する攻撃活動が発生した場合に、攻撃活動分析支援装置０１は発生した攻撃活動に類似する過去の攻撃活動の分析履歴を表示装置１０を用いてオペレーターに提示する。

なお、攻撃活動とは、情報セキュリティ上の脅威を発生させるあらゆる活動である。攻撃活動には、各種の不正アクセス、「・・・攻撃」と称される攻撃、これら攻撃の予備動作等が含まれる。

なお、攻撃活動分析支援装置０１は情報処理装置に相当する。また、攻撃活動分析支援装置０１により行われる動作は、情報処理方法に相当する。

[0021] 図２は、攻撃活動分析支援装置０１の機能構成例を示し、図１０は、攻撃活動分析支援装置０１のハードウェア構成例を示す。

[0022] 本実施の形態に係る攻撃活動分析支援装置０１は、コンピュータである。

攻撃活動分析支援装置０１は、ハードウェアとして、図１０に示すように、プロセッサ１０１、記憶装置１０２、ネットワークインタフェース１０３、表示インタフェース１０４及び入力インタフェース１０５を備える。

また、攻撃活動分析支援装置０１は、機能構成として、図２に示すように、警告情報収集部０２、監視情報収集部０３、分析情報算出部０４、警告重要度推定部０５、警告情報蓄積部０６、監視情報蓄積部０７及び分析履歴蓄積部０８を備える。

記憶装置１０２には、警告情報収集部０２、監視情報収集部０３、分析情

報算出部０４及び警告重要度推定部０５の機能を実現するプログラムが記憶されている。

そして、プロセッサ１０１がこれらプログラムを実行して、後述する警告情報収集部０２、監視情報収集部０３、分析情報算出部０４及び警告重要度推定部０５の動作を行う。

図１０では、プロセッサ１０１が警告情報収集部０２、監視情報収集部０３、分析情報算出部０４及び警告重要度推定部０５の機能を実現するプログラムを実行している状態を模式的に表している。

警告情報収集部０２、監視情報収集部０３、分析情報算出部０４及び警告重要度推定部０５の機能を実現するプログラムは、情報処理プログラムに相当する。

また、警告情報蓄積部０６、監視情報蓄積部０７及び分析履歴蓄積部０８は、記憶装置１０２により実現される。

ネットワークインタフェース１０３は、内部ネットワーク１８の通信ケーブルとのインタフェースである。

表示インタフェース１０４は、表示装置１０とのインタフェースである。

入力インタフェース１０５は、入力装置０９とのインタフェースである。

[0023] 図２において、警告情報収集部０２は、ネットワークインタフェース１０３を介して侵入検知装置１２から検知ログを収集する。また、警告情報収集部０２は、収集した検知ログを警告情報蓄積部０６に格納する。

[0024] 監視情報収集部０３は、ネットワークインタフェース１０３を介してプロキシサーバー１３からプロキシログを収集する。監視情報収集部０３は、収集したプロキシログを監視情報蓄積部０７に格納する。

[0025] 分析情報算出部０４は、侵入検知装置１２により攻撃活動が検知された場合に、検知された攻撃活動である現在の攻撃活動が検知された際の状況と、検知ルールを用いて過去に検知された複数の攻撃活動である複数の過去の攻撃活動のそれぞれが検知された際の状況と、検知ルールが前提としている状況とを分析する。なお、複数の過去の攻撃活動のそれぞれが検知された際の

状況は、分析履歴蓄積部０８に蓄積されている分析履歴に記載されている。また、検知ルールが前提としている状況が示される情報は、例えば、記憶装置１０２で記憶されている。

分析情報算出部０４は、具体的には、現在の攻撃活動が検知された際の状況と複数の過去の攻撃活動のそれぞれが検知された際の状況との類似度を分析する。また、分析情報算出部０４は、複数の過去の攻撃活動のそれぞれが検知された際の状況と検知ルールが前提としている状況との類似度を分析する。例えば、分析情報算出部０４は、現在の攻撃活動が検知された時刻と複数の過去の攻撃活動のそれぞれが検知された時間帯との類似度を分析する。また、分析情報算出部０４は、現在の攻撃活動が検知された際の通信量と複数の過去の攻撃活動のそれぞれが検知された際の通信量との類似度を分析する。また、分析情報算出部０４は、複数の過去の攻撃活動のそれぞれが検知された時間帯と検知ルールが前提とする時間帯との類似度を分析する。また、分析情報算出部０４は、複数の過去の攻撃活動のそれぞれが検知された際の通信量と検知ルールが前提とする通信量との類似度を分析する。更に、分析情報算出部０４は、複数の過去の攻撃活動のそれぞれのターゲットの機器の種類と検知ルールが前提とするターゲットの機器の種類との類似度を分析する。

そして、分析情報算出部０４は、分析結果に基づき、複数の過去の攻撃活動の中から任意数の攻撃活動を選択する。

分析情報算出部０４は選択部に相当する。また、分析情報算出部０４により行われる処理は、選択処理に相当する。

[0026] 警告重要度推定部０５は、分析情報算出部０４により選択された攻撃活動に対して行われた対応処置を表示装置１０を通じてオペレーターに提示する。

分析情報算出部０４により２以上の攻撃活動が選択された場合に、警告重要度推定部０５は、選択された２以上の攻撃活動の間の序列を決定する。警告重要度推定部０５は、例えば、選択された２以上の攻撃活動の各々の対応

処置の重要度に基づき、選択された２以上の攻撃活動の間の序列を決定する。そして、警告重要度推定部０５は、決定した序列に従って、選択された２以上の攻撃活動に対して行われた対応処置を提示する。

警告重要度推定部０５は、対応処置提示部に相当する。また、警告重要度推定部０５により行われる処理は、対応処置提示処理に相当する。

[0027] 警告情報蓄積部０６は、検知ログを蓄積する。

[0028] 監視情報蓄積部０７は、プロキシログを蓄積する。

[0029] 分析履歴蓄積部０８は、分析履歴を蓄積する。

[0030] 次に、本実施の形態で扱われるデータを説明する。

[0031] 図４は、分析情報算出部０４が生成する分析履歴テーブル２０３の例を示す。

[0032] 図４に示すように、分析履歴テーブル２０３には、過去の攻撃活動を分析した結果である分析履歴が複数含まれる。図４の各レコードが分析履歴である。各分析履歴には、分析履歴番号、警告名、発生時間帯、対応処置、解析情報が含まれる。

[0033] 分析履歴番号は、分析情報算出部０４により自動的に設定される通し番号である。

対応処置は、攻撃活動分析支援装置０１のオペレーターにより指定される。

[0034] 警告名、発生時間帯は、侵入検知装置１２から送信された検知ログから生成される。侵入検知装置１２は、外部ネットワーク１６から内部ネットワーク１８への通信を検知ルールを用いて解析する。攻撃活動を検知した場合に、侵入検知装置１２は、検知ルールに基づき、攻撃活動の種類を特定する。侵入検知装置１２は、検知した攻撃の種類が、例えば、Ｄｏｓ攻撃、ポートスキャン、ファイル送信のうちのいずれであるかを特定する。そして、侵入検知装置１２は、特定した攻撃の種類を警告名として検知ログに含ませる。また、侵入検知装置１２は、攻撃活動を検知した日時を検知ログに含ませる。

また、解析情報の値も、検知ログから生成される。例えば、侵入検知装置１２は、攻撃活動に用いられる通信データの送信先のＩＰアドレスから攻撃活動の通信先を特定し、特定した通信先の種類を検知ログに含ませる。また、侵入検知装置１２は、攻撃活動に用いられる通信データの送信先のＩＰアドレスのみを検知ログに含ませるようにしてもよい。この場合は、分析情報算出部０４が検知ログに含まれる送信先のＩＰアドレスから通信先の種類を特定する。より具体的には、分析情報算出部０４は図５に例示する機器管理テーブル２０４を用いて通信先の種類を特定する。図５の機器管理テーブル２０４には、監視対象１４及び監視対象１５のそれぞれを構成する機器のＩＰアドレスが示され、ＩＰアドレスごとに、各機器の用途が示される。機器の用途はメールサーバー、Ｗｅｂサーバー、個人端末、ファイルサーバー、ＡＤサーバー等である。分析情報算出部０４は、検知ログで示される送信先のＩＰアドレスを機器管理テーブル２０４と照合して、通信先の種類を特定する。

