

(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
2017年6月22日(22.06.2017)



(10) 国際公開番号
WO 2017/103974 A1

- (51) 国際特許分類:
G06F 21/55 (2013.01)
- (21) 国際出願番号: PCT/JP2015/084931
- (22) 国際出願日: 2015年12月14日(14.12.2015)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (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: 居城 秀明(IJIRO, Hideaki); 〒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). 河内 清人(KAWAUCHI, Kiyoto); 〒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).
- (74) 代理人: 溝井 章司, 外(MIZOI, Shoji et al.); 〒2470056 神奈川県鎌倉市大船二丁目17番10号 N T A大船ビル3階 溝井国際特許事務所 Kanagawa (JP).
- (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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.

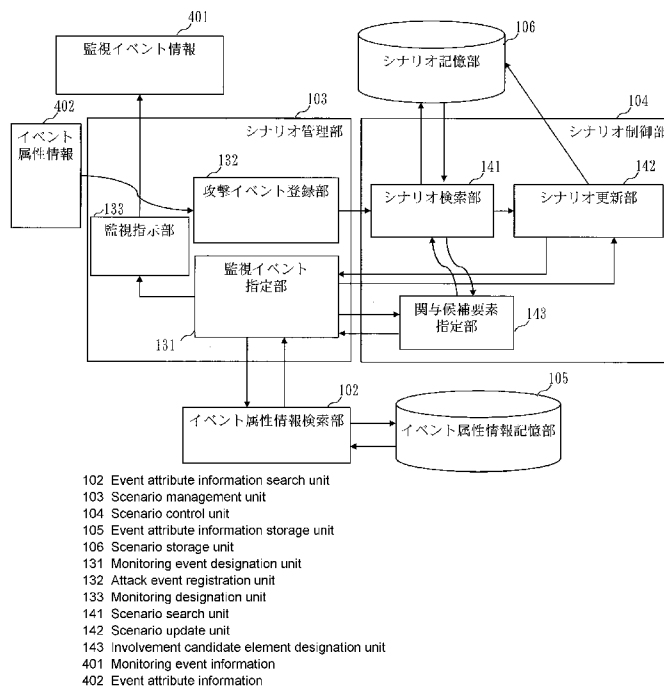
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ユーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,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

(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



(57) Abstract: In the present invention, when an attack event is detected in which an information system including a plurality of system constituent elements is attacked, and if notification is performed of a detection event which is the detected attack event, and an event involvement element which is a system constituent element that was involved in the occurrence of the detection event, a monitoring event designation unit (131) designates, as a monitoring event, an attack event which could occur due the involvement of the event involvement element following the detection event. An involvement candidate element designation unit (143) designates, as an involvement candidate element, a system constituent element(s) among the plurality of system constituent elements which can be involved in the occurrence of the monitoring event besides the event involvement element.

(57) 要約: 監視イベント指定部 (131) は、複数のシステム構成要素が含まれる情報システムを攻撃する攻撃イベントが検知され、検知された攻撃イベントである検知イベントと検知イベントの発生に関与したシステム構成要素であるイベント関与要素とが通知された場合に、検知イベントの次に、イベント関与要素の関与により発生し得る攻撃イベントを監視イベントとして指定する。関与候補要素指定部 (143) は、複数のシステム構成要素のうちイベント関与要素以外に監視イベントの発生に関与し得るシステム構成要素を関与候

補要素として指定する。

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、情報システムへの攻撃を検知する技術に関する。

背景技術

[0002] 情報システムへの攻撃として、例えば標的型攻撃がある。標的型攻撃においては、攻撃者は正規のユーザに成りすまして活動を行うため、正規の活動と攻撃活動とを区別することが難しい。正規の活動と攻撃活動とを正しく区別するためには、攻撃検知のための検知ルールをチューニングすることが必要である。

しかし、従来の統合ログ監視では、攻撃の検知漏れと誤検知とのバランスをとれるように検知ルールをチューニングすることが困難であった。

これに対し、攻撃者が行う活動によって観測されるイベントの推移をシナリオとして定義しておき、シナリオにそったイベントの発生が観測された場合に攻撃が発生したとみなす手法が提案されている（例えば、特許文献1）。

具体的には、特許文献1の手法では、標的型攻撃において発生すると考えられる複数のイベントのそれぞれに対して、攻撃活動定義情報が定義される。攻撃活動定義情報には、イベントの内容やイベントが発生するための事前条件、イベントの発生によって攻撃者が得ると期待される新たな知識や状態を示す達成状態等が定義される。標的型攻撃の検知は、標的型攻撃検知S／W（Software）が、SIEM（Security Information and Event Management）等のセキュリティ機器から送られてくるイベントを受信し、標的型攻撃の確度が高いと判断した場合に管理者へ警報を行う。

警報を行う程の確度に達していなかった場合は、標的型攻撃検知S／Wは

、受信したイベントに対応する攻撃活動定義情報を利用して次に発生するイベントの予測を行う。また、標的型攻撃検知 S/W は、予測したイベントを必要に応じて用い、より詳細な監視が行えるよう S I E M や監視対象ネットワーク上の機器に対して監視設定を変更する。

[0003] 攻撃者の情報システムへの攻撃活動は、攻撃活動定義情報に、攻撃が発生した端末装置の I P (I n t e r n e t P r o t o c o l) アドレスや端末識別番号といった束縛済み変数情報を追記し管理している。これにより、情報システムのシステム構成要素（例えば計算機端末 A）に侵入することで発生した一連の攻撃活動と、他のシステム構成要素（例えば計算機端末 B）に侵入することで発生した一連の攻撃活動をそれぞれ別のシナリオとして管理することができる。

また、次に発生するイベントの予測を行う際も、束縛済み変数情報と併せて条件付きの監視を行うことで、正常なユーザの活動を攻撃活動と誤検知することを防いでいる。

先行技術文献

特許文献

[0004] 特許文献1：国際公開 WO 2 0 1 5 / 0 5 9 7 9 1 号

発明の概要

発明が解決しようとする課題

[0005] しかし、特許文献 1 の手法では、攻撃者が複数のシステム構成要素に侵入し、複数のシステム構成要素から攻撃活動を実施した場合に検知漏れが発生する場合がある。

例えば、攻撃者がある計算機端末 2 台に不正に侵入した場合を想定する。このとき、攻撃者が一方の計算機端末 A からファイルサーバのログインパスワードを取得したことを検知できた場合に、特許文献 1 の手法では攻撃活動定義情報と束縛済み変数情報を用いて、次に攻撃者が計算機端末 A からファイルサーバへログインすることを予測し、計算機端末 A からファイルサーバ

ヘログインを監視することができる。

しかし、このとき、他方の計算機端末Bにも侵入している攻撃者は、計算機端末Aで不正に取得したパスワードを用いて計算機端末Bからファイルサーバに不正にログインすることも可能である。

特許文献1の手法では計算機端末Aからのログインのみを予測し監視しているため、計算機端末Bからのファイルサーバへの攻撃の検知漏れが発生し得る。

このように、特許文献1の手法では、検知された攻撃イベントの発生に関与したシステム構成要素のみを監視対象とするため、他のシステム構成要素を介した攻撃を検知できないという課題がある。

[0006] 本発明は、このような課題を解決することを主な目的としており、検知された攻撃イベントの発生に関与したシステム構成要素以外のシステム構成要素を介した攻撃を検知できるようにすることを主な目的とする。

課題を解決するための手段

[0007] 本発明に係る情報処理装置は、

複数のシステム構成要素が含まれる情報システムを攻撃する攻撃イベントが検知され、検知された攻撃イベントである検知イベントと前記検知イベントの発生に関与したシステム構成要素であるイベント関与要素とが通知された場合に、前記検知イベントの次に、前記イベント関与要素の関与により発生し得る攻撃イベントを監視イベントとして指定する監視イベント指定部と、

前記複数のシステム構成要素のうち前記イベント関与要素以外に前記監視イベントの発生に関与し得るシステム構成要素を関与候補要素として指定する関与候補要素指定部とを有する。

発明の効果

[0008] 本発明によれば、検知された攻撃イベントの発生に関与したシステム構成要素であるイベント関与要素以外に監視イベントの発生に関与し得るシステム構成要素を関与候補要素として指定するため、関与候補要素に対する監視

を行うことで、イベント関与要素以外のシステム構成要素を介した攻撃を検知することができる。

図面の簡単な説明

[0009] [図1]実施の形態1に係るシステム構成例を示す図。

[図2]実施の形態1に係る情報処理装置の機能構成例を示す図。

[図3]実施の形態1に係るシナリオ管理部及びシナリオ制御部の内部構成例を示す図。

[図4]実施の形態1に係る情報処理装置のハードウェア構成例を示す図。

[図5]実施の形態1に係る情報処理方法を示すフローチャート図。

[図6]実施の形態1に係る検知アラート受信後のイベント属性情報の例を示す図。

[図7]実施の形態1に係るシナリオの例を示す図。

[図8]実施の形態1に係る監視イベント情報の例を示す図。

[図9]実施の形態1に係る連携予測条件が記述される監視イベント情報の例を示す図。

[図10]実施の形態1に係る情報処理装置の動作の概要を示すフローチャート図。

[図11]実施の形態1に係る情報処理装置の動作の概要を示すフローチャート図。

[図12]実施の形態1に係るシナリオ管理部及びシナリオ制御部の動作例を示すフローチャート図。

[図13]実施の形態1に係るシナリオ管理部及びシナリオ制御部の動作例を示すフローチャート図。

[図14]実施の形態1に係るシナリオ管理部及びシナリオ制御部の動作例を示すフローチャート図。

[図15]実施の形態1に係るシナリオ管理部及びシナリオ制御部の動作例を示すフローチャート図。

[図16]実施の形態1に係るシナリオ検索部の動作例を示すフローチャート図

。

[図17]実施の形態1に係るシナリオ検索部の動作例を示すフローチャート図

。

[図18]実施の形態1に係るシナリオ検索部の動作例を示すフローチャート図

。

[図19]実施の形態2に係るシナリオ管理部及びシナリオ制御部の内部構成例を示す図。

[図20]実施の形態2に係るシナリオ管理部及びシナリオ制御部の動作例を示すフローチャート図。

[図21]実施の形態2に係るシナリオ管理部及びシナリオ制御部の動作例を示すフローチャート図。

[図22]実施の形態2に係る連携予測IDが記述される監視イベント情報の例を示す図。

[図23]実施の形態2に係るシナリオ制御部の動作例を示すフローチャート図

。

[図24]実施の形態2に係る集約後のイベント属性情報の例を示す図。

[図25]実施の形態3に係るシナリオ管理部及びシナリオ制御部の内部構成例を示す図。

[図26]実施の形態3に係るシナリオ統合除外識別子が記述されるイベント属性情報の例を示す図。

[図27]実施の形態3に係るシナリオ管理部及びシナリオ制御部の動作例を示すフローチャート図。

[図28]実施の形態3に係るシナリオ管理部及びシナリオ制御部の動作例を示すフローチャート図。

[図29]実施の形態4に係るシナリオ管理部及びシナリオ制御部の内部構成例を示す図。

[図30]実施の形態4に係るシナリオ管理部及びシナリオ制御部の動作例を示すフローチャート図。

[図31]実施の形態4に係るシナリオ管理部及びシナリオ制御部の動作例を示すフローチャート図。

[図32]実施の形態1に係る検知アラート受信前のイベント属性情報の例を示す図。

発明を実施するための形態

[0010] 実施の形態1.

構成の説明

図1は、本実施の形態に係るシステム構成例を示す。

本実施の形態では、情報システム200と監視装置500と情報処理装置100がネットワーク600で接続されている。

情報システム200には、複数のシステム構成要素300が含まれる。

システム構成要素300には、端末装置、サーバ装置といった計算機要素が含まれる。

また、システム構成要素300には、端末装置を利用するユーザ、情報システム200を管理するシステム管理者といった人的要素が含まれる。

更に、システム構成要素300には、ファイル、テーブル、関数、変数、定数といったデータ要素が含まれる。

また、情報システム200ではイベントが発生し、監視装置500により情報システム200への攻撃又は攻撃の兆候となるイベント（以下、攻撃イベントという）が検知される。

図1では、監視装置500は情報システム200外に配置されているが、監視装置500が情報システム200内に配置されていてもよい。

監視装置500は、情報システム200を監視する。

なお、監視装置500における「監視」とは、情報システム200への攻撃の進展度合いを解析するためにイベントの発生有無を定期的又は不定期にログ検索等により調査することである。

監視装置500は、例えばS I E M等のセキュリティ機器である。

監視装置500によって検知された攻撃イベントは、検知アラート400

として、情報処理装置１００に通知される。

[0011] 図２は、情報処理装置１００の機能構成例を示す。

情報処理装置１００は、アラート受信部１０１、イベント属性情報検索部１０２、シナリオ管理部１０３、シナリオ制御部１０４、イベント属性情報記憶部１０５、シナリオ記憶部１０６が含まれる。

また、図３に示すように、シナリオ管理部１０３には、監視イベント指定部１３１、攻撃イベント登録部１３２、監視指示部１３３が含まれ、シナリオ制御部１０４には、シナリオ検索部１４１、シナリオ更新部１４２、関与候補要素指定部１４３が含まれる。

[0012] 情報処理装置１００には、図４に示すように、プロセッサ９０１、記憶装置９０２、レシーバー９０３及びトランスミッター９０４というハードウェアが含まれる。

記憶装置９０２には、アラート受信部１０１、イベント属性情報検索部１０２、シナリオ管理部１０３、シナリオ制御部１０４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９０１がこれらプログラムを実行して、後述するアラート受信部１０１、イベント属性情報検索部１０２、シナリオ管理部１０３、シナリオ制御部１０４の動作を行う。

図４では、プロセッサ９０１がアラート受信部１０１、イベント属性情報検索部１０２、シナリオ管理部１０３、シナリオ制御部１０４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。

また、イベント属性情報記憶部１０５及びシナリオ記憶部１０６は、記憶装置９０２により実現される。

レシーバー９０３及びトランスミッター９０４は、監視装置５００との間で通信を行う。

[0013] ***動作の説明***

まず、本実施の形態に係る情報処理装置１００の動作の詳細を説明する前に、図５を参照して、情報処理装置１００により行われる動作の概要を説明

する。

なお、図5に示される手順は、情報処理方法及び情報処理プログラムの例に相当する。

[0014] 情報システム200を攻撃する攻撃イベントが監視装置500で検知された場合に、ステップS11において、アラート受信部101が、レシーバー903を介して監視装置500から検知アラート400を受信する。

検知アラート400では、監視装置500で検知された攻撃イベント（以下、検知イベントという）と、検知イベントの発生に関与したシステム構成要素300（以下、イベント関与要素という）とが通知される。

なお、「関与」とは、検知イベントの発生主体になること、検知イベントの客体となること、検知イベントでパラメータとして利用されること等を含む意味である。従って、「検知イベントの発生に関与したシステム構成要素300」は、検知イベントの発生主体のシステム構成要素300、検知イベントの客体となるシステム構成要素300、検知イベントでパラメータとして利用されているシステム構成要素300等を意味する。

[0015] 次に、ステップS12において、シナリオ管理部103内の監視イベント指定部131が、検知イベントの次に、イベント関与要素の関与により発生し得る攻撃イベントを監視イベントとして指定する（監視イベント指定処理）。