また、侵入検知装置１２は、攻撃活動を検知した際のＤＭＺネットワーク１７または内部ネットワーク１８の通信量を検知ログに含ませる。

なお、侵入検知装置１２は、通信先の種類及び通信量の少なくともいずれかを特定しなくてもよい。つまり、侵入検知装置１２は、通信先の種類及び通信量の少なくともいずれかを検知ログに含めなくてもよい。この場合は、分析情報算出部０４は、プロキシログから解析情報を生成する。

つまり、プロキシサーバー１３は、通信先の種類及び攻撃活動が検知された際の通信量を特定し、特定した通信先の種類及び通信量をプロキシログに記載してもよい。

[0035] 図６は、類似履歴比較テーブル２０５の例を示す。

[0036] 図６に示すように、類似履歴比較テーブル２０５は、分析履歴番号、検知ルールが前提とする状況、過去の攻撃活動の検知時の状況で構成される。

分析履歴番号は、図５の分析履歴番号を示す。

「検知ルールが前提とする状況」では、検知ルールが生成される際に前提

とされた状況が示される。図６の例では、ＤｏＳ攻撃を検知するための検知ルールが前提とする状況が示される。「検知ルールが前提とする状況」は、例えば、時間帯と通信量とターゲットの機器である。図６の例では、ＤｏＳ攻撃が発生する時間帯が「１０：００－１２：００」であり、また、ＤｏＳ攻撃が発生する際の通信量が５０００アクセス／分であり、また、ＤｏＳ攻撃がターゲットにする機器がＷｅｂサーバーであるとの前提で、ＤｏＳ攻撃を検知するための検知ルールが生成されている。

「過去の攻撃活動の検知時の状況」では、ＤｏＳ攻撃と判定された過去の攻撃活動、すなわち、Ｄｏｓ攻撃を検知するための検知ルールが適用されて検知された過去の攻撃活動の検知時の状況が示される。「過去の攻撃活動の検知時の状況」は、例えば、時間帯と通信量とターゲットの機器である。分析履歴番号：１のＤｏＳ攻撃が検知された時間帯は「１０：００－１２：００」であり、当該ＤｏＳ攻撃が検知された際の通信量は５５００アクセス／分であり、また、当該ＤｏＳ攻撃がターゲットにした機器はＷｅｂサーバーである。

類似履歴比較テーブル２０５は、過去の攻撃活動ごとに、検知ルールが前提とする状況と、各攻撃活動が検知された際の状況との比較に用いられる。

[0037] 図６は、ＤｏＳ攻撃についての類似履歴比較テーブル２０５を示すが、他の攻撃活動（ポートスキャン、ファイル送信等）についても、同様の類似履歴比較テーブル２０５が存在する。

[0038] 図９は、侵入検知装置１２が新たに攻撃活動を検知した際に侵入検知装置１２から攻撃活動分析支援装置０１に送信される検知ログ３０１の例を示す。

[0039] 検知ログ３０１は、警告名、発生日時及び解析情報で構成される。

警告名、発生日時及び解析情報のそれぞれの意味は、図４に示すものと同じである。

図４に示す警告名、発生日時及び解析情報は、過去に検知された過去の攻撃活動の属性であるのに対し、図９に示す警告名、発生日時及び解析情報は

、新たに検知された現在の攻撃活動の属性である。

図９では、解析情報の値も検知ログ３０１として侵入検知装置１２から送信される例を示すが、前述したように、解析情報の値はプロキシログとしてプロキシサーバー１３から送信されてもよい。

[0040] ＊＊＊動作の説明＊＊＊

次に、本実施の形態に係る攻撃活動分析支援装置０１の動作例を説明する。

図３は、攻撃活動分析支援装置０１の動作例を示すフローチャートである。

[0041] 図４に示す分析履歴テーブル２０３が分析履歴蓄積部０８に蓄積されていなければ、分析情報算出部０４が初期設定として、分析履歴テーブル２０３を生成する（ステップＳ００１）。

また、分析情報算出部０４は、必要であれば、監視対象１４と監視対象１５の機器管理テーブル２０４を生成する。

[0042] 警告情報収集部０２は侵入検知装置１２から定期的に検知ログを受信し、受信した検知ログを警告情報蓄積部０６に格納する（ステップＳ００２）。

侵入検知装置１２は、攻撃活動を検知していない場合にも検知ログを定期的に送信する。侵入検知装置１２は、攻撃活動を検知していない場合は、攻撃活動を検知した場合の検知ログとは異なる検知ログを送信する。例えば、侵入検知装置１２は、図９の警告名の欄が空欄の検知ログを送信する。

警告情報収集部０２は、受信した検知ログが攻撃活動の検知を通知する検知ログが否かを判定する（ステップＳ００３）。例えば、警告情報収集部０２は、受信した検知ログの警告名の欄に値が設定されているか否かを判定する。

受信した検知ログが攻撃活動の検知を通知する検知ログであれば、処理がステップＳ００４に移行する。一方、受信した検知ログが攻撃活動の検知を通知する検知ログでなければ、処理がステップＳ００２に戻る。

ここでは、警告情報収集部０２が図９に示す検知ログ３０１を受信したと

仮定する。つまり、侵入検知装置１２によりＤｏＳ攻撃が検知されたものとする。

[0043] ステップＳ００３がＹＥＳの場合、すなわち、侵入検知装置１２において攻撃活動が検知された場合は、警告情報収集部０２は、侵入検知装置１２から受信した検知ログを分析情報算出部０４に出力する。

分析情報算出部０４は、分析履歴蓄積部０８から、警告情報収集部０２から取得した検知ログに示される警告名に対応する分析履歴テーブル２０３を取得する（ステップＳ００４）。具体的には、分析情報算出部０４は、図９の検知ログ３０１の警告名であるＤｏＳ攻撃に対応する図４の分析履歴テーブル２０３を取得する。

[0044] 次に、分析情報算出部０４は、分析履歴テーブル２０３から、検知ログに示される通信先と共通の通信先が示される分析履歴を抽出する（ステップＳ００５）。

図４の例では、分析情報算出部０４は、通信先がＷｅｂサーバーである分析履歴番号１、３、４、５、１０の分析履歴を抽出する。

[0045] 次に、分析情報算出部０４は、ステップＳ００５で抽出した分析履歴の類似度を分析する（ステップＳ００６）。

類似度の分析には、類似履歴比較テーブル２０５が用いられる。具体的には、分析情報算出部０４は、検知ログに示される現在の攻撃活動が検知された時刻と、分析履歴番号１、３、４、５、１０の「過去の攻撃活動の検知時の状況」の「発生時間帯」に示される時間帯との類似度を算出する。また、分析情報算出部０４は、検知ログに示される現在の攻撃活動が検知された際の通信量と分析履歴番号１、３、４、５、１０の「過去の攻撃活動の検知時の状況」の「通信量」に示される通信量との類似度を算出する。また、分析情報算出部０４は、分析履歴番号１、３、４、５、１０の「過去の攻撃活動の検知時の状況」の「発生時間帯」に示される時間帯と「検知ルールが前提とする状況」の「発生時間帯」に示される時間帯との類似度を算出する。また、分析情報算出部０４は、分析履歴番号１、３、４、５、１０の「過去の

攻撃活動の検知時の状況」の「通信量」に示される通信量と「検知ルールが前提とする状況」の「通信量」に示される通信量との類似度を算出する。更に、分析情報算出部０４は、分析履歴番号１、３、４、５、１０の「過去の攻撃活動の検知時の状況」の「ターゲット」に示される機器の種類と「検知ルールが前提とする状況」「ターゲット」に示される機器の種類との類似度を算出する。

[0046] 図９の検知ログ３０１では、発生時刻は「１０：１８」であり、通信量は「５５００アクセス／分」である。このため、現在の攻撃活動との関係では、分析履歴番号１、３、４に高い類似度が付与される。また、図６の「検知ルールが前提とする状況」では発生時間帯は「１０：００－１２：００」であり、「通信量」は「５０００」であり、「ターゲット」は「Ｗｅｂ」である。このため、検知ルールとの関係でも、分析履歴番号１、３、４に高い類似度が付与される。なお、本実施の形態では、類似度の算出方法自体は問わない。