より具体的には、監視イベント指定部131は、検知アラート400で通知された検知イベントとイベント関与要素とに基づき、シナリオ検索部141を用いて、シナリオ記憶部106内のシナリオを検索して、監視イベントを指定する。

[0016] シナリオは、システム構成要素別にシナリオ記憶部106で記憶されている。

シナリオ記憶部106は、監視装置500で検知された攻撃イベントのイベント属性情報を、検知された攻撃イベントの発生に関与したシステム構成要素と対応付けて、シナリオとして記憶する。

イベント属性情報は、攻撃イベントの属性値が示される情報であり、イベント属性情報記憶部 105 で記憶されている。

イベント属性情報記憶部 105 は、複数の攻撃イベントについて、攻撃イベントごとに、イベント属性情報を記憶している。

なお、シナリオ及びイベント属性情報の詳細は後述する。

[0017] 次に、ステップ S 13 において、シナリオ制御部 104 内の関与候補要素指定部 143 が、監視イベントと関連する攻撃イベントが発生しているシステム構成要素を関与候補要素として指定する（関与候補要素指定処理）。

関与候補要素は、複数のシステム構成要素のうちイベント関与要素以外に監視イベントの発生に関与し得るシステム構成要素である。

[0018] 次に、ステップ S 14 において、シナリオ制御部 104 内のシナリオ更新部 114 がシナリオを更新する。

より具体的には、シナリオ更新部 114 は、監視イベントのイベント属性情報（以下、監視イベント情報という）を、イベント関与要素のシナリオと関与候補要素のシナリオに追加する。

なお、シナリオ更新部 114 は、監視イベント情報のイベント関与要素のシナリオへの追加は、ステップ S 12 とステップ S 13 との間で行うようにしてもよい。

[0019] 最後に、シナリオ管理部 103 内の監視指示部 133 が、監視装置 500 に、イベント関与要素での監視イベントの監視と関与候補要素での監視イベントの監視を指示する。

監視装置 500 では、監視指示部 133 からの指示に基づき、イベント関与要素及び関与候補要素について、定期的又は不定期にログを検索することで監視イベントが発生したか否かを判定する。

[0020] 次に、本実施の形態に係る情報処理装置 100 の動作の詳細を説明する。

[0021] イベント属性情報記憶部 105 は、複数の攻撃イベントについて、攻撃イベントごとに、イベント属性情報を記憶する。

[0022] 図 6 及び図 32 は、イベント属性情報 8 の例である。

図6は検知アラート受信後のイベント属性情報8の例であり、図32は検知アラート受信前のイベント属性情報の例である。

以下、図6を参照してイベント属性情報8の詳細を説明する。

図6に示すように、イベント属性情報8は、事前条件9、イベント10、達成状態11、束縛済み変数情報12で構成されている。

事前条件9には、攻撃イベントが発生するための前提条件が述語論理の形式で記述されている。

つまり、事前条件9には、攻撃イベントが観測される前の攻撃の進展段階（イベント前段階）が記述されている。

例えば、図6の符号13で示す述語論理「login(A, H)」は、攻撃イベントの発生のための事前条件として、「AがHにログインしている」状態が必要であることを表している。なお、符号13で示される「A」及び「H」は変数であり、検知アラート400から得られた具体的な値などは束縛済み変数情報12の欄に保持される。

イベント10は、情報システム200に対する攻撃が行われる過程において情報システム200で観測される攻撃イベントを表す。

イベント10には、イベント発生源14、イベント種別15、イベントパラメータ16が含まれる。

イベント発生源14は、イベント属性情報8が対象とする攻撃イベントのイベント発生源を示している。

符号17は、イベント発生源として許される値を示しており、図6の例では、イベント発生源14が変数Hによって事前条件13と関連付けられている（「\$H」の冒頭にあるドルマーク（\$）は、Hが変数であることを示している）。

イベント種別15は、イベント属性情報8が対象としている攻撃イベントの種別を示す。

具体的には、イベント種別15は、符号18のように指定される。

イベント種別15の具体値（符号18）は、イベント種別情報ともいう。

イベントパラメータ 16 は、イベントのパラメータを示す。

イベントパラメータ 16 では、イベント属性情報 8 が対象とする値が指定されている。

図 6 の例では、符号 19 で、「USER」という名称のパラメータが符号 13 で示されている変数 A と同じ値をとることが求められている。

達成状態 11 は、イベント属性情報 8 の符号 14 ~ 16 の項目に合致する攻撃イベントが発生した時に、攻撃者が達成した状態を述語論理で示している。

つまり、達成状態 11 には、符号 14 ~ 16 の項目に合致する攻撃イベントが検知された後の攻撃の進展段階（イベント後段階）が記述されている。

達成状態 11 は、進展状態ともいう。

図 6 の例では、符号 20 の「hasSecret (A, H)」は、「ユーザ A がホスト H の機密情報を入手した」段階であることを示している。

前述したように検知アラートの受信前、すなわち、イベント属性情報記憶部 105 で記憶されているイベント属性情報では、図 32 のように、束縛済み変数情報 12 には、値が記述されていない（束縛済み変数情報 12 は空欄である）。

アラート受信部 101 が検知アラート 400 を受信した際に、アラート受信部 101 が、検知アラート 400 に記述されている変数の値を束縛済み変数情報 12 に追記し、図 6 のイベント属性情報 8 が得られる。

[0023] 検知アラート 400 では、図 6 のイベント属性情報 8 と同様に、イベント発生源、イベント種別、イベントパラメータが通知される。

図 6 のイベント属性情報 8 では、イベント発生源 17、イベントパラメータ 19 の各変数の値は特定されていないが、検知アラート 400 では、イベント発生源、イベントパラメータの各変数の値が特定されている。

図 6 は、アラート受信部 101 が、変数「A」の具体値として「USER 1」が記述され、変数「H」の具体値として「H__1」が記述されている検知アラート 400 を受信した場合に生成される束縛済み変数情報 12 を表し

ている。

つまり、図6の例では、アラート受信部101は、変数「A」の具体値である「USER1」を束縛済み変数情報12の変数名「A」に対する束縛値に記述し、変数「H」の具体値である「H__1」を束縛済み変数情報12の変数名「H」に対する束縛値に記述している。

[0024] 以上述べたイベント属性情報8は、標的型攻撃で発生すると考えられる複数の攻撃イベントに対して予め定義されており、イベント属性情報記憶部105内に検索可能な状態で格納されている。

なお、束縛済み変数情報12の欄に記載されている束縛値である「USER1」、「H__1」は、情報システム200に含まれるシステム構成要素300である。

[0025] シナリオ記憶部106は、検知アラート400が受信される度に、検知アラート400で通知された検知イベントのイベント属性情報を、検知アラート400で通知されたイベント関与要素と対応付けて、シナリオとして記憶する。

つまり、シナリオは、システム構成要素300別にグルーピングされた、検知イベントのイベント属性情報の集合である。

[0026] 図7は、シナリオの例を示す。図7では、シナリオ記憶部106に、シナリオAとシナリオBとが記憶されている例を示す。

シナリオAについては、イベント種別が「ANOMALOUS__FILE__ACCESS」であるイベント属性情報8とイベント種別が「SEND__LARGE__FILES」であるイベント属性情報8とが格納されている。

これらのイベント属性情報8は、ともに変数Aの束縛値が「USER1」であり、変数Hの束縛値が「H__1」であるため、攻撃者による一連の攻撃活動として同じシナリオに格納されている。

一方で、シナリオBにはイベント種別が「ANOMALOUS__FILE__ACCESS」であるイベント属性情報8が格納されている。

イベント種別が「ANOMALOUS__FILE__ACCESS」である

イベント属性情報 8 はシナリオ A にも格納されているが、格納されている束縛済み変数情報 1 2 が異なっているため、異なるシナリオ B に格納されている。

[0027] アラート受信部 1 0 1 は、情報システム 2 0 0 を攻撃する攻撃イベントが監視装置 5 0 0 で検知された場合に、レシーバー 9 0 3 を介して、監視装置 5 0 0 から検知アラート 4 0 0 を受信する。

検知アラート 4 0 0 には、情報システム 2 0 0 への攻撃の一環として送信された可能性のあるパケットの送信元の識別子（IP アドレス及びポート番号等）、送信先の識別子（IP アドレス及びポート番号等）が含まれる。

更に、検知アラート 4 0 0 には、TCP（Transmission Control

Protocol）やUDP（User Datagram Protocol）などのプロトコル、検知された攻撃イベント（ログイン、ポートスキャン等）のイベント種別情報が含まれている。

前述したように、検知アラート 4 0 0 で通知された、検知された攻撃イベントが検知イベントであり、攻撃の一環として送信された可能性のあるパケットの送信元のシステム構成要素及び送信先のシステム構成要素は、イベント関連要素である。

検知アラート 4 0 0 の一例として、IDS（Intrusion Detection

System）アラートがある。

また、アラート受信部 1 0 1 は、検知アラート 4 0 0 で通知された検知イベントのイベント種別情報をイベント属性情報検索部 1 0 2 に出力し、検知イベントに対応するイベント属性情報 8 をイベント属性情報検索部 1 0 2 を介してイベント属性情報記憶部 1 0 5 から受信する。

また、アラート受信部 1 0 1 は、検知アラート 4 0 0 から得られた変数の具体値を、イベント属性情報記憶部 1 0 5 から受信した検知イベントのイベント属性情報 4 0 2 の束縛済み変数情報 1 2 に記述する。

また、アラート受信部 101 は、変数の具体値が束縛済み変数情報 12 に記述された検知イベントのイベント属性情報 402 をシナリオ管理部 103 内の攻撃イベント登録部 132 に出力する。

[0028] イベント属性情報検索部 102 は、アラート受信部 101 から検知イベントのイベント種別情報を受信し、受信したイベント種別情報に対応するイベント属性情報 402 を、イベント属性情報記憶部 105 から受信する。

そして、イベント属性情報検索部 102 は、イベント属性情報記憶部 105 から受信したイベント属性情報 402 を、アラート受信部 101 に出力する。

[0029] シナリオ管理部 103 において、攻撃イベント登録部 132 は、検知イベントのイベント属性情報 402 をアラート受信部 101 から受信する。

そして、攻撃イベント登録部 132 は、受信した検知イベントのイベント属性情報 402 をシナリオ制御部 104 内のシナリオ検索部 141 に送信する。

シナリオ検索部 141 は、後述するように、検知イベントのイベント属性情報 402 をシナリオ記憶部 106 内のシナリオに追加する。

[0030] 監視イベント指定部 131 は、イベント関与要素が関与して検知イベントの次に発生し得る攻撃イベントの候補を監視イベントとして指定する。

より具体的には、監視イベント指定部 131 は、シナリオ更新部 142 から検知イベントのイベント属性情報を受信し、受信した検知イベントのイベント属性情報から達成状態の述語論理を抽出する。そして、監視イベント指定部 131 は、検知イベントのイベント属性情報から抽出した述語論理が事前条件に記述されているイベント属性情報を、イベント属性情報検索部 102 を介して、イベント属性情報記憶部 105 から取得する。該当するイベント属性情報が複数ある場合は、監視イベント指定部 131 は、複数のイベント属性情報を取得する。

次に、監視イベント指定部 131 は、取得したイベント属性情報がシナリオに追加されているか否か、更に、取得したイベント属性情報の事前条件が

、検知イベントのイベント属性情報の達成状態によって満たされているか否かを確認する。

取得したイベント属性情報がシナリオに未だ追加されておらず、かつ、取得したイベント属性情報の事前条件が、検知イベントのイベント属性情報の達成状態によって満たされている場合に、取得したイベント属性情報が対象としている攻撃イベントを監視イベントに指定する。

更に、監視イベント指定部 131 は、監視イベントのイベント属性情報の束縛済み変数情報 12 に、検知イベントのイベント属性情報の束縛済み変数情報 12 の具体値を格納する。

以降、束縛済み変数情報 12 に具体値が記述された後の監視イベントのイベント属性情報を、監視イベント情報という。

監視イベント情報には、イベント関与要素のシナリオに追加する監視イベント情報と、関与候補要素のシナリオに追加する監視イベント情報の二種類がある。以下では、イベント関与要素のシナリオに追加する監視イベント情報をイベント関与要素の監視イベント情報といい、関与候補要素のシナリオに追加する監視イベント情報を関与候補要素の監視イベント情報という。

監視イベント指定部 131 は、イベント関与要素の監視イベント情報を関与候補要素指定部 143 に送信する。

また、監視イベント指定部 131 は、関与候補要素指定部 143 から関与候補要素の監視イベント情報と関与候補要素のシナリオを受信する。

また、監視イベント指定部 131 は、関与候補要素指定部 143 から受信した関与候補要素の監視イベント情報と関与候補要素のシナリオをシナリオ更新部 142 に送信する。

シナリオ更新部 142 は、関与候補要素のシナリオを更新する。具体的には、シナリオ更新部 142 は、関与候補要素のシナリオに関与候補要素の監視イベント情報を追加する。

なお、監視イベント指定部 131 により行われる処理は、監視イベント指定処理という。

[0031] 図8は監視イベント情報27の例を示す。

図8に示すように、監視イベント情報27は、図6のイベント属性情報8に含まれる項目に加え、符号28に示される「状態」属性が含まれる。

符号29に示されるように、「状態」属性は「監視中」となっており、検知アラート400で通知された検知イベントのイベント属性情報と区別される。

なお、イベント関与要素の監視イベント情報27と、関与候補要素の監視イベント情報27では、束縛済み変数情報の束縛値が異なっている。

つまり、イベント関与要素の監視イベント情報27の束縛済み変数情報には、検知アラート400に記述されている具体値が記述されている。

一方、関与候補要素の監視イベント情報27の束縛済み変数情報には、関与候補要素のシナリオ内のイベント属性情報の束縛済み変数情報の束縛値が記述されている。

[0032] 監視指示部133は、監視装置500に、イベント関与要素での監視イベントの監視と関与候補要素での監視イベントの監視を指示する。

より具体的には、監視指示部133は、監視イベント指定部131から、イベント関与要素の監視イベント情報27と関与候補要素の監視イベント情報27を取得し、取得したイベント関与要素の監視イベント情報27と関与候補要素の監視イベント情報27をトランスミッター904を介して監視装置500に送信する。

[0033] シナリオ制御部104において、シナリオ検索部141は、攻撃イベント登録部132から検知イベントのイベント属性情報402を取得し、イベント関与要素のシナリオをシナリオ記憶部106から取得する。また、シナリオ検索部141は、検知イベントのイベント属性情報402と、イベント関与要素のシナリオをシナリオ更新部142に出力する。

更に、シナリオ検索部141は、関与候補要素指定部143からイベント関与要素の監視イベント情報27を取得し、イベント関与要素の監視イベント情報27に基づき、関与候補要素のシナリオをシナリオ記憶部106から

取得する。また、シナリオ検索部 141 は、関与候補要素のシナリオを関与候補要素指定部 143 に出力する。

[0034] シナリオ更新部 142 は、シナリオ検索部 141 から検知イベントのイベント属性情報 402 とイベント関与要素のシナリオを取得した場合に、検知イベントのイベント属性情報 402 をイベント関与要素のシナリオに追加して、イベント関与要素のシナリオを更新する。そして、シナリオ更新部 142 は、更新後のイベント関与要素のシナリオをシナリオ記憶部 106 に格納する。

また、シナリオ更新部 142 はシナリオ検索部 141 から検知イベントのイベント属性情報 402 のみを受信した場合は、イベント関与要素のシナリオを新規に生成する。そして、シナリオ更新部 142 は新規に生成したイベント関与要素のシナリオに検知イベントのイベント属性情報 402 を追加し、イベント関与要素のシナリオをシナリオ記憶部 106 に格納する。

更に、シナリオ更新部 142 は、監視イベント指定部 131 からイベント関与要素の監視イベント情報 27 とイベント関与要素のシナリオを取得した場合に、イベント関与要素の監視イベント情報 27 をイベント関与要素のシナリオに追加して、イベント関与要素のシナリオを更新する。そして、シナリオ更新部 142 は、更新後のイベント関与要素のシナリオをシナリオ記憶部 106 に格納する。

また、シナリオ更新部 142 は、監視イベント指定部 131 から関与候補要素の監視イベント情報 27 と関与候補要素のシナリオを取得した場合に、関与候補要素の監視イベント情報 27 を関与候補要素のシナリオに追加して、関与候補要素のシナリオを更新する。そして、シナリオ更新部 142 は、更新後の関与候補要素のシナリオをシナリオ記憶部 106 に格納する。

[0035] 関与候補要素指定部 143 は、監視イベント指定部 113 からイベント関与要素の監視イベント情報 27 を取得し、取得したイベント関与要素の監視イベント 27 に連携予測条件が含まれているかどうかを確認する。イベント関与要素の監視イベント情報 27 に連携予測条件が含まれていた場合は、関

与候補要素指定部 143 は、シナリオ検索部 141 にイベント関与要素の監視イベント情報 27 を送信する。そして、関与候補要素指定部 143 は、シナリオ検索部 141 から連携予測条件を達成状態に持つイベント属性情報を含むシナリオを関与候補要素のシナリオとして取得する。

また、関与候補要素指定部 143 は、取得した関与候補要素のシナリオ内の、連携予測条件を達成状態に持つイベント属性情報の束縛済み変数情報の束縛値で、イベント関与要素の監視イベント情報 27 の束縛済み変数情報を書き換えて、関与候補要素の監視イベント情報 27 を得る。

そして、関与候補要素指定部 143 は、関与候補要素の監視イベント情報 27 と関与候補要素のシナリオを、監視イベント指定部 131 に送信する。

なお、関与候補要素指定部 143 により行われる処理は、関与候補要素指定処理という。

[0036] 図 9 は連携予測条件が含まれている監視イベント情報 27 の例を示す。

図 9 の監視イベント情報 27 には連携予測条件 30 として、符号 31 に示される「`suspiciousConnection (H)`」が記述されている。連携予測条件 30 は、監視イベントに関連する攻撃イベントの属性値である。

前述したように、関与候補要素指定部 143 は、イベント関与要素の監視イベント情報 27 に連携予測条件 30 が含まれる場合は、イベント関与要素の監視イベント情報 27 をシナリオ検索部 141 に送信する。そして、シナリオ検索部 141 は、達成状態に連携予測条件 30 の述語論理が記述されているイベント属性情報が含まれるシナリオを関与候補要素のシナリオとして抽出する。図 9 の例では、シナリオ検索部 141 は、達成条件に「`suspiciousConnection (H)`」が記述されているイベント属性情報が含まれるシナリオを関与候補要素のシナリオとして抽出する。

また、前述したように、関与候補要素指定部 143 は、関与候補要素のシナリオ内のイベント属性情報のうち、連携予測条件 30 と同じ述語論理が達成状態に記述されているイベント属性情報の束縛済み変数情報の束縛値を用

いて、関与候補要素の監視イベント情報 27 を生成する。図 9 の例では、関与候補要素指定部 143 は、達成条件に「`suspiciousConnection (H)`」が記述されているイベント属性情報の束縛済み変数情報の束縛値を用いて、関与候補要素の監視イベント情報 27 を生成する。

[0037] 次に、本実施の形態に係る情報処理装置 100 の動作を、図 10 及び図 11 を参照して説明する。

図 10 及び図 11 は、本実施の形態に係る情報処理装置 100 の全体の処理の流れを示すフローチャートである。

[0038] まず、ステップ S101 において、アラート受信部 101 が検知アラート 400 を受信する。

検知アラート 400 は、前述のとおり、監視装置 500 から送信される警告メッセージである。

次に、ステップ S102 において、アラート受信部 101 は、検知アラート 400 のイベント種別情報（例えば、`ANOMALOUS__FILE__ACCESS`）をイベント属性情報検索部 102 に入力する。

次に、ステップ S103 において、イベント属性情報検索部 102 がイベント種別情報に該当するイベント属性情報をイベント属性情報記憶部 105 から取得し、アラート受信部 101 に入力する。

具体的には、イベント属性情報検索部 102 は、イベント種別情報のイベント種別と同じイベント種別が記述されているイベント属性情報を取得する。

次に、ステップ S104 において、アラート受信部 101 はイベント属性情報の束縛済み変数情報に具体値を代入する。具体的には、アラート受信部 101 は、検知アラート 400 から得られたイベント発生源の具体値、イベントパラメータの具体値を、イベント属性情報検索部 102 から得られたイベント属性情報の束縛済み変数情報に代入する。

[0039] 次に、ステップ S105 において、アラート受信部 101 は束縛済み変数情報に具体値が記述されたイベント属性情報をシナリオ管理部 103 に入力

する。

次に、ステップS 1 0 6において、シナリオ管理部1 0 3はシナリオ制御部1 0 4を用いて、シナリオ記憶部1 0 6内のシナリオの更新またはシナリオの生成を行う。

次に、ステップS 1 0 7において、シナリオ管理部1 0 3はシナリオ制御部1 0 4及びイベント属性情報検索部1 0 2を用いて監視イベントを指定し、監視イベント情報4 0 1を生成する。

次に、ステップS 1 0 8において、シナリオ管理部1 0 3は監視イベント情報4 0 1を監視装置5 0 0に送信する。

[0040] 次に、図3に示した、情報処理装置1 0 0におけるシナリオ管理部1 0 3及びシナリオ制御部1 0 4の詳細な構成を用いて、ステップS 1 0 5～S 1 0 8の動作の詳細を説明する。

動作の流れは、図1 2、図1 3、図1 4及び図1 5を参照して説明する。

図1 2、図1 3、図1 4及び図1 5は、本実施の形態に係る情報処理装置1 0 0におけるシナリオ管理部1 0 3及びシナリオ制御部1 0 4の詳細な構成の動作の流れを示すフローチャートである。

図1 2、図1 3、図1 4及び図1 5では、ステップS 2 0 1がステップS 1 0 5に、ステップS 2 0 2～S 2 0 6がステップS 1 0 6に、ステップS 2 0 7～S 2 1 7がステップS 1 0 7に、ステップS 2 1 8がステップS 1 0 8に対応している。

[0041] まず、ステップS 2 0 1において、攻撃イベント登録部1 3 2は、束縛済み変数情報に具体値が記述されたイベント属性情報をアラート受信部1 0 1から受信する。

次に、ステップS 2 0 2において、攻撃イベント登録部1 3 2は、受信したイベント属性情報をシナリオ検索部1 4 1に入力する。

次に、ステップS 2 0 3において、シナリオ検索部1 4 1はシナリオ記憶部1 0 6から条件に合ったシナリオを検索し、検索により得られたシナリオをシナリオ更新部1 4 2に出力する。

具体的な処理の流れは、図 1 6 及び図 1 7 を参照して説明する。

図 1 6 及び図 1 7 は、シナリオ検索部 1 4 1 が攻撃イベント登録部 1 3 2 からイベント属性情報を受信した場合に、シナリオ記憶部 1 0 6 から条件に合ったシナリオを取得する動作の流れを説明したフローチャートである。

[0042] まず、ステップ S 3 0 1 において、シナリオ検索部 1 4 1 はイベント属性情報を攻撃イベント登録部 1 3 2 から受信する。

次に、ステップ S 3 0 2 において、シナリオ検索部 1 4 1 は、受信したイベント属性情報とイベント種別が共通する監視イベント情報が含まれるシナリオを、シナリオ記憶部 1 0 6 から検索する。

次に、ステップ S 3 0 3 において、ステップ S 3 0 2 の結果、シナリオ検索部 1 4 1 がシナリオを取得したかどうかで処理が分かれる。シナリオ検索部 1 4 1 がシナリオを取得した場合は S 3 0 4 が実施される。一方、シナリオ検索部 1 4 1 がシナリオを取得しない場合は S 3 0 6 が実施される。

[0043] ステップ S 3 0 4 では、シナリオ検索部 1 4 1 は、S 3 0 2 で得られたシナリオに含まれる監視イベント情報の束縛済み変数情報と、受信したイベント属性情報の束縛済み変数情報を比較する。

次に、ステップ S 3 0 5 において、シナリオ検索部 1 4 1 は、受信したイベント属性情報と束縛済み変数情報が共通する監視イベント情報が含まれるシナリオをシナリオ更新部 1 4 2 に出力し、処理を終了する。

ステップ S 3 0 6 では、シナリオ検索部 1 4 1 は、受信したイベント属性情報に記述されている事前条件の述語論理と同じ述語論理が達成状態に記述されるイベント属性情報が含まれるシナリオを、シナリオ記憶部 1 0 6 から検索する。

次に、ステップ S 3 0 7 において、S 3 0 6 の結果、シナリオ検索部 1 4 1 がシナリオを取得したかどうかで処理が分かれる。シナリオ検索部 1 4 1 がシナリオを取得した場合は S 3 0 8 が実施される。一方、シナリオ検索部 1 4 1 がシナリオを取得しない場合は処理が終了する。

ステップ S 3 0 8 では、シナリオ検索部 1 4 1 は、S 3 0 6 で得られたシ

ナリオに含まれる該当するイベント属性情報と、受信したイベント属性情報の束縛済み変数情報を比較する。

次に、ステップS 3 0 9において、シナリオ検索部1 4 1は、受信したイベント属性情報と束縛済み変数情報が共通するイベント属性情報が含まれるシナリオをシナリオ更新部1 4 2に出力し、処理を終了する。

[0044] 次に、図1 2のステップS 2 0 4において、S 2 0 3においてシナリオ検索部1 4 1がシナリオ記憶部1 0 6からシナリオを取得できたかどうかによって処理が分かれる。シナリオ検索部1 4 1がシナリオを取得できた場合はS 2 0 5が実施され、シナリオ検索部1 4 1がシナリオを取得できない場合はS 2 0 6が実施される。

ステップS 2 0 5では、シナリオ更新部1 4 2がシナリオを更新する。より具体的には、シナリオ検索部1 4 1が、取得したシナリオ及びステップS 2 0 1で受信したイベント属性情報をシナリオ更新部1 4 2に入力し、シナリオ更新部1 4 2が、入力されたイベント属性情報を入力されたシナリオに追加する。このとき、追加するイベント属性情報と同じイベント種別情報をもつ監視イベント情報がシナリオに含まれている場合は、監視イベント情報を削除し、入力されたイベント属性情報をシナリオに追加する。そして、シナリオ更新部1 4 2は、イベント属性情報が追加されたシナリオでシナリオ記憶部1 0 6のシナリオを更新する。

ステップS 2 0 6では、シナリオ更新部1 4 2がシナリオを生成し、入力されたイベント属性情報をシナリオに追加する。より具体的には、シナリオ検索部1 4 1が、ステップS 2 0 1で受信されたイベント属性情報をシナリオ更新部1 4 2に入力し、シナリオ更新部1 4 2がシナリオを新規に生成し、入力されたイベント属性情報を生成したシナリオに追加する。そして、シナリオ更新部1 4 2は、イベント属性情報が追加されたシナリオをシナリオ記憶部1 0 6に登録する。

[0045] ステップS 2 0 7では、シナリオ更新部1 4 2は、ステップS 2 0 1で受信された検知イベントのイベント属性情報を監視イベント指定部1 3 1に入

力する。

次に、ステップS 2 0 8において、監視イベント指定部 1 3 1 は、シナリオ更新部 1 4 2 により入力されたイベント属性情報の達成状態を抽出し、抽出した達成状態をイベント属性情報検索部 1 0 2 に入力する。

次に、ステップS 2 0 9において、監視イベント指定部 1 3 1 はイベント属性情報検索部 1 0 2 から、イベント属性情報検索部 1 0 2 に入力した達成状態を事前条件に持つイベント属性情報を取得する。

次に、ステップS 2 1 0において、監視イベント指定部 1 3 1 は取得したイベント属性情報から未だシナリオに追加されていないイベント属性情報を監視イベント情報の候補として抽出する。

次に、ステップS 2 1 1において、監視イベント指定部 1 3 1 は監視イベント情報の候補のうち、事前条件がすべて満たされているものをイベント関与要素の監視イベント情報として選択し、イベント関与要素の監視イベント情報を関与候補要素指定部 1 4 3 に入力する。

なお、イベント関与要素の監視イベント情報のイベント種別の欄に記述されているイベントが監視イベントである。

[0046] 次に、ステップS 2 1 2において、関与候補要素指定部 1 4 3 は入力されたイベント関与要素の監視イベント情報に、連携予測条件が記述されている監視イベント情報が含まれているかどうかを確認する。

連携予測条件が記述されている監視イベント情報が存在するか否かによって、以降の処理が分かれる。連携予測条件が記述されている監視イベント情報が存在する場合はステップS 2 1 3 が実施され、連携予測条件が記述されている監視イベント情報が存在しない場合はS 2 1 8 が実施される。

ステップS 2 1 3 では、関与候補要素指定部 1 4 3 は、連携予測条件が記述されている監視イベント情報をシナリオ検索部 1 4 1 に入力する。シナリオ検索部 1 4 1 は監視イベント情報に含まれる連携予測条件に基づいてシナリオを検索する。

シナリオ検索部 1 4 の具体的な処理の流れを、図 1 8 を参照して説明する

。

図 1 8 は、シナリオ検索部 1 4 1 が関与候補要素指定部 1 4 3 から監視イベント情報を受信した場合に、シナリオ記憶部 1 0 6 から条件に合ったシナリオを取得する動作の流れを説明したフローチャートである。

[0047] まず、ステップ S 4 0 1 において、シナリオ検索部 1 4 1 は、連携予測条件が記述されている監視イベント情報を関与候補要素指定部 1 4 3 から受信する。

次に、ステップ S 4 0 2 において、シナリオ検索部 1 4 1 は、監視イベント情報に含まれる連携予測条件の述語論理と同じ述語論理を達成状態に持つイベント属性情報が含まれるシナリオをシナリオ記憶部 1 0 6 から検索する。シナリオ検索部 1 4 1 は、束縛済み変数情報は考慮せずに、監視イベント情報に含まれる連携予測条件の述語論理と同じ述語論理を達成状態に持つイベント属性情報が含まれるシナリオを検索する。

次に、ステップ S 4 0 3 において、S 4 0 2 の検索の結果、該当するシナリオを取得したかどうかで処理が分かれる。シナリオ検索部 1 4 1 がシナリオを取得した場合は、S 4 0 4 が実施され、シナリオ検索部 1 4 1 がシナリオを取得しなかった場合は、処理が終了する。

ステップ S 4 0 4 では、シナリオ検索部 1 4 1 は、取得したシナリオ（関与候補要素のシナリオ）を関与候補要素指定部 1 4 3 に出力し、処理を終了する。