この結果、図６の例では、分析情報算出部０４は、新規に発生した検知ログの分析に適した履歴として、類似度の高い分析履歴番号１、３、４の分析履歴を選択する。

そして、分析情報算出部０４は、分析履歴番号１、３、４の分析履歴（図４の該当するレコード）を警告重要度推定部０５に出力する。

[0047] 警告重要度推定部０５は、分析情報算出部０４から分析履歴を取得し、取得した分析履歴の重要度に従って、取得した分析履歴を表示装置１０を介してオペレーターに提示する（ステップＳ００７）。

警告重要度推定部０５は、分析情報算出部０４から取得した分析履歴が一つである場合は、取得した分析履歴を表示装置１０を介してオペレーターに提示する。

一方、分析情報算出部０４から取得した分析履歴が複数である場合は、警告重要度推定部０５は、分析履歴の重要度を判定する。そして、警告重要度推定部０５は、重要度の順に複数の分析履歴の間の序列を決定し、決定した

序列に従って、複数の分析履歴を表示装置１０を介してオペレーターに提示する。

分析履歴の重要度の判定方法は以下のとおりである。

まず、警告重要度推定部０５は、分析履歴内の「対応処置」に記載された対策の要否の項目から、対策が必要であった分析履歴を上位に並べ替える。次に分析履歴内の「対応処置」に記載された処置内容の項目に「客先に通報」が記載されている分析履歴を上位に並べ替える。

図７は、警告重要度推定部０５に通知された分析履歴の順序を示す。図７の例では、分析履歴番号１、３、４の順序で分析情報算出部０４から警告重要度推定部０５に通知されている。

図８は、警告重要度推定部０５により順序が変更されたのちの分析履歴の順序を示す。図８の例では、分析履歴が分析歴番号３、１、４の順序に変更されている。つまり、「客先に通報」が記載されている分析履歴番号３の分析履歴が最も重要度が高く、「対策要」が記載されている分析履歴番号１の分析履歴が２番目に重要度が高い。

警告重要度推定部０５は、図８に示す順序で複数の分析履歴をオペレーターに提示する。

オペレーターは、警告重要度推定部０５から提示された分析履歴の「対応処置」の欄の記載を参考に、新たに検知された現在の攻撃活動に対する対応処置を検討することができる。

なお、新たに検知された現在の攻撃活動に対する対応処置がオペレーターにより決定された後に、分析情報算出部０４は、図９の検知ログ３０１の記載内容とオペレータにより決定された対応処置とが示される新たなレコードを分析履歴テーブル２０３に追加する。

[0048] ＊＊＊実施の形態の効果の説明＊＊＊

このように、本実施の形態では、現在の攻撃活動が検知された際の状況と、複数の過去の攻撃活動のそれぞれが検知された際の状況と、検知ルールが前提とする状況とを分析する。そして、本実施の形態では、複数の過去の攻

撃活動の中から現在の攻撃活動に適した過去の攻撃活動が選択され、選択された過去の攻撃活動に対する対応処置が提示される。このため、本実施の形態によれば、経験の浅いアナリスト（オペレーター）であっても、現在の攻撃活動に適した対応処置をとることができる。

[0049] ＊＊＊ハードウェア構成の説明＊＊＊

最後に、攻撃活動分析支援装置０１のハードウェア構成の補足説明を行う。

図１０に示すプロセッサ１０１は、プロセッシングを行うＩＣ（Ｉｎｔｅｇｒａｔｅｄ Ｃｉｒｃｕｉｔ）である。

プロセッサ１０１は、ＣＰＵ、ＤＳＰ（Ｄｉｇｉｔａｌ Ｓｉｇｎａｌ Ｐｒｏｃｅｓｓｏｒ）等である。

図３に示す記憶装置１０２は、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、フラッシュメモリ、ＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）等である。

図３に示すネットワークインタフェース１０３は、データの通信処理を実行する電子回路である。

ネットワークインタフェース１０３は、例えば、通信チップ又はＮＩＣ（Ｎｅｔｗｏｒｋ Ｉｎｔｅｒｆａｃｅ Ｃａｒｄ）である。

[0050] また、記憶装置１０２には、ＯＳ（Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ）も記憶されている。

そして、ＯＳの少なくとも一部がプロセッサ１０１により実行される。

プロセッサ１０１はＯＳの少なくとも一部を実行しながら、警告情報収集部０２、監視情報収集部０３、分析情報算出部０４及び警告重要度推定部０５の機能を実現するプログラムを実行する。

プロセッサ１０１がＯＳを実行することで、タスク管理、メモリ管理、ファイル管理、通信制御等が行われる。

また、警告情報収集部０２、監視情報収集部０３、分析情報算出部０４及

び警告重要度推定部０５の処理の結果を示す情報、データ、信号値及び変数値の少なくともいずれかが、記憶装置１０２、プロセッサ１０１内のレジスタ及びキャッシュメモリの少なくともいずれかに記憶される。

また、警告情報収集部０２、監視情報収集部０３、分析情報算出部０４及び警告重要度推定部０５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等の可搬記憶媒体に記憶されてもよい。

[0051] また、警告情報収集部０２、監視情報収集部０３、分析情報算出部０４及び警告重要度推定部０５の「部」を、「回路」又は「工程」又は「手順」又は「処理」に読み替えてもよい。

また、攻撃活動分析支援装置０１は、処理回路により実現されてもよい。処理回路は、例えば、ロジックＩＣ（Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）、ＧＡ（Ｇａｔｅ　Ａｒｒａｙ）、ＡＳＩＣ（Ａｐｐｌｉｃａｔｉｏｎ　Ｓｐｅｃｉｆｉｃ　Ｉｎｔｅｇｒａｔｅｄ　Ｃｉｒｃｕｉｔ）、ＦＰＧＡ（Ｆｉｅｌｄ－Ｐｒｏｇｒａｍｍａｂｌｅ　Ｇａｔｅ　Ａｒｒａｙ）である。

この場合は、警告情報収集部０２、監視情報収集部０３、分析情報算出部０４及び警告重要度推定部０５は、それぞれ処理回路の一部として実現される。

なお、本明細書では、プロセッサと、メモリと、プロセッサとメモリの組合せと、処理回路との上位概念を、「プロセッシングサーキットリー」という。

つまり、プロセッサと、メモリと、プロセッサとメモリの組合せと、処理回路とは、それぞれ「プロセッシングサーキットリー」の具体例である。

符号の説明

[0052] ０１　攻撃活動分析支援装置、０２　警告情報収集部、０３　監視情報収集部、０４　分析情報算出部、０５　警告重要度推定部、０６　警告情報蓄積部、０７　監視情報蓄積部、０８　分析履歴蓄積部、０９　入力装置、１

０　表示装置、１１　ファイアウォール、１２　侵入検知装置、１３　プロキシサーバー、１４　監視対象、１５　監視対象、１６　外部ネットワーク、１７　ＤＭＺネットワーク、１８　内部ネットワーク、１０１　プロセッサ、１０２　記憶装置、１０３　ネットワークインタフェース、１０４　表示インタフェース、１０５　入力インタフェース。

請求の範囲

[請求項1] 検知ルールを用いて攻撃活動が検知された場合に、検知された攻撃活動である現在の攻撃活動が検知された際の状況と、前記検知ルールを用いて過去に検知された複数の攻撃活動である複数の過去の攻撃活動のそれぞれが検知された際の状況と、前記検知ルールが前提としている状況とを分析し、分析結果に基づき、前記複数の過去の攻撃活動の中から任意数の攻撃活動を選択する選択部と、

前記選択部により選択された攻撃活動に対して行われた対応処置を提示する対応処置提示部とを有する情報処理装置。

[請求項2] 前記選択部は、

前記現在の攻撃活動が検知された際の状況と前記複数の過去の攻撃活動のそれぞれが検知された際の状況との類似度を分析し、前記複数の過去の攻撃活動のそれぞれが検知された際の状況と前記検知ルールが前提としている状況との類似度を分析する請求項１に記載の情報処理装置。

[請求項3] 前記選択部は、

前記現在の攻撃活動が検知された時刻と前記複数の過去の攻撃活動のそれぞれが検知された時間帯との類似度と、前記現在の攻撃活動が検知された際の通信量と前記複数の過去の攻撃活動のそれぞれが検知された際の通信量との類似度と、前記複数の過去の攻撃活動のそれぞれが検知された時間帯と前記検知ルールが前提とする時間帯との類似度と、前記複数の過去の攻撃活動のそれぞれが検知された際の通信量と前記検知ルールが前提とする通信量との類似度とを分析する請求項１に記載の情報処理装置。

[請求項4] 前記選択部は、

前記複数の過去の攻撃活動のそれぞれのターゲットの機器の種類と、前記検知ルールが前提とするターゲットの機器の種類との類似度を分析する請求項３に記載の情報処理装置。

[請求項5] 前記対応処置提示部は、

前記選択部により前記複数の過去の攻撃活動の中から２以上の攻撃活動が選択された場合に、選択された２以上の攻撃活動の間の序列を決定し、決定した序列に従って、選択された２以上の攻撃活動に対して行われた対応処置を提示する請求項１に記載の情報処理装置。

[請求項6] 前記対応処置提示部は、

選択された２以上の攻撃活動の各々の対応処置の重要度に基づき、選択された２以上の攻撃活動の間の序列を決定する請求項５に記載の情報処理装置。

[請求項7] 前記選択部は、

前記現在の攻撃活動の種類と同じ種類の複数の過去の攻撃活動であって、前記現在の攻撃活動のターゲットの機器の種類と同じ種類の機器をターゲットとする複数の過去の攻撃活動のそれぞれが検知された際の状況を分析する請求項１に記載の情報処理装置。

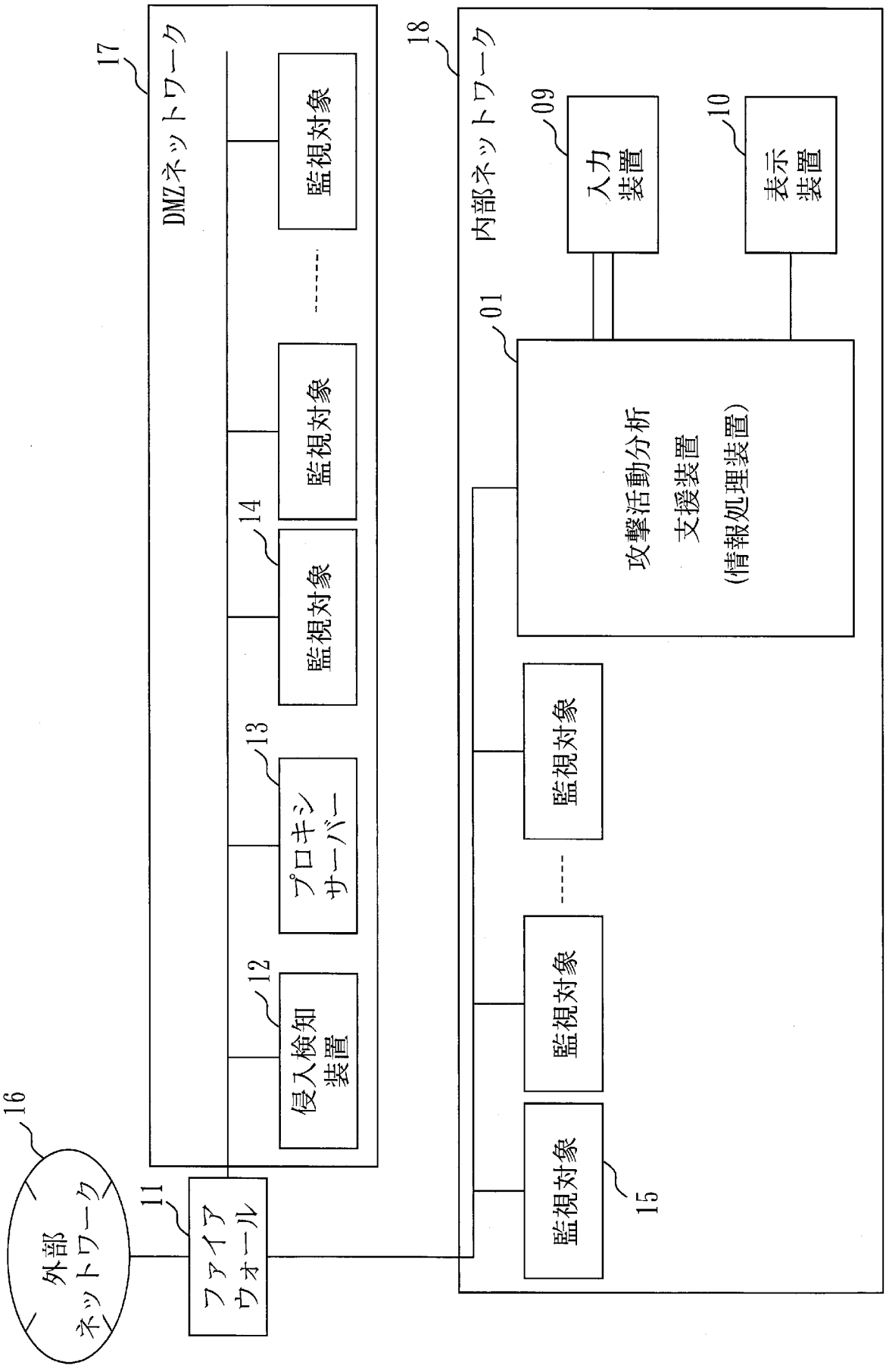
[請求項8] 検知ルールを用いて攻撃活動が検知された場合に、コンピュータが、検知された攻撃活動である現在の攻撃活動が検知された際の状況と、前記検知ルールを用いて過去に検知された複数の攻撃活動である複数の過去の攻撃活動のそれぞれが検知された際の状況と、前記検知ルールが前提としている状況とを分析し、分析結果に基づき、前記複数の過去の攻撃活動の中から任意数の攻撃活動を選択し、

前記コンピュータが、選択された攻撃活動に対して行われた対応処置を提示する情報処理方法。

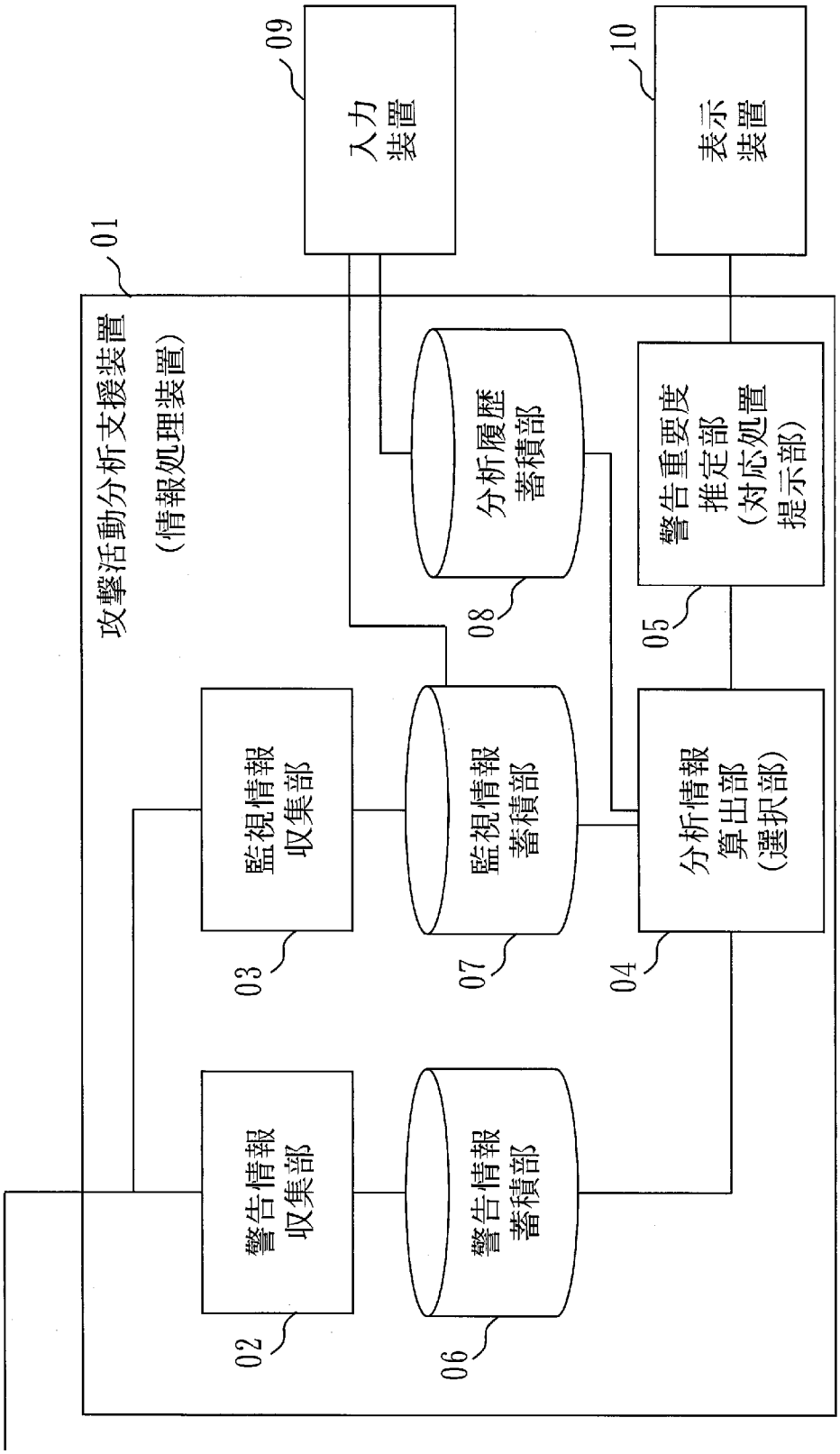
[請求項9] 検知ルールを用いて攻撃活動が検知された場合に、検知された攻撃活動である現在の攻撃活動が検知された際の状況と、前記検知ルールを用いて過去に検知された複数の攻撃活動である複数の過去の攻撃活動のそれぞれが検知された際の状況と、前記検知ルールが前提としている状況とを分析し、分析結果に基づき、前記複数の過去の攻撃活動の中から任意数の攻撃活動を選択する選択処理と、