[0048] 次に、図 1 4 のステップ S 2 1 4 において、関与候補要素指定部 1 4 3 がシナリオ検索部 1 4 1 から関与候補要素のシナリオを取得したかどうかによって処理が分かれる。関与候補要素指定部 1 4 3 がシナリオ検索部 1 4 1 から関与候補要素のシナリオを取得した場合は処理 S 2 1 5 が実施され、関与候補要素指定部 1 4 3 がシナリオ検索部 1 4 1 から関与候補要素のシナリオを取得しなかった場合は、S 2 1 8 が実施される。

ステップ S 2 1 5 では、関与候補要素指定部 1 4 3 は取得結果のシナリオごとに束縛済み変数情報を設定した関与候補要素の監視イベント情報を生成

し、生成した関与候補要素の監視イベント情報と関与候補要素のシナリオを監視イベント指定部 131 に出力する。より具体的には、関与候補要素指定部 143 は、ステップ S 214 で取得したシナリオから、連携予測条件の述語論理が達成状態に記述されているイベント属性情報を抽出し、抽出したイベント属性情報の束縛済み変数情報の具体値を、ステップ S 212 で取得したイベント関与要素の監視イベントの束縛済み変数情報に設定して、関与候補要素の監視イベント情報を生成する。そして、関与候補要素指定部 143 は、生成した関与候補要素の監視イベント情報と、関与候補要素のシナリオを監視イベント指定部 131 に出力する。

なお、ステップ S 214 で関与候補要素指定部 143 が取得したシナリオが対象としているシステム構成要素が関与候補要素に相当する。

[0049] 次に、ステップ S 216 において、監視イベント指定部 131 は、取得した関与候補要素のシナリオ及び関与候補要素の監視イベント情報の対をシナリオ更新部 142 に入力する。

次に、ステップ S 217 において、シナリオ更新部 142 は関与候補要素のシナリオに関与候補要素の監視イベント情報を追加し、関与候補要素の監視イベント情報が追加された関与候補要素のシナリオでシナリオ記憶部 106 の関与候補要素のシナリオを更新する。

次に、ステップ S 218 において、監視指示部 133 が監視イベント情報 401 を監視装置 500 に送信する。具体的には、監視イベント指定部 131 がイベント関与要素の監視イベント情報 401 と関与候補要素の監視イベント情報 401 を監視指示部 133 に入力し、監視指示部 133 がイベント関与要素の監視イベント情報 401 と関与候補要素の監視イベント情報 401 を監視装置 500 に送信する。

なお、ステップ S 212 で NO の場合、ステップ S 214 で NO の場合は、関与候補要素の監視イベント情報 401 は生成されないので、監視指示部 133 はイベント関与要素の監視イベント情報 401 のみを監視装置 500 に送信する。

[0050] ***実施の形態の効果の説明***

このように、本実施の形態では、関与候補要素指定部は、イベント関与要素の監視イベント情報に、連携予測条件として、監視イベントに関連する攻撃イベントの属性値が記述されている場合に、イベント関与要素以外のシステム構成要素のうち、イベント関与要素の監視イベント情報に記述されている属性値と同じ属性値が達成状態の状態値に記述されているイベント属性情報がシナリオに含まれるシステム構成要素を、関与候補要素として指定する。

つまり、本実施の形態では、関与候補要素指定部が、イベント関与要素以外に監視イベントの発生に関与し得るシステム構成要素を関与候補要素として指定するため、関与候補要素での監視イベントの監視を可能にする。

例えば、攻撃者が計算機端末Aからファイルサーバのログインパスワードを取得したことが検知イベントとして検知された場合を想定する。本実施の形態に係る情報処理装置は、次に攻撃者が計算機端末Aからファイルサーバへログインすることを監視イベントとして予測し、計算機端末A以外に監視イベントの発生に関与する可能性のある計算機端末Bを関与候補要素として指定し、計算機端末Aからファイルサーバへのログインと、計算機端末Bからのファイルサーバへのログインとを監視装置に監視させることができる。

このように、本実施の形態によれば、イベント関与要素以外のシステム構成要素を介した攻撃を検知することができ、検知漏れを防ぐことができる。

[0051] 実施の形態2.

構成の説明

本実施の形態では、イベント関与要素のシナリオと関与候補要素のシナリオとを統合する構成を説明する。

以下では、主に実施の形態1との差異を説明する。以下で説明していない事項は、実施の形態1と同様である。

本実施の形態においても、システム構成例は図1に示す通りである。

また、本実施の形態においても、情報処理装置100の機能構成例は図2

に示す通りであるが、シナリオ制御部 104 の内部構成例が実施の形態 1 とは異なる。

図 19 は、本実施の形態に係るシナリオ管理部 103 及びシナリオ制御部 104 の詳細な構成の例を示す。

図 19 に示すように、シナリオ管理部 103 は実施の形態 1 と同様の構成であり、シナリオ制御部 104 には実施の形態 1 の構成に加え、シナリオ統合部 144 が配置されている。

シナリオ統合部 144 は、シナリオ記憶部 106 のイベント関与要素のシナリオと関与候補要素のシナリオとを統合する。

より具体的には、シナリオ統合部 144 は、シナリオ記憶部 106 にイベント関与要素のシナリオと、関与候補要素のシナリオが記憶されており、監視装置 500 からの検知アラート 400 において、新たに検知された攻撃イベントとして監視イベントが通知され、監視イベントの発生に関与したシステム構成要素として関与候補要素が通知された場合に、イベント関与要素のシナリオと関与候補要素のシナリオとを統合する。

なお、本実施の形態でも、情報処理装置 100 は、図 4 に示すように、例えばプロセッサ 901、記憶装置 902、レシーバー 903、トランスミッター 904 というハードウェアで構成される。

[0052] ***動作の説明***

次に、実施の形態 2 に係る情報処理装置 100 の動作例を図 20 及び図 21 を参照して説明する。

図 20 及び図 21 は、実施の形態 2 に係る情報処理装置 100 のシナリオ管理部 103 及びシナリオ制御部 104 の詳細動作の流れを示すフローチャートである。

まず、ステップ S201～S203 が行われる。なお、S201～S203 は図 12 に示したものと同様であるため、説明を省略する。

次に、ステップ S501 では、S203 においてシナリオ検索部 141 がシナリオ記憶部 106 からシナリオを取得できたかどうかによって処理が分

かれる。シナリオ検索部 141 がシナリオを取得できた場合は S502 が実施され、シナリオ検索部 141 がシナリオを取得できない場合は S206 が実施される。

ステップ S502 では、シナリオ更新部 142 がシナリオ検索部 141 から得られたシナリオ及び攻撃イベント登録部 132 から入力されたイベント属性情報をシナリオ統合部 144 に入力する。

次に、ステップ S503 において、シナリオ検索部 141 が取得したシナリオに関与候補要素の監視イベント情報が含まれるか否かで処理が分かれる。シナリオ検索部 141 が取得したシナリオに関与候補要素の監視イベント情報が含まれる場合、すなわち、検知アラート 400 で通知された検知イベントが監視イベントであり、検知アラート 400 で通知された検知イベントの発生に関与したシステム構成要素が関与候補要素である場合には、ステップ S504 が実施される。一方、シナリオ検索部 141 が取得したシナリオに関与候補要素の監視イベント情報が含まれない場合は、ステップ S205 が実施される。

なお、シナリオ統合部 144 は、連携予測 ID が記述される監視イベント情報がシナリオに含まれるか否かを確認することで S504 の判定を行うことができる。

図 22 に連携予測 ID を含む監視イベント情報の例を示す。

[0053] 図 22 の監視イベント情報 33 には符号 34 に示すように「連携予測 ID」が含まれており、符号 35 に示されるように、連携予測 ID の要素として主 ID と子 ID がある。

符号 35 の主 ID は、関与候補要素のシナリオへの関与候補要素の監視イベント情報の追加の起点となった監視イベント情報（イベント関与要素の監視イベント情報）の ID である。主 ID は、関与候補要素指定部 143 が、他のシナリオ（関与候補要素のシナリオ）に監視イベント情報を追加可能となった際に、起点となった監視イベント情報（イベント関与要素の監視イベント情報）に付与する。なお、主 ID に付与する値は、主 ID ごとに個別の

値とする。

符号 35 の子 I D は、主 I D が付与された監視イベント情報（イベント関与要素の監視イベント情報）から派生した監視イベント情報（関与候補要素の監視イベント情報）の I D である。

子 I D は、関与候補要素指定部 143 が、関与候補要素の監視イベント情報を関与要素のシナリオに追加する際に、関与候補要素の監視イベント情報に付与する。なお、子 I D に付与する値は、子 I D ごとに個別の値とする。

以下では、主 I D が付与されている監視イベント情報（イベント関与要素の監視イベント情報）を派生元の監視イベント情報ともいい、子 I D が付与されている監視イベント情報（関与候補要素の監視イベント情報）を派生先の監視イベント情報ともいう。

[0054] シナリオ統合部 144 は、シナリオ検索部 141 が取得したシナリオに連携予測 I D 34 が記述されている監視イベント情報が含まれ、連携予測 I D 34 に主 I D と子 I D が記述されている場合に、ステップ S 503 で YES と判定する。

一方、連携予測 I D 34 に主 I D のみであれば、シナリオ統合部 144 はステップ S 503 で NO と判定する。

[0055] ステップ S 504 では、シナリオ統合部 144 は、シナリオ検索部 141 から、関与候補要素の監視イベント情報の派生元の監視イベント情報（イベント関与要素の監視イベント情報）が含まれるシナリオ（イベント関与情報のシナリオ）を取得する。

ステップ S 504 の具体的な処理の流れは、図 23 を参照して説明する。

図 23 は、シナリオ統合部 144 が関与候補要素の監視イベント情報の派生元の監視イベント情報（イベント関与要素の監視イベント情報）が含まれるシナリオ（イベント関与情報のシナリオ）を検索する動作の流れを示す。

[0056] まず、ステップ S 601 において、シナリオ統合部 144 は、シナリオ更新部 142 から入力されたシナリオから関与候補要素の監視イベント情報を取得し、取得した関与候補要素の監視イベント情報をシナリオ検索部 141

に入力する。

次に、ステップS 6 0 2において、シナリオ検索部1 4 1は、関与候補要素の監視イベント情報内の連携予測IDの主IDと同じ主IDが記述されるが、子IDは記述されていない監視イベント情報を含むシナリオを検索する。

次に、ステップS 6 0 3において、S 6 0 2の検索の結果、シナリオ検索部1 4 1がシナリオを取得したかどうかで処理が分かれる。シナリオ検索部1 4 1がシナリオを取得した場合は、S 6 0 4が実行され、シナリオ検索部1 4 1がシナリオを取得しなかった場合は、処理が終了する。

ステップS 6 0 4において、シナリオ検索部1 4 1は、S 6 0 2の検索で取得したシナリオをシナリオ統合部1 4 4に出力し、処理を終了する。

[0057] 次に、図2 1のステップS 5 0 5において、シナリオ統合部1 4 4はS 5 0 4で取得した派生元のシナリオと、シナリオ更新部1 4 2から入力されたシナリオとを統合する。

シナリオ統合部1 4 4は、2つのシナリオ内のイベント属性情報を1つのシナリオに集約させてシナリオを統合する。このとき、2つのシナリオに同じイベント種別情報が含まれている場合は、シナリオ統合部1 4 4は、イベント属性情報の束縛済み変数情報を集約させ、1つのイベント属性情報とする。

[0058] 図2 4に、集約後のイベント属性情報の例を示す。

図2 4の例では、イベント属性情報3 6のうち、符号3 7に示される束縛変数情報において、符号3 8に示されるように、変数名A及び変数名Hの要素がそれぞれ「USER 1

OR USER 2」、「H__1 OR H__2」となっている。図2 4は、イベント種別として「ANOMALOUS__FILE__ACCESS」が記述されており、束縛済み変数情報に変数Aの束縛値として「USER 1」が記述され、変数Hの束縛値として「H__1」が記述されているイベント属性情報と、イベント種別として「ANOMALOUS__FILE__ACCE

SS」が記述されており、束縛済み変数情報に変数Aの束縛値として「USER2」が記述され、変数Hの束縛値として「H__2」が記述されているイベント属性情報とを集約させた例を示す。シナリオ統合部144は、図24のように、束縛済み変数の異なる要素はORで統合する。

[0059] なお、図20及び図21において、ステップS205～S218の処理は図12～図15と同様であり、説明を省略する。

[0060] ***実施の形態の効果の説明***

以上のように、本実施の形態では、実施の形態1によって新たに監視を開始した攻撃イベントを検知した際に、派生元のシナリオと、検知された攻撃イベントについてのシナリオとを統合することで、攻撃者の一連の攻撃活動を1つのシナリオで管理することができる。

これにより、例えば1つのシナリオ上で一定個数の攻撃イベントを検知した場合にサイバー攻撃が発生したとみなす検知システムでは、2以上のシナリオで管理していた攻撃者の活動が1つのシナリオに集約され、管理されることで、サイバー攻撃の検知精度を向上させることができる。

[0061] 実施の形態3.

構成の説明

本実施の形態では、シナリオ統合部144によるシナリオの統合を許可するか否かを判定する構成を説明する。

以下では、主に実施の形態1及び実施の形態2との差異を説明する。以下で説明していない事項は、実施の形態1及び実施の形態2と同様である。

本実施の形態においても、システム構成例は図1に示す通りである。

また、本実施の形態においても、情報処理装置100の機能構成例は図2に示す通りであるが、シナリオ制御部104の内部構成例が実施の形態1及び実施の形態2とは異なる。

図25は、本実施の形態に係るシナリオ管理部103及びシナリオ制御部104の詳細な構成の例を示す。

図25に示すように、シナリオ管理部103は実施の形態1及び実施の形

態２と同様の構成であり、シナリオ制御部１０４には実施の形態２の構成に加え、シナリオ統合判定部１４５が配置されている。

シナリオ統合判定部１４５は、シナリオ統合部１４４によるイベント関与要素のシナリオと関与候補要素のシナリオとの統合を許可するか否かを判定する。

なお、本実施の形態でも、情報処理装置１００は、図４に示すように、例えばプロセッサ９０１、記憶装置９０２、レシーバー９０３、トランスミッター９０４というハードウェアで構成される。

[0062] ***動作の説明***

実施の形態３に係る情報処理装置１００の動作例を図２７及び図２８を参照して説明する。

図２７及び図２８は、実施の形態３に係る情報処理装置１００のシナリオ管理部１０３及びシナリオ制御部１０４の詳細動作の流れを示すフローチャートである。

まず、図２０におけるステップＳ５０３までの処理が行われ、更に、図２１のＳ５０４の処理が行われて、シナリオ統合部１４４が派生元のシナリオを取得する。

次に、ステップＳ８０１において、シナリオ統合部１４４が、Ｓ５０２で取得したシナリオとＳ５０４で取得したシナリオを、シナリオ統合判定部１４５に入力する。

次に、ステップＳ８０２において、シナリオ統合判定部１４５は、双方のシナリオにおいて、共通するイベント属性情報にシナリオ統合除外識別子が記述されているかどうかを確認する。

双方のシナリオにおいて、共通するイベント属性情報にシナリオ統合除外識別子が記述されている場合は、ステップＳ２０５が実施される。つまり、シナリオ統合判定部１４５は、イベント関与要素のシナリオと関与候補要素のシナリオとの統合を許可せず、このため、シナリオ統合部１４４は、イベント関与要素のシナリオと関与候補要素のシナリオとを統合しない。

一方、共通するイベント属性情報にシナリオ統合除外識別子が記述されていない場合は、S 5 0 5 が実施される。つまり、シナリオ統合判定部 1 4 5 は、イベント関与要素のシナリオと関与候補要素のシナリオとの統合を許可し、このため、シナリオ統合部 1 4 4 は、イベント関与要素のシナリオと関与候補要素のシナリオとを統合する。

以降の処理は実施の形態 2 と同様である。

[0063] 図 2 6 にシナリオ統合除外識別子が記述されるイベント属性情報の例を示す。

図 2 6 が示すように、イベント属性情報 4 0 には、符号 4 1 に示されるように、シナリオ統合除外識別子が含まれている。

前述したように、シナリオ統合判定部 1 4 5 は、2つのシナリオにおいて、共通するイベント属性情報にシナリオ統合除外識別子が記述されているかどうかを確認する。そして、共通するイベント属性情報にシナリオ統合除外識別子が記述されていなければ、シナリオ統合判定部 1 4 5 は、シナリオの統合を許可し、記述されていればシナリオの統合を許可しない。

なお、シナリオ統合判定部 1 4 5 は、共通するイベント属性情報にシナリオ統合除外識別子が記述されているか否かを確認する際は、イベント属性情報に含まれる束縛済み変数情報の違いは考慮せず、イベント種別のみを比較する。

[0064] ***実施の形態の効果の説明***

以上のように、本実施の形態では、シナリオの統合を行わないことで、複数の攻撃者が存在した場合に攻撃者ごとのシナリオで攻撃活動を監視することが可能である。これにより、複数の攻撃活動を 1 人の攻撃者による攻撃活動と誤認してしまうことによる被害を防ぐことができる。複数の攻撃活動を 1 人の攻撃者による攻撃活動と誤認すると、各攻撃活動を有効に検知することができずに、被害が拡大してしまうが、本実施の形態ではこうした被害を未然に防止することができる。

[0065] 実施の形態 4.