前記選択処理により選択された攻撃活動に対して行われた対応処置を提示する対応処置提示処理とをコンピュータに実行させる情報処理プログラム。

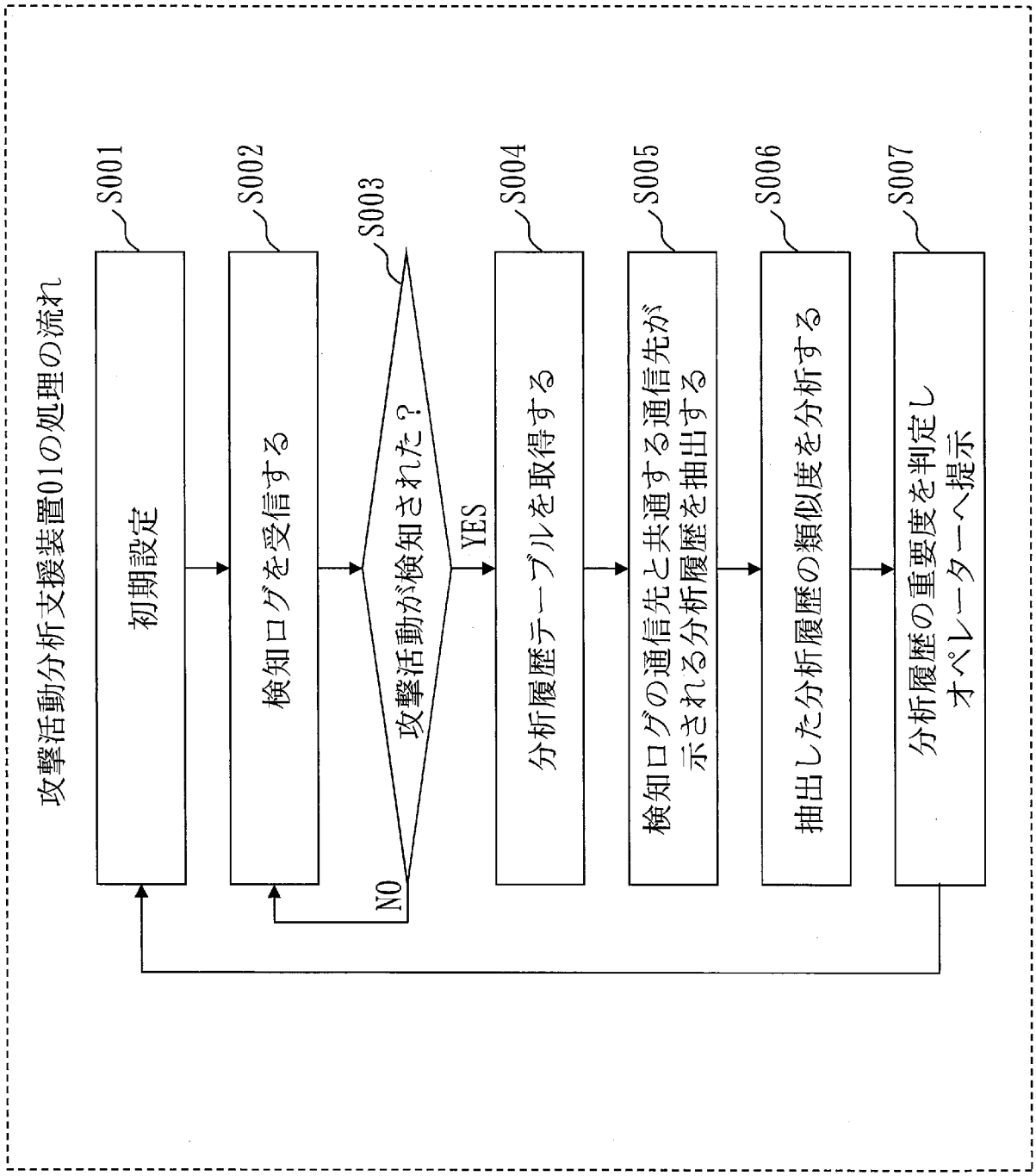
[図1]


外部
ネットワーク
16
ファイア
ウォール
11
DMZネットワーク
17
侵入検知
装置
12
プロキシ
サーバー
13
監視対象
14
監視対象
監視対象
監視対象
15
内部ネットワーク
18
攻撃活動分析
支援装置
(情報処理装置)
01
入力
装置
09
表示
装置
10

[図2]


01
攻撃活動分析支援装置
(情報処理装置)
09
入力
装置
10
表示
装置
02
警告情報
収集部
03
監視情報
収集部
04
分析情報
算出部
(選択部)
05
警告重要度
推定部
(対応処置
提示部)
06
警告情報
蓄積部
07
監視情報
蓄積部
08
分析履歴
蓄積部

[図3]

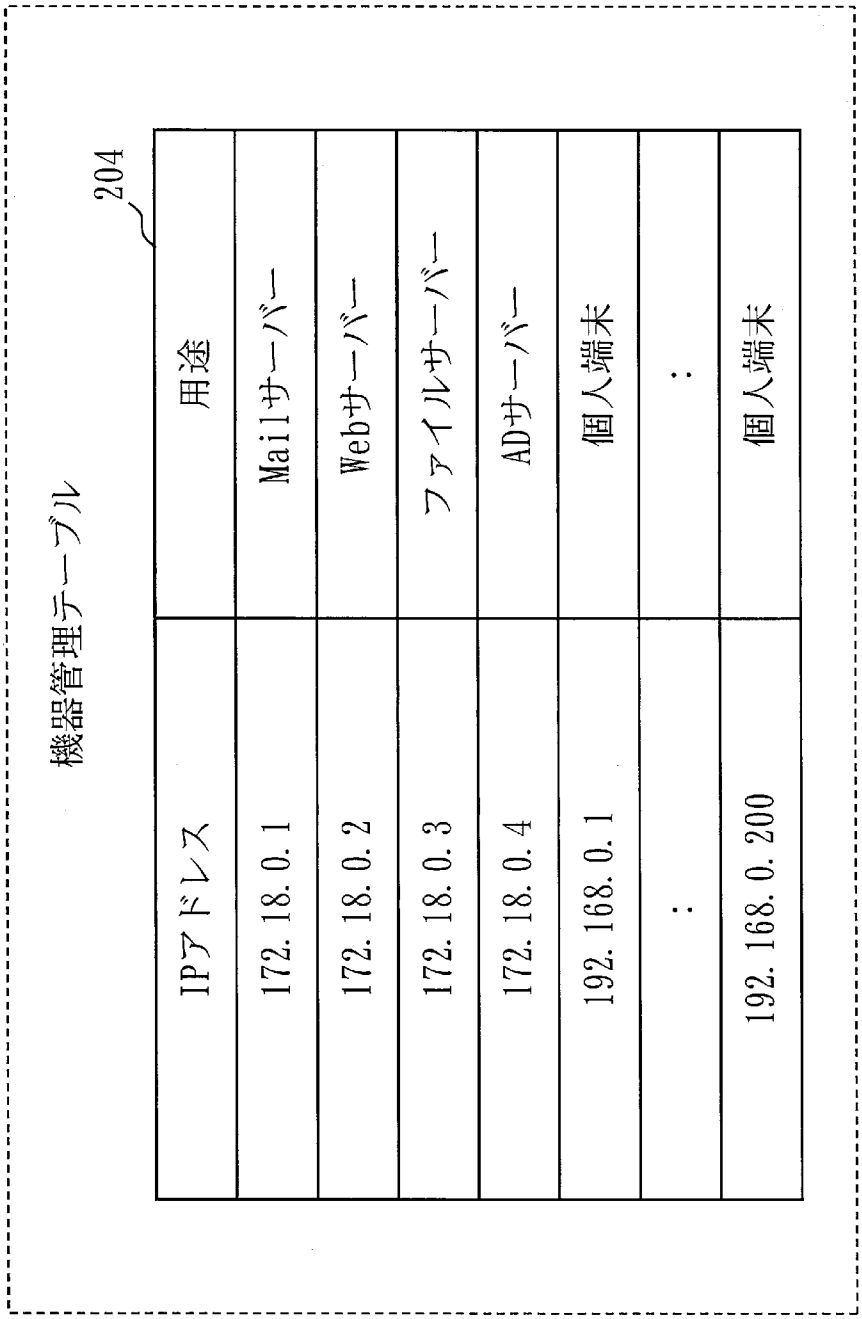

攻撃活動分析支援装置01の処理の流れ
S001
初期設定
S002
検知ログを受信する
S003
攻撃活動が検知された？
YES
NO
S004
分析履歴テーブルを取得する
S005
検知ログの通信先と共通する通信先が示される分析履歴を抽出する
S006
抽出した分析履歴の類似度を分析する
S007
分析履歴の重要度を判定しオペレーターへ提示

[図4]

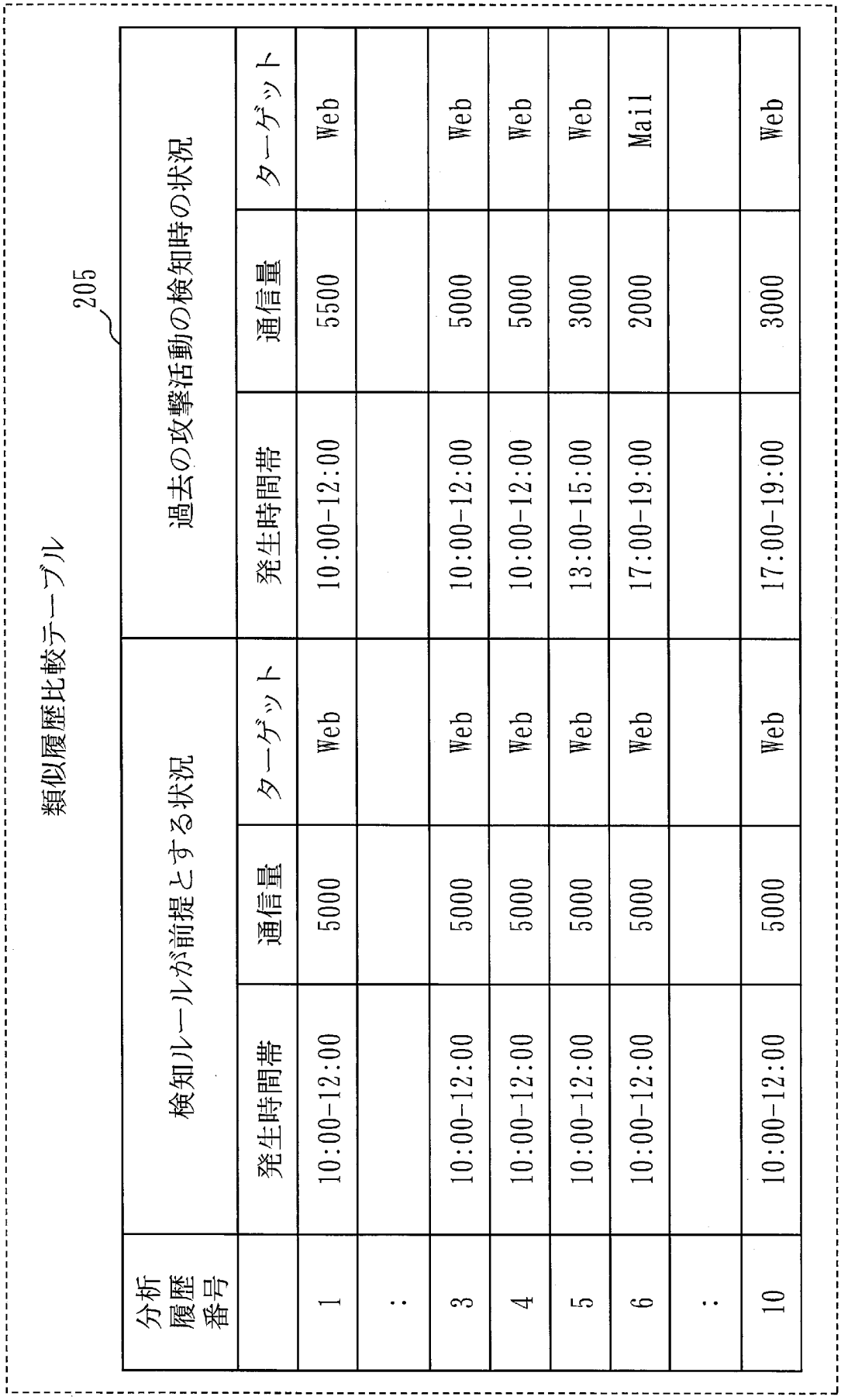
分析履歴テーブル 203

分析履歴番号	警告名	発生時間帯	対応処置	解析情報
1	DoS 攻撃	2017/01/03 10:45	対策要。レポート作成。	通信先：Webサーバー、 通信量：5500アクセス/分
2	ポートスキャン	2017/01/04 13:23	対策不要。	通信先：個人端末
3	DoS 攻撃	2017/01/05 10:05	対策要。客先に通報。	通信先：Webサーバー、 通信量：5000アクセス/分
4	DoS 攻撃	2017/01/05 11:05	対策不要。	通信先：Webサーバー、 通信量：5000アクセス/分
5	DoS 攻撃	2017/01/05 13:05	対策要。レポート作成。	通信先：Webサーバー、 通信量：3000アクセス/分
6	DoS 攻撃	2017/01/14 17:11	対策不要。	通信先：Mailサーバー、 通信量：2000アクセス/分
7	ファイル送信	2017/01/15 12:00	対策要。レポート作成。	通信先：個人端末
8	ポートスキャン	2017/01/15 09:27	対策要。レポート作成。	通信先：個人端末
9	ファイル送信	2017/01/21 15:25	対策不要。	通信先：個人端末
10	DoS 攻撃	2017/01/21 17:30	対策不要。	通信先：Webサーバー、 通信量：3000アクセス/分

[図5]