構成の説明

本実施の形態では、シナリオ更新部 142 による関与候補要素の監視イベント情報の関与候補要素のシナリオへの追加を許可するか否かを判定する構成を説明する。

以下では、主に実施の形態 1～3 との差異を説明する。以下で説明していない事項は、実施の形態 1～3 と同様である。

本実施の形態においても、システム構成例は図 1 に示す通りである。

また、本実施の形態においても、情報処理装置 100 の機能構成例は図 2 に示す通りであるが、シナリオ制御部 104 の内部構成例が実施の形態 1～3 とは異なる。

図 29 は、本実施の形態に係るシナリオ管理部 103 及びシナリオ制御部 104 の詳細な構成の例を示す。

図 29 に示すように、シナリオ管理部 103 は実施の形態 1～3 と同様の構成であり、シナリオ制御部 104 には実施の形態 3 の構成に加え、シナリオ追加判定部 146 が配置されている。

シナリオ追加判定部 146 は、シナリオ更新部 142 による関与候補要素の監視イベント情報の関与候補要素のシナリオへの追加を許可するか否かを判定する。

なお、本実施の形態でも、情報処理装置 100 は、図 4 に示すように、例えばプロセッサ 901、記憶装置 902、レシーバー 903、トランスミッター 904 というハードウェアで構成される。

[0066] ***動作の説明***

実施の形態 4 に係る情報処理装置 100 の動作例を図 30 及び図 31 を参照して説明する。

図 30 及び図 31 は、実施の形態 4 に係る情報処理装置 100 のシナリオ管理部 103 及びシナリオ制御部 104 の詳細動作の流れを示すフローチャートである。

まず、図 14 におけるステップ S213 までの処理が行われ、更に、図 1

4におけるステップS 2 1 4の処理が行われる。

ステップS 2 1 4において関与候補要素指定部1 4 3が検索結果のシナリオを取得した場合は、S 7 0 1が実施され、関与候補要素指定部1 4 3が検索結果のシナリオを取得しない場合は、S 2 1 5が実施される。

ステップS 7 0 1では、関与候補要素指定部1 4 3が、シナリオ追加判定部1 4 6に、イベント関与要素のシナリオと関与候補要素のシナリオを入力する。

次に、ステップS 7 0 2において、シナリオ追加判定部1 4 6は、双方のシナリオにおいて、共通するイベント属性情報にシナリオ統合除外識別子が記述されているかどうかを確認する。シナリオ統合除外識別子は、実施の形態3で説明したものと同様である。

双方のシナリオにおいて、共通するイベント属性情報にシナリオ統合除外識別子が記述されている場合は、ステップS 7 0 3が実施される。つまり、シナリオ追加判定部1 4 6は、監視イベント情報の関与候補要素のシナリオへの追加を許可せず、このため、シナリオ更新部1 4 2は、関与候補要素のシナリオを破棄する。

一方、共通するイベント属性情報にシナリオ統合除外識別子が記述されていない場合は、S 2 1 5が実施される。つまり、シナリオ追加判定部1 4 6は、監視イベント情報の関与候補要素のシナリオへの追加を許可し、このため、関与候補要素指定部1 4 3は、関与候補要素のシナリオごとに、監視イベント情報を生成し、監視イベント情報とシナリオを監視イベント指定部1 3 1に出力する。

以降の処理は実施の形態1と同様であり、シナリオ更新部1 4 2は関与候補要素の監視イベント情報を関与候補要素のシナリオに追加して、関与候補要素のシナリオを更新する。

[0067] ***実施の形態の効果の説明***

以上のように、本実施の形態では、監視イベント情報の生成前に、監視イベント情報を関与候補要素のシナリオに追加するか否かを判定するため、不

要な監視イベント情報の生成を削減することが可能である。

これにより、情報処理装置 100 の演算負荷を低減することができる。

[0068] ***付記***

[0069] 以上、本発明の実施の形態について説明したが、これらの実施の形態のうち、2つ以上を組み合わせる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つを部分的に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、2つ以上を部分的に組み合わせて実施しても構わない。

なお、本発明は、これらの実施の形態に限定されるものではなく、必要に応じて種々の変更が可能である。

[0070] ***ハードウェア構成の説明***

最後に、情報処理装置 100 のハードウェア構成の補足説明を行う。

情報処理装置 100 はコンピュータである。

図 4 に示すプロセッサ 901 は、プロセッシングを行う IC (Integrated Circuit) である。

プロセッサ 901 は、CPU (Central Processing Unit)、DSP (Digital Signal Processor) 等である。

図 4 に示す記憶装置 902 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 4 に示すレシーバー 903 はデータを受信し、トランスミッター 904 はデータを送信する。レシーバー 903 及びトランスミッター 904 は、例えば、通信チップ又は NIC (Network Interface Card) である。

[0071] また、記憶装置 902 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901により実行される。

プロセッサ901はOSの少なくとも一部を実行しながら、アラート受信部101、イベント属性情報検索部102、シナリオ管理部103及びシナリオ制御部104（以下、これらをまとめて「部」という）の機能を実現するプログラムを実行する。

図4では、1つのプロセッサが図示されているが、情報処理装置100が複数のプロセッサを備えていてもよい。

また、「部」の処理の結果を示す情報やデータや信号値や変数値が、記憶装置902、又は、プロセッサ901内のレジスタ又はキャッシュメモリに記憶される。

また、「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等の可搬記憶媒体に記憶されてもよい。

[0072] また、「部」を「プロセッシングサークイットリー」又は「回路」又は「工程」又は「手順」又は「処理」に読み替えてもよい。

「プロセッシングサークイットリー」又は「回路」は、プロセッサ901だけでなく、ロジックIC又はGA（Gate Array）又はASIC（Application Specific Integrated Circuit）又はFPGA（Field-Programmable Gate Array）といった他の種類の処理回路をも包含する概念である。

[0073] なお、図4の構成は、あくまでも情報処理装置100のハードウェア構成の一例を示すものであり、情報処理装置100のハードウェア構成は図4に記載の構成に限らず、他の構成であってもよい。

符号の説明

[0074] 100 情報処理装置、101 アラート受信部、102 イベント属性情報検索部、103 シナリオ管理部、104 シナリオ制御部、105 イベント属性情報記憶部、106 シナリオ記憶部、131 監視イベント

指定部、１３２ 攻撃イベント登録部、１３３ 監視指示部、１４１ シナリオ検索部、１４２ シナリオ更新部、１４３ 関与候補要素指定部、１４４ シナリオ統合部、１４５ シナリオ統合判定部、１４６ シナリオ追加判定部、２００ 情報システム、３００ システム構成要素、４００ 検知アラート、４０１ 監視イベント情報、４０２ イベント属性情報、５００ 監視装置、６００ ネットワーク。

請求の範囲

- [請求項1] 複数のシステム構成要素が含まれる情報システムを攻撃する攻撃イベントが検知され、検知された攻撃イベントである検知イベントと前記検知イベントの発生に関与したシステム構成要素であるイベント関与要素とが通知された場合に、前記検知イベントの次に、前記イベント関与要素の関与により発生し得る攻撃イベントを監視イベントとして指定する監視イベント指定部と、
- 前記複数のシステム構成要素のうち前記イベント関与要素以外に前記監視イベントの発生に関与し得るシステム構成要素を関与候補要素として指定する関与候補要素指定部とを有する情報処理装置。
- [請求項2] 前記関与候補要素指定部は、
- 前記イベント関与要素以外のシステム構成要素のうち、前記監視イベントと関連する攻撃イベントが発生しているシステム構成要素を、前記関与候補要素として指定する請求項1に記載の情報処理装置。
- [請求項3] 前記情報処理装置は、更に、
- 複数の攻撃イベントについて、攻撃イベントごとに、攻撃イベントの属性値が示されるイベント属性情報を記憶するイベント属性情報記憶部と、
- 検知された攻撃イベントのイベント属性情報を、検知された攻撃イベントの発生に関与したシステム構成要素と対応付けて、シナリオとして記憶するシナリオ記憶部とを有し、
- 前記関与候補要素指定部は、
- 前記イベント属性情報記憶部に記憶されている複数のイベント属性情報のうち前記監視イベントのイベント属性情報を取得し、取得した前記監視イベントのイベント属性情報に前記監視イベントに関連する攻撃イベントの属性値が記述されている場合に、前記イベント関与要素以外のシステム構成要素のうち、前記監視イベントのイベント属性情報に記述されている属性値と同じ属性値が記述されているイベント

属性情報がシナリオに含まれるシステム構成要素を、前記関与候補要素として指定する請求項2に記載の情報処理装置。

[請求項4]

前記イベント属性情報記憶部は、

攻撃イベントの属性値として、攻撃イベントの発生後の状態を表す状態値が少なくとも示されるイベント属性情報を記憶しており、

前記関与候補要素指定部は、

前記監視イベントのイベント属性情報に前記状態値以外に前記監視イベントに関連する攻撃イベントの属性値が記述されている場合に、前記イベント関与要素以外のシステム構成要素のうち、前記監視イベントのイベント属性情報に記述されている属性値と同じ状態値が記述されているイベント属性情報がシナリオに含まれるシステム構成要素を、前記関与候補要素として指定する請求項3に記載の情報処理装置。

[請求項5]

前記情報処理装置は、

前記監視イベントのイベント属性情報を、前記イベント関与要素のシナリオと前記関与候補要素のシナリオに追加するシナリオ更新部を有し、

前記シナリオ記憶部は、

前記監視イベントのイベント属性情報が追加された前記イベント関与要素のシナリオと、前記監視イベントのイベント属性情報が追加された前記関与候補要素のシナリオを記憶する請求項3に記載の情報処理装置。

[請求項6]

前記情報処理装置は、更に、

前記シナリオ更新部による前記監視イベントのイベント属性情報の前記関与候補要素のシナリオへの追加を許可するか否かを判定するシナリオ追加判定部を有し、

前記シナリオ更新部は、

前記シナリオ追加判定部により前記監視イベントのイベント属性情

報の前記関与候補要素のシナリオへの追加が許可された場合に、前記監視イベントのイベント属性情報を前記イベント関与要素のシナリオと前記関与候補要素のシナリオに追加し、

前記シナリオ追加判定部により前記監視イベントのイベント属性情報の前記関与候補要素のシナリオへの追加が許可されない場合に、前記監視イベントのイベント属性情報を前記イベント関与要素のシナリオにのみ追加する請求項5に記載の情報処理装置。

[請求項7] 前記情報処理装置は、更に、

前記シナリオ記憶部に前記監視イベントのイベント属性情報が追加された前記イベント関与要素のシナリオと、前記監視イベントのイベント属性情報が追加された前記関与候補要素のシナリオが記憶されており、新たに検知された攻撃イベントとして前記監視イベントが通知され、前記監視イベントの発生に関与したシステム構成要素として前記関与候補要素が通知された場合に、前記シナリオ記憶部の前記イベント関与要素のシナリオと前記関与候補要素のシナリオとを統合するシナリオ統合部を有する請求項5に記載の情報処理装置。

[請求項8] 前記情報処理装置は、更に、

前記シナリオ統合部による前記イベント関与要素のシナリオと前記関与候補要素のシナリオとの統合を許可するか否かを判定するシナリオ統合判定部を有し、

前記シナリオ統合部は、

前記シナリオ統合判定部により前記イベント関与要素のシナリオと前記関与候補要素のシナリオとの統合が許可された場合に、前記イベント関与要素のシナリオと前記関与候補要素のシナリオとを統合し、

前記シナリオ統合判定部により前記イベント関与要素のシナリオと前記関与候補要素のシナリオとの統合が許可されない場合に、前記イベント関与要素のシナリオと前記関与候補要素のシナリオとを統合しない請求項7に記載の情報処理装置。

[請求項9] 前記情報処理装置は、更に、

前記情報システムを監視する監視装置に、前記イベント関与要素での前記監視イベントの監視と前記関与候補要素での前記監視イベントの監視を指示する監視指示部を有する請求項1に記載の情報処理装置。

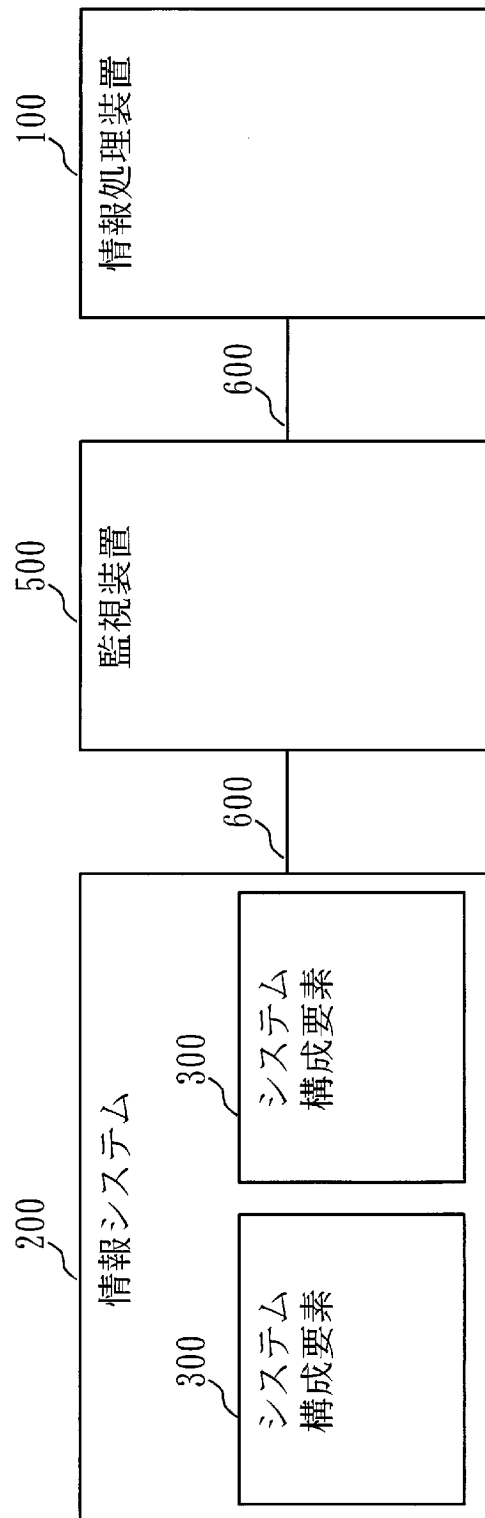
[請求項10] 複数のシステム構成要素が含まれる情報システムを攻撃する攻撃イベントが検知され、検知された攻撃イベントである検知イベントと前記検知イベントの発生に関与したシステム構成要素であるイベント関与要素とが通知された場合に、コンピュータが、前記検知イベントの次に、前記イベント関与要素の関与により発生し得る攻撃イベントを監視イベントとして指定し、