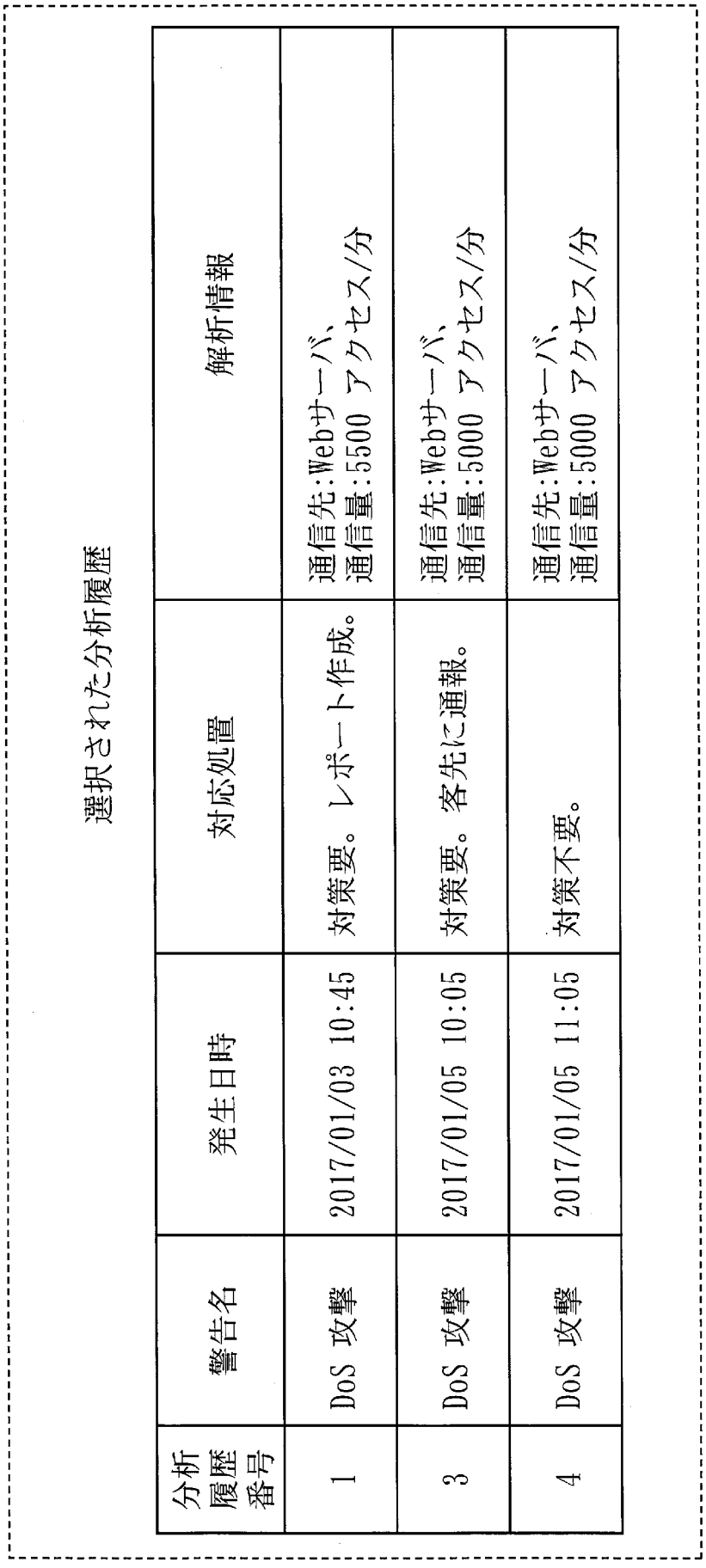

機器管理テーブル
204
IPアドレス
用途
172.18.0.1
Mailサーバー
172.18.0.2
Webサーバー
172.18.0.3
ファイルサーバー
172.18.0.4
ADサーバー
192.168.0.1
個人端末
:
:
192.168.0.200
個人端末

[図6]



分析履歴番号	検知ルールが前提とする状況			過去の攻撃活動の検知時の状況		
	発生時間帯	通信量	ターゲット	発生時間帯	通信量	ターゲット
1	10:00-12:00	5000	Web	10:00-12:00	5500	Web
:						
3	10:00-12:00	5000	Web	10:00-12:00	5000	Web
4	10:00-12:00	5000	Web	10:00-12:00	5000	Web
5	10:00-12:00	5000	Web	13:00-15:00	3000	Web
6	10:00-12:00	5000	Web	17:00-19:00	2000	Mail
:						
10	10:00-12:00	5000	Web	17:00-19:00	3000	Web

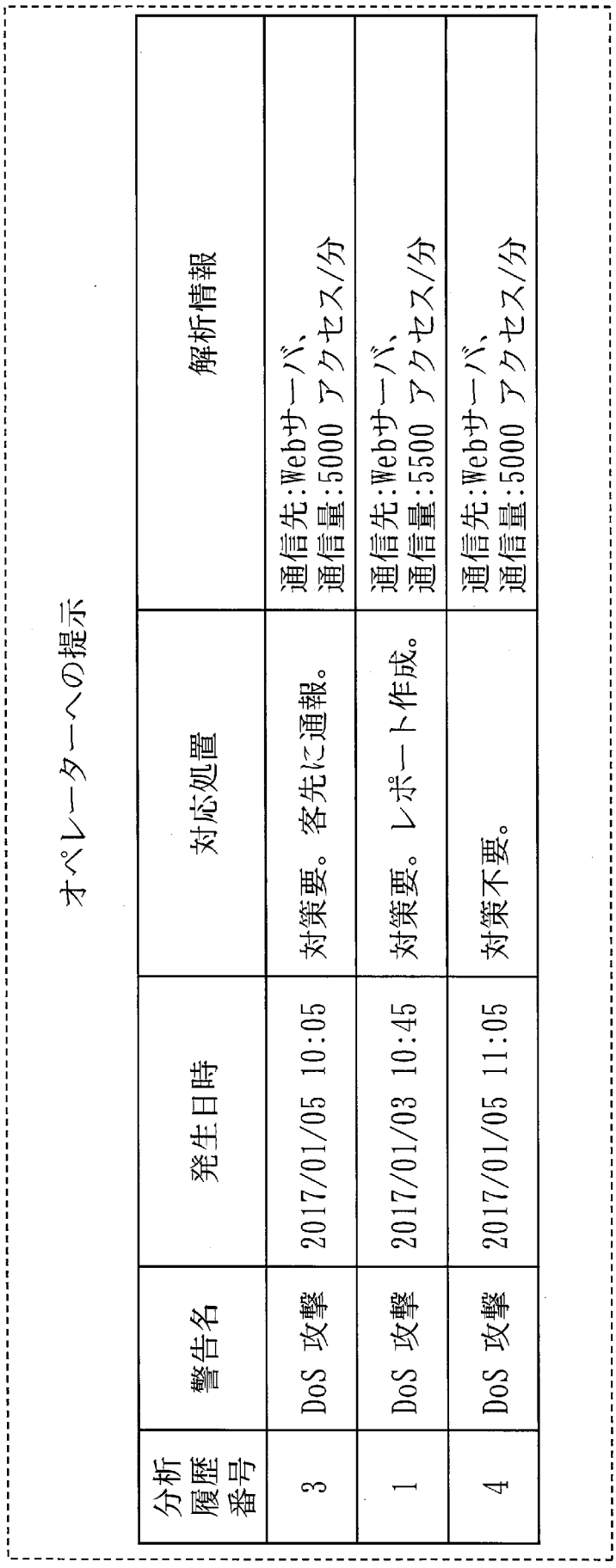
[図7]