前記コンピュータが、前記複数のシステム構成要素のうち前記イベント関与要素以外に前記監視イベントの発生に関与し得るシステム構成要素を関与候補要素として指定する情報処理方法。

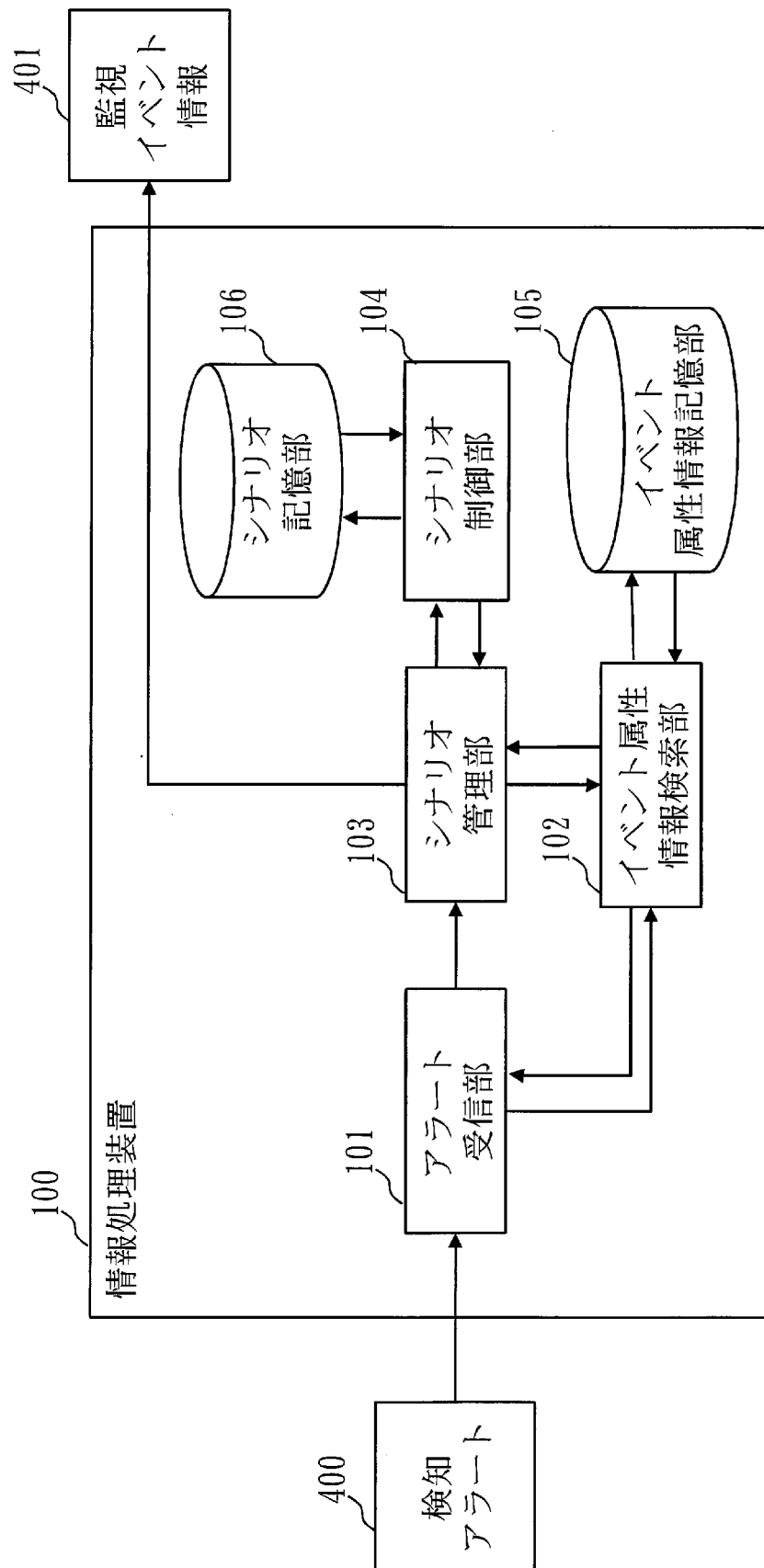
[請求項11] 複数のシステム構成要素が含まれる情報システムを攻撃する攻撃イベントが検知され、検知された攻撃イベントである検知イベントと前記検知イベントの発生に関与したシステム構成要素であるイベント関与要素とが通知された場合に、前記検知イベントの次に、前記イベント関与要素の関与により発生し得る攻撃イベントを監視イベントとして指定する監視イベント指定処理と、

前記複数のシステム構成要素のうち前記イベント関与要素以外に前記監視イベントの発生に関与し得るシステム構成要素を関与候補要素として指定する関与候補要素指定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。

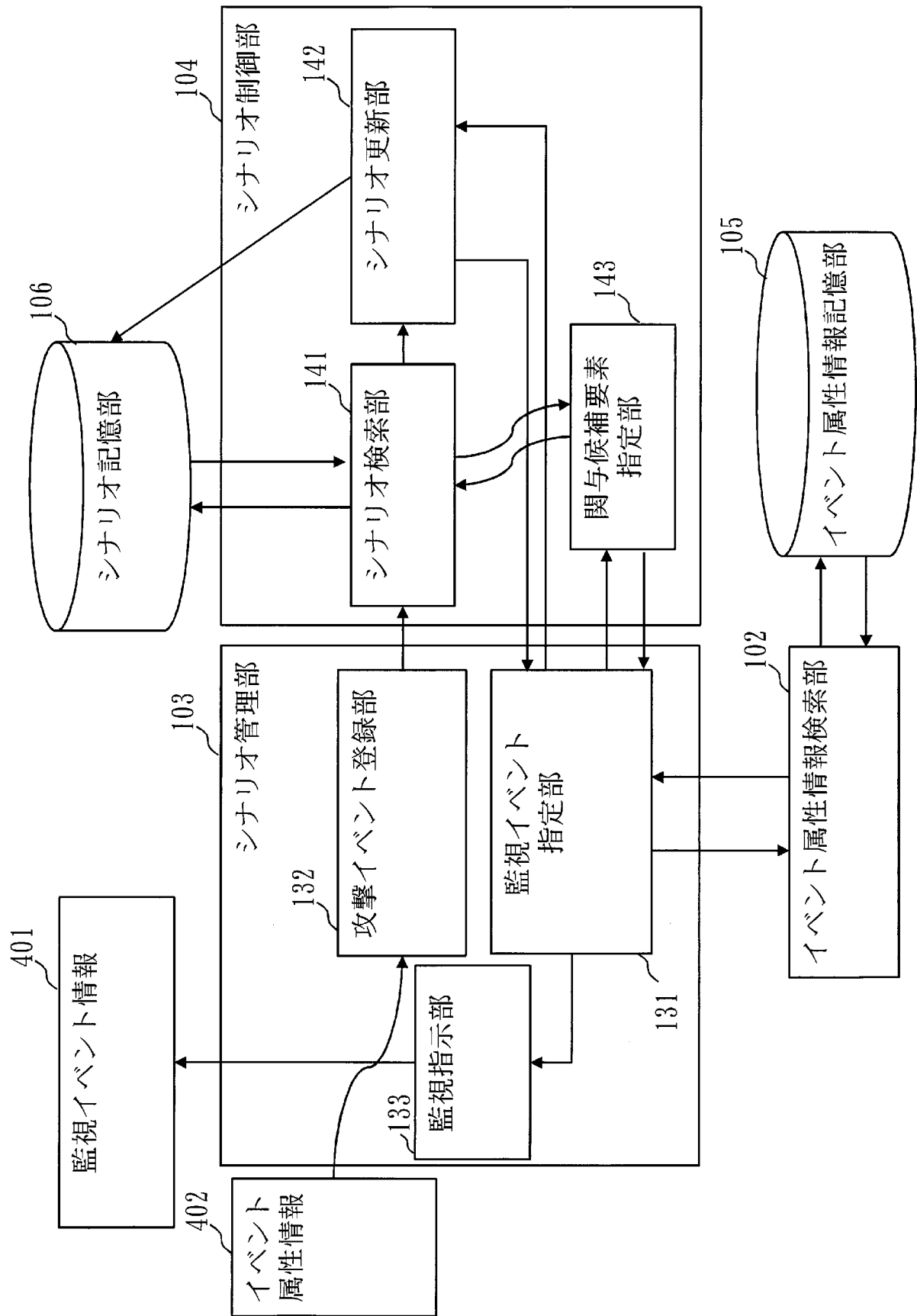
[図1]



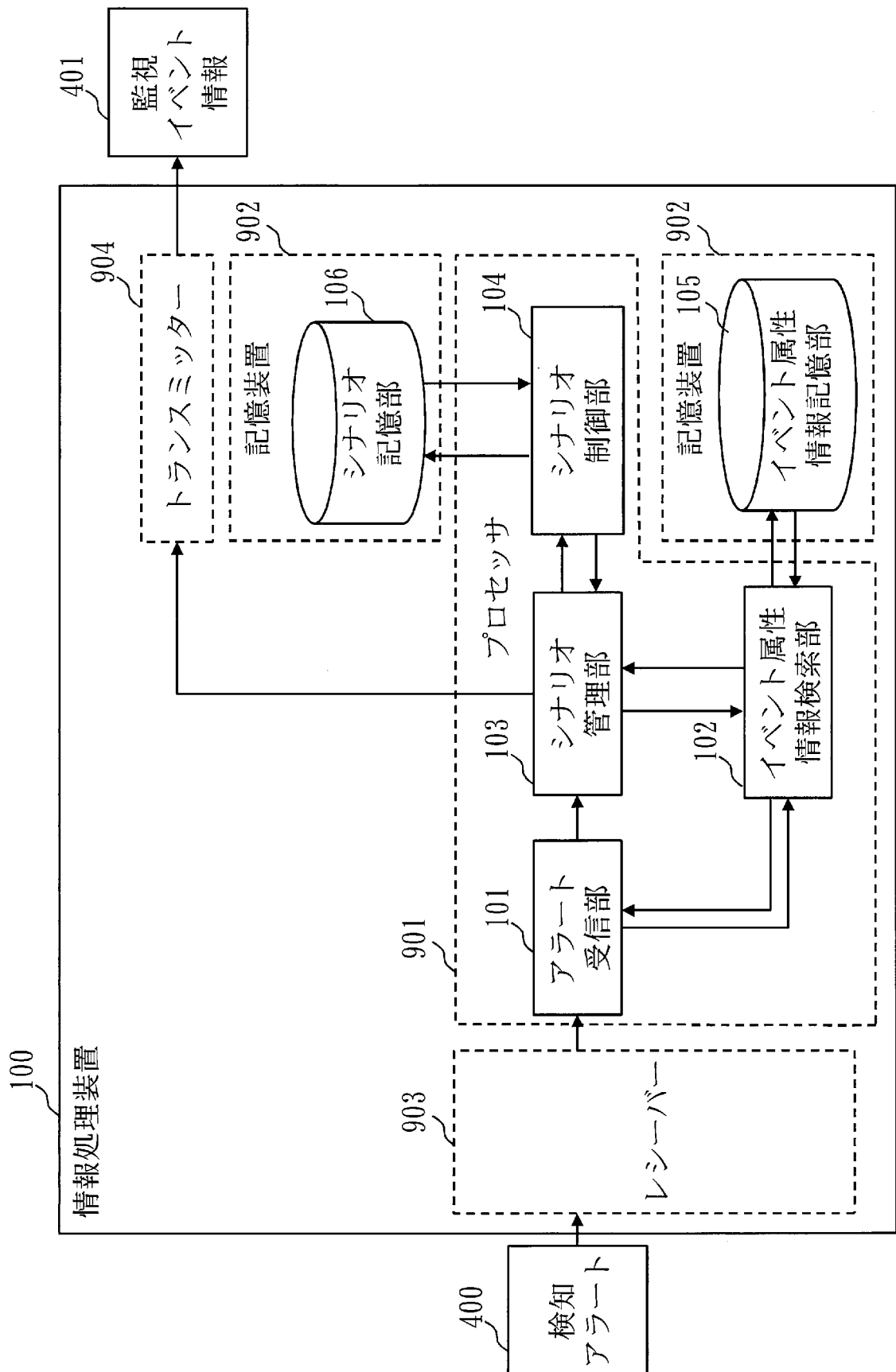
[図2]



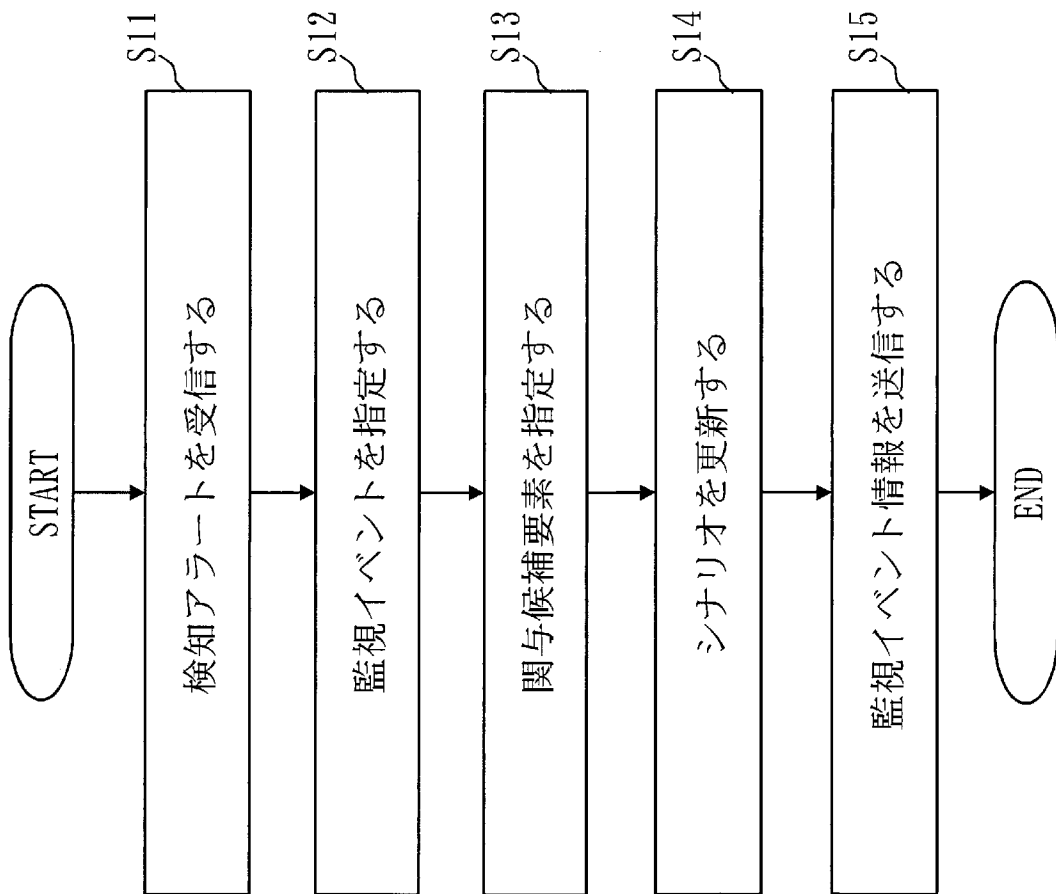
[図3]