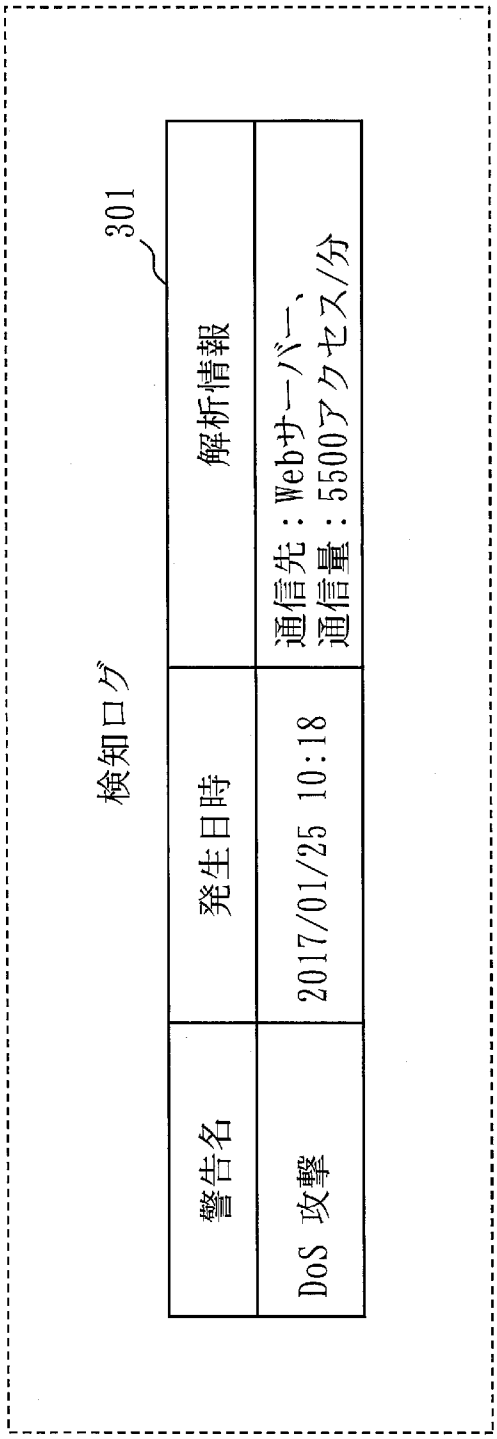
選択された分析履歴

分析履歴番号	警告名	発生日時	対応処置	解析情報
1	DoS 攻撃	2017/01/03 10:45	対策要。レポート作成。	通信先:Webサーバ、 通信量:5500 アクセス/分
3	DoS 攻撃	2017/01/05 10:05	対策要。客先に通報。	通信先:Webサーバ、 通信量:5000 アクセス/分
4	DoS 攻撃	2017/01/05 11:05	対策不要。	通信先:Webサーバ、 通信量:5000 アクセス/分

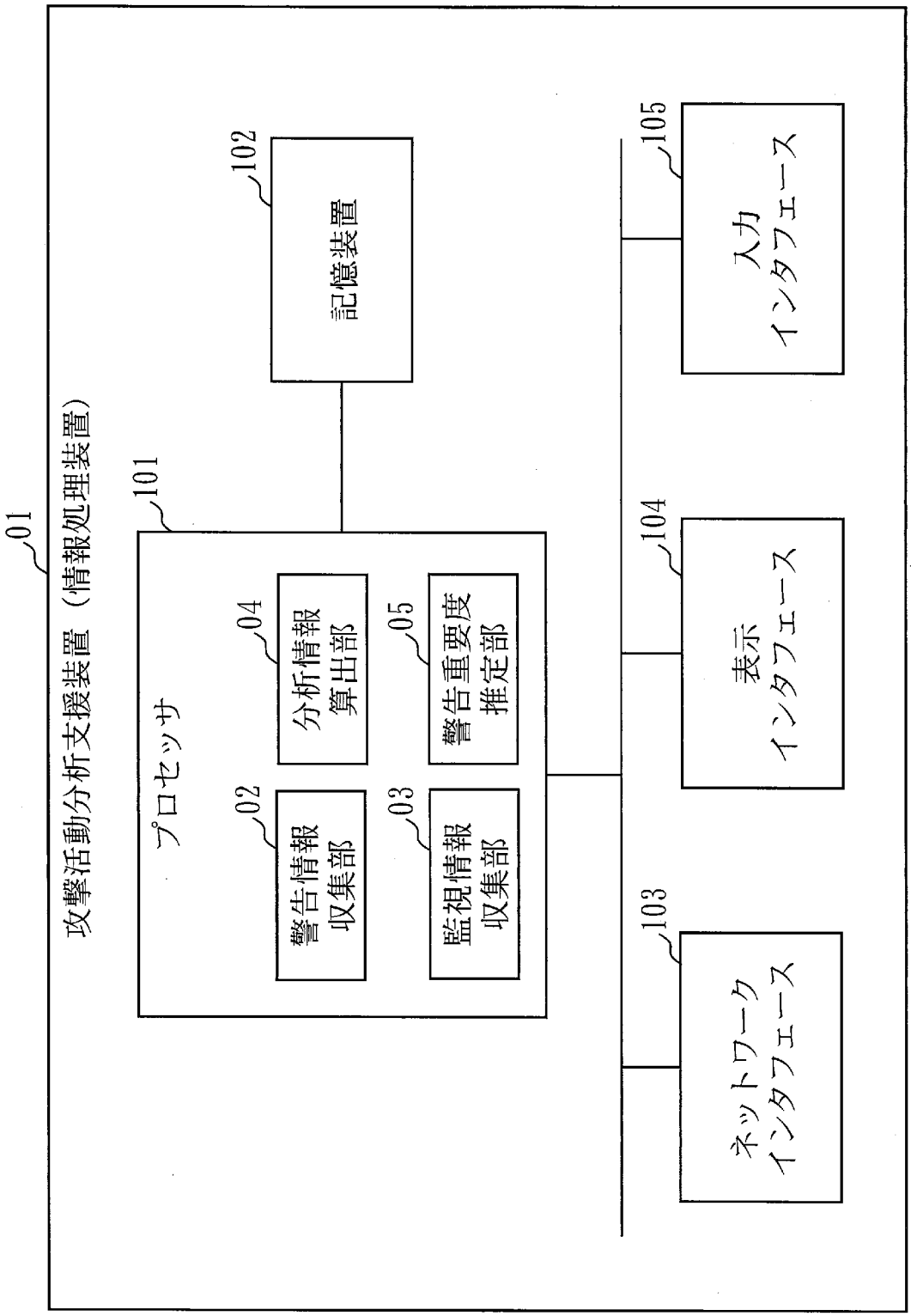
[図8]


オペレーターへの提示
分析履歴番号
警告名
発生日時
対応処置
解析情報
3
DoS 攻撃
2017/01/05 10:05
対策要。客先に通報。
通信先:Webサーバ、
通信量:5000 アクセス/分
1
DoS 攻撃
2017/01/03 10:45
対策要。レポート作成。
通信先:Webサーバ、
通信量:5500 アクセス/分
4
DoS 攻撃
2017/01/05 11:05
対策不要。
通信先:Webサーバ、
通信量:5000 アクセス/分

[図9]


検知ログ
301
警告名
発生日時
解析情報
DoS 攻撃
2017/01/25 10:18
通信先：Webサーバー、
通信量：5500アクセス/分

[図10]


01
攻撃活動分析支援装置（情報処理装置）
101
プロセッサ
02
警告情報収集部
03
監視情報収集部
04
分析情報算出部
05
警告重要度推定部
102
記憶装置
103
ネットワークインタフェース
104
表示インタフェース
105
入力インタフェース

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/043869

A. CLASSIFICATION OF SUBJECT MATTER
Int. Cl. G06F21/55(2013.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int. Cl. G06F21/55

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Published examined utility model applications of Japan 1922-1996
Published unexamined utility model applications of Japan 1971-2018
Registered utility model specifications of Japan 1996-2018
Published registered utility model applications of Japan 1994-2018

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2011-76161 A (NOMURA RESEARCH INSTITUTE, LTD.) 14 April 2011, claim 1, paragraphs [0028]-[0030], [0034], [0066]-[0077], [0108] (Family: none)	1-9
A	WO 2016/147403 A1 (MITSUBISHI ELECTRIC CORP.) 22 September 2016, paragraphs [0014]-[0048], fig. 1-9 (Family: none)	1-9

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

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

Date of the actual completion of the international search	Date of mailing of the international search report
28.02.2018	13.03.2018
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

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

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１７／０４３８６９

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/55(2013.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/55

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１８年
日本国実用新案登録公報	１９９６－２０１８年
日本国登録実用新案公報	１９９４－２０１８年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2011-76161 A (株式会社野村総合研究所) 2011.04.14, 請求項1, [0028]-[0030], [0034], [0066]-[0077], [0108] (ファミリーなし)	1-9
A	WO 2016/147403 A1 (三菱電機株式会社) 2016.09.22, [0014]-[0048], 図 1-9 (ファミリーなし)	1-9

☐　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
２８．０２．２０１８	１３．０３．２０１８

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　１２０６
宮司　卓佳
電話番号　０３－３５８１－１１０１　内線　３５４６