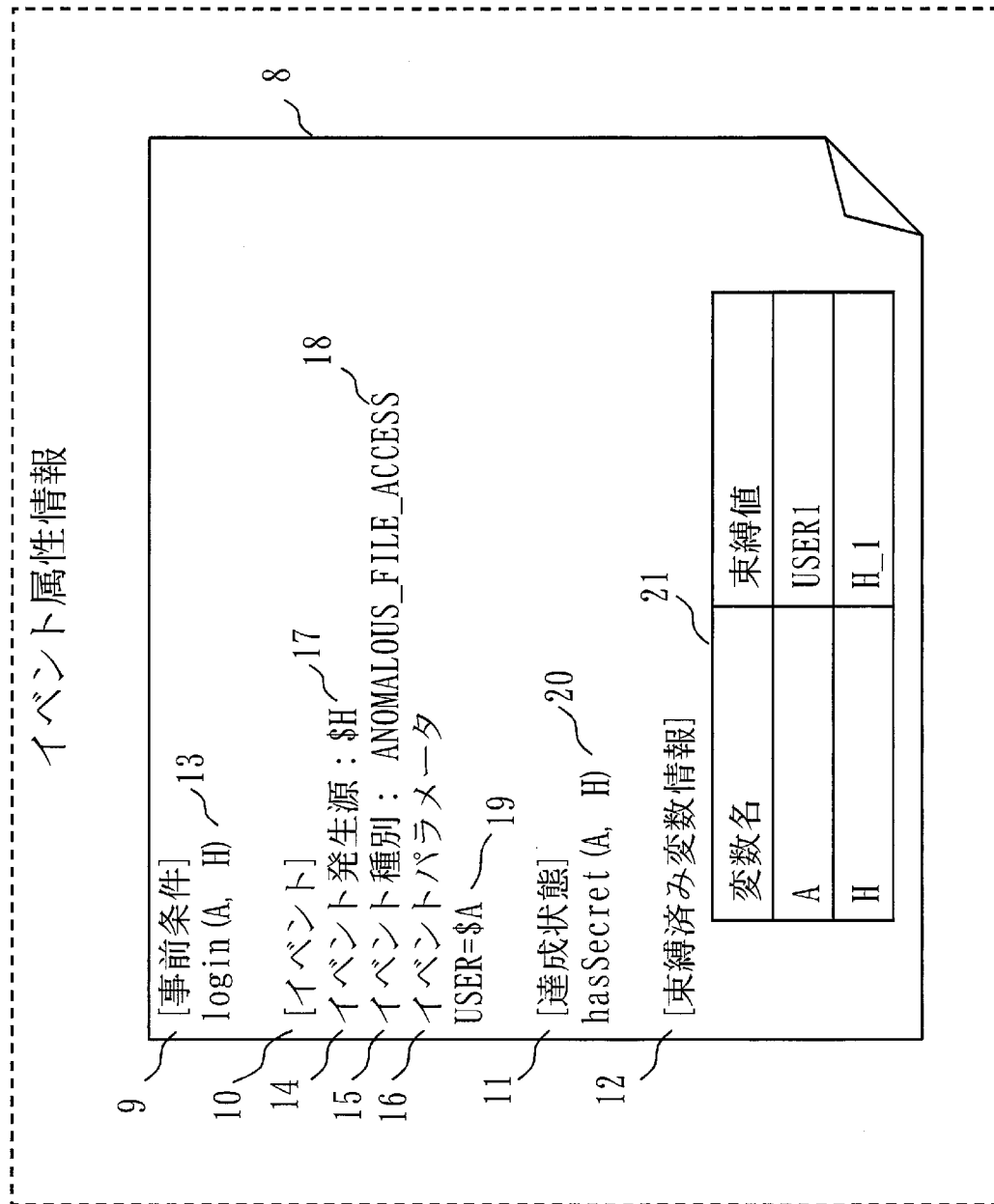
[図4]



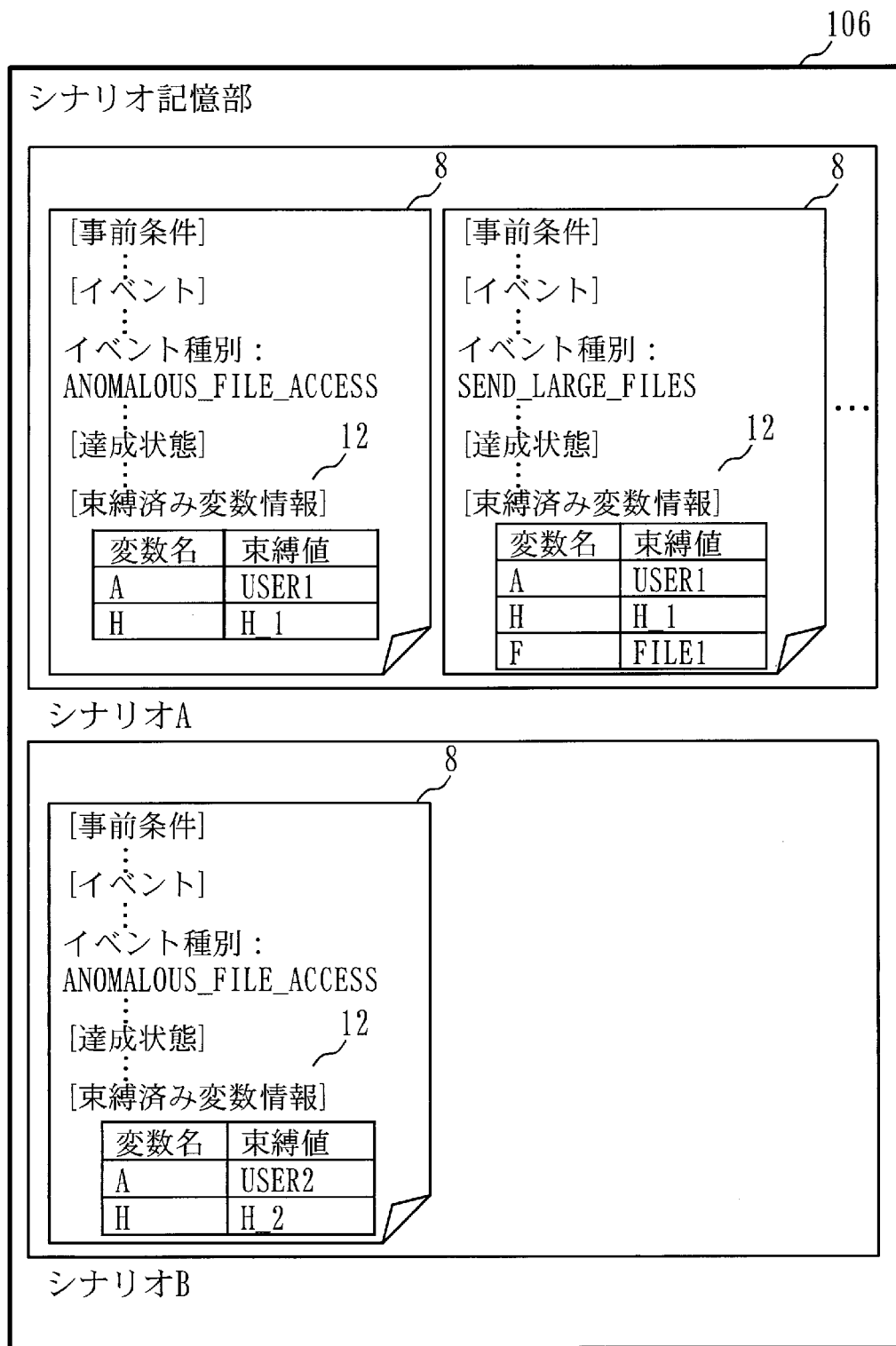
[図5]



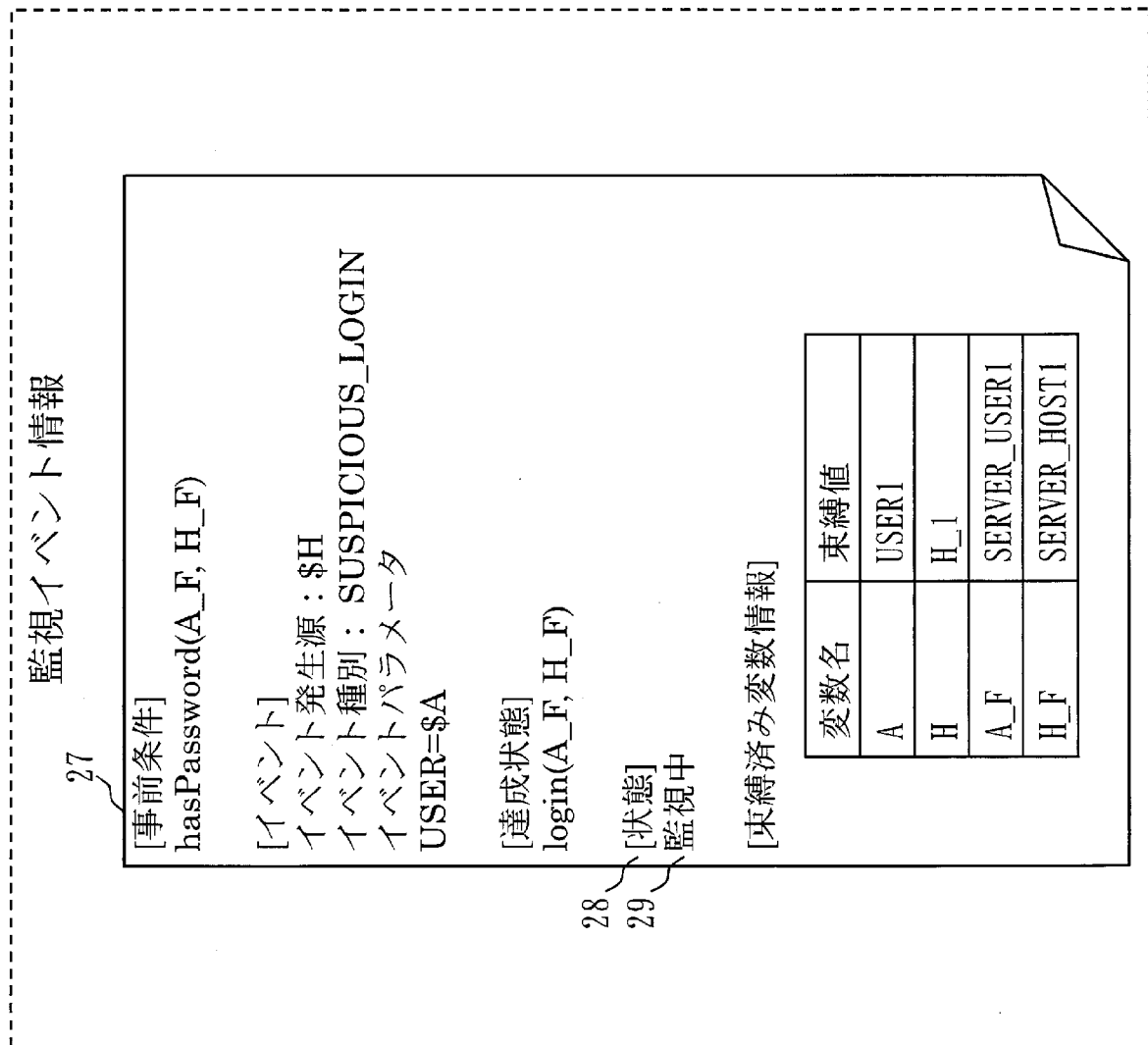
[図6]



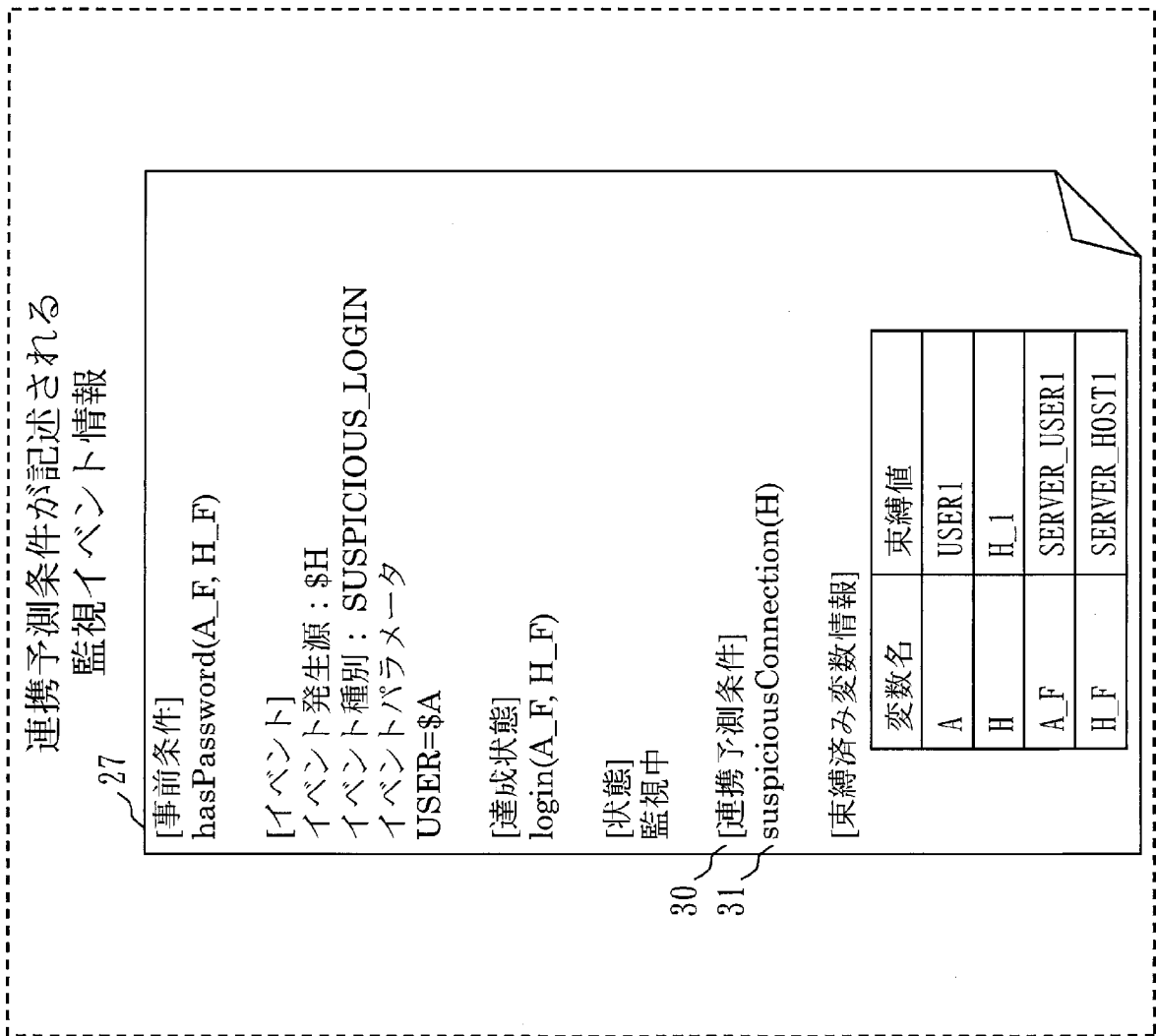
[図7]



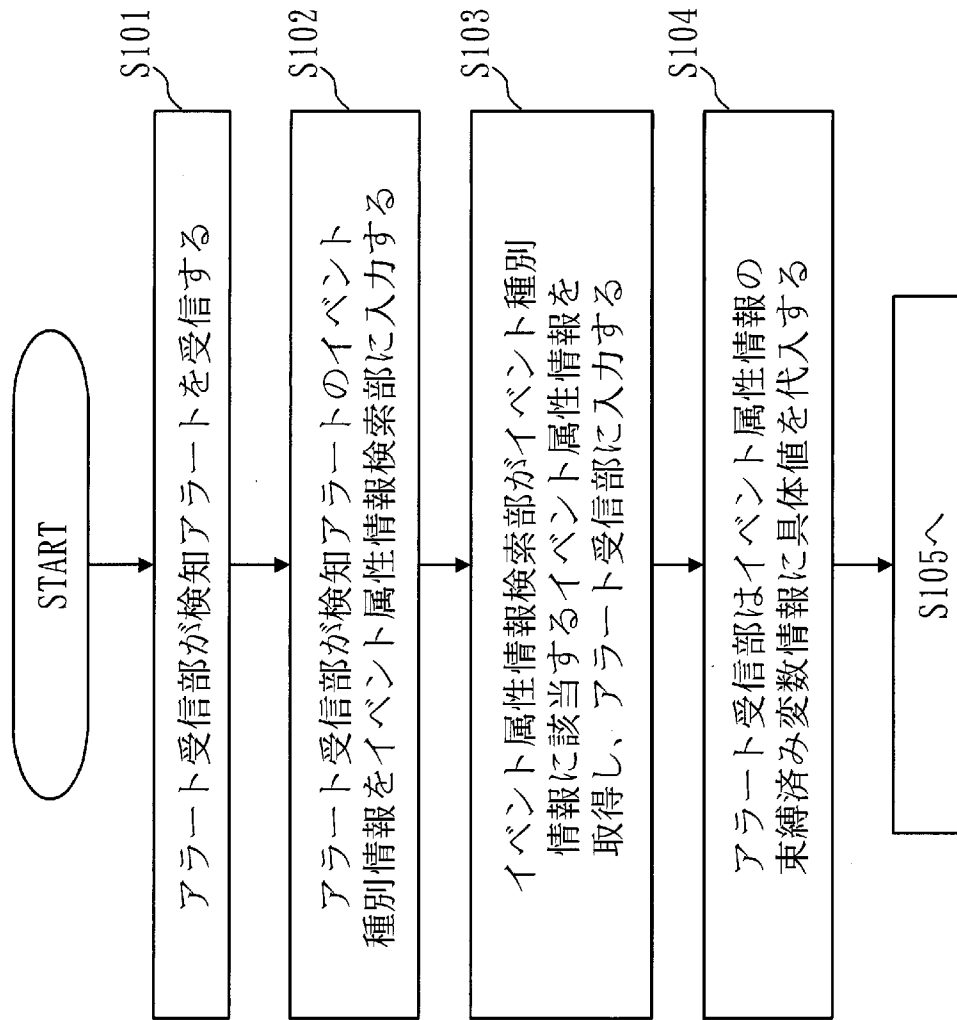
[図8]



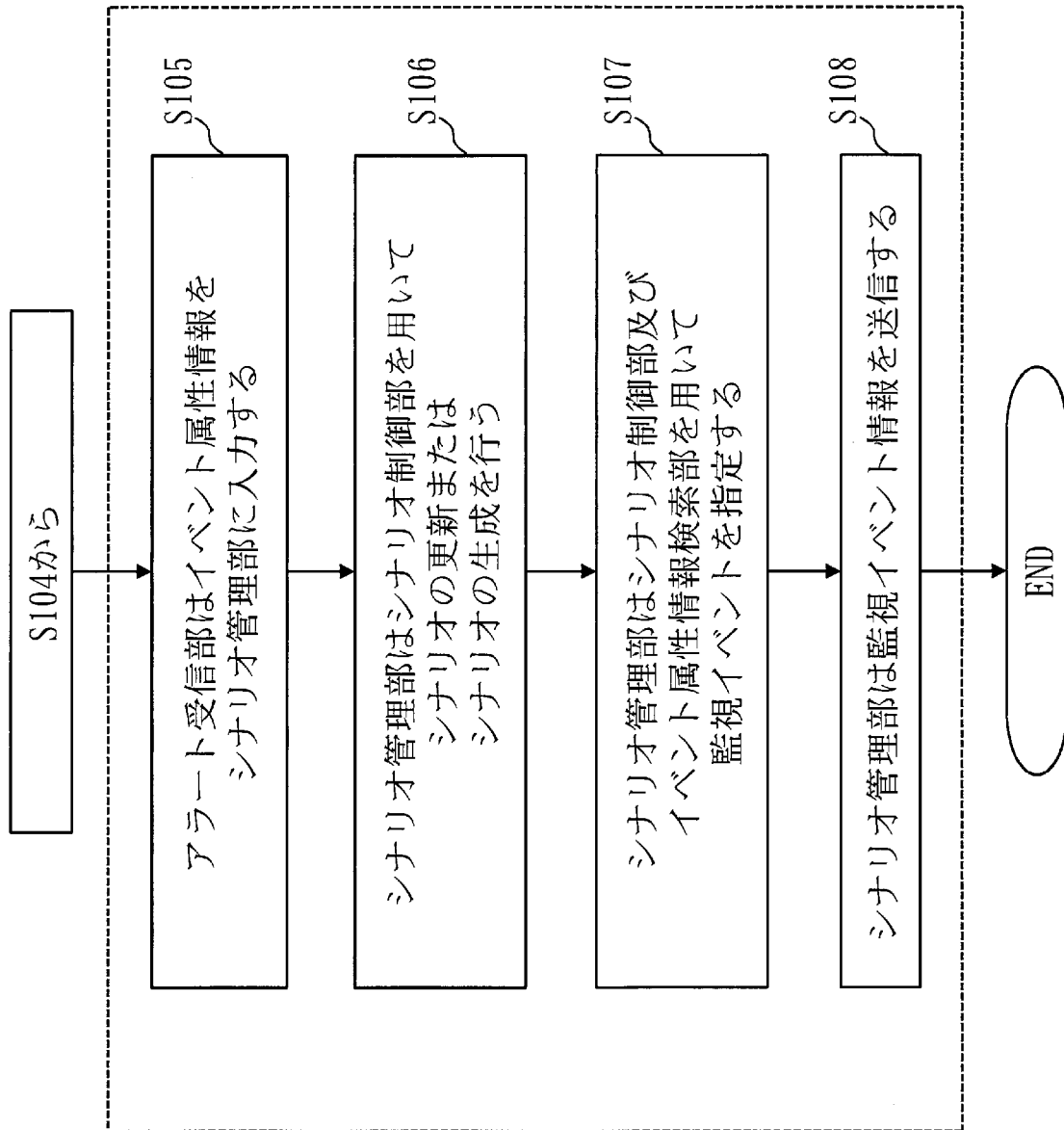
[図9]



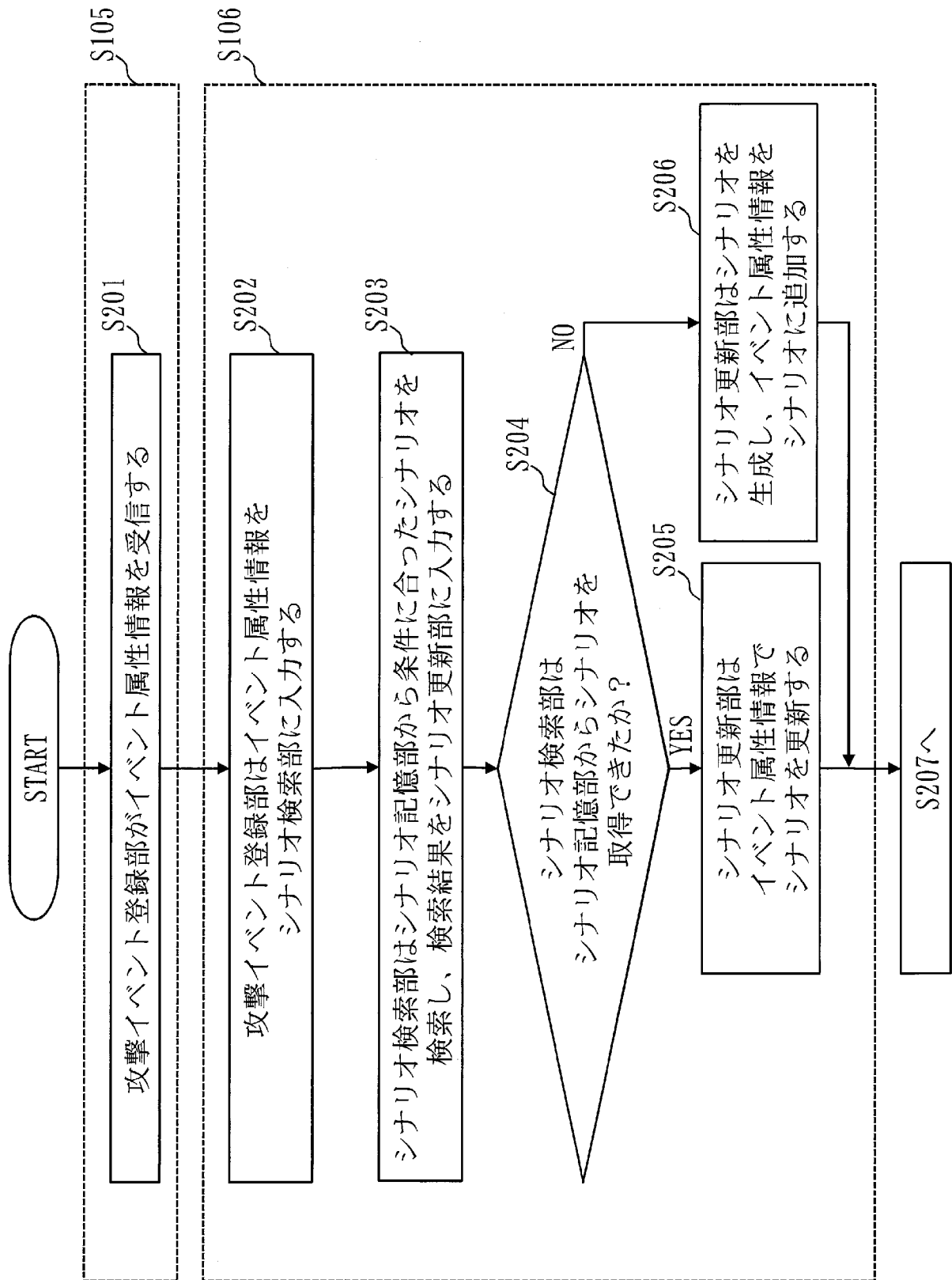
[図10]



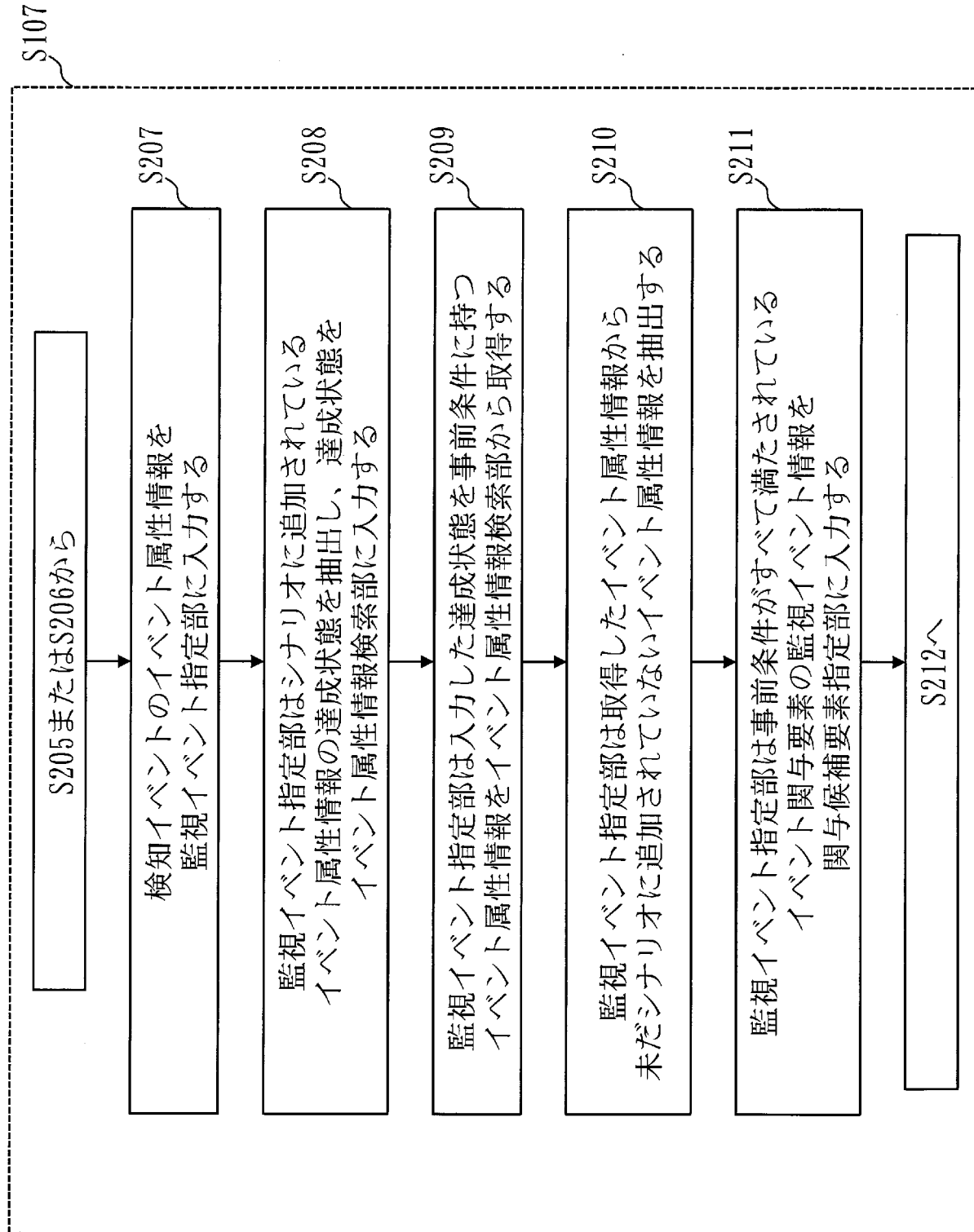
[図11]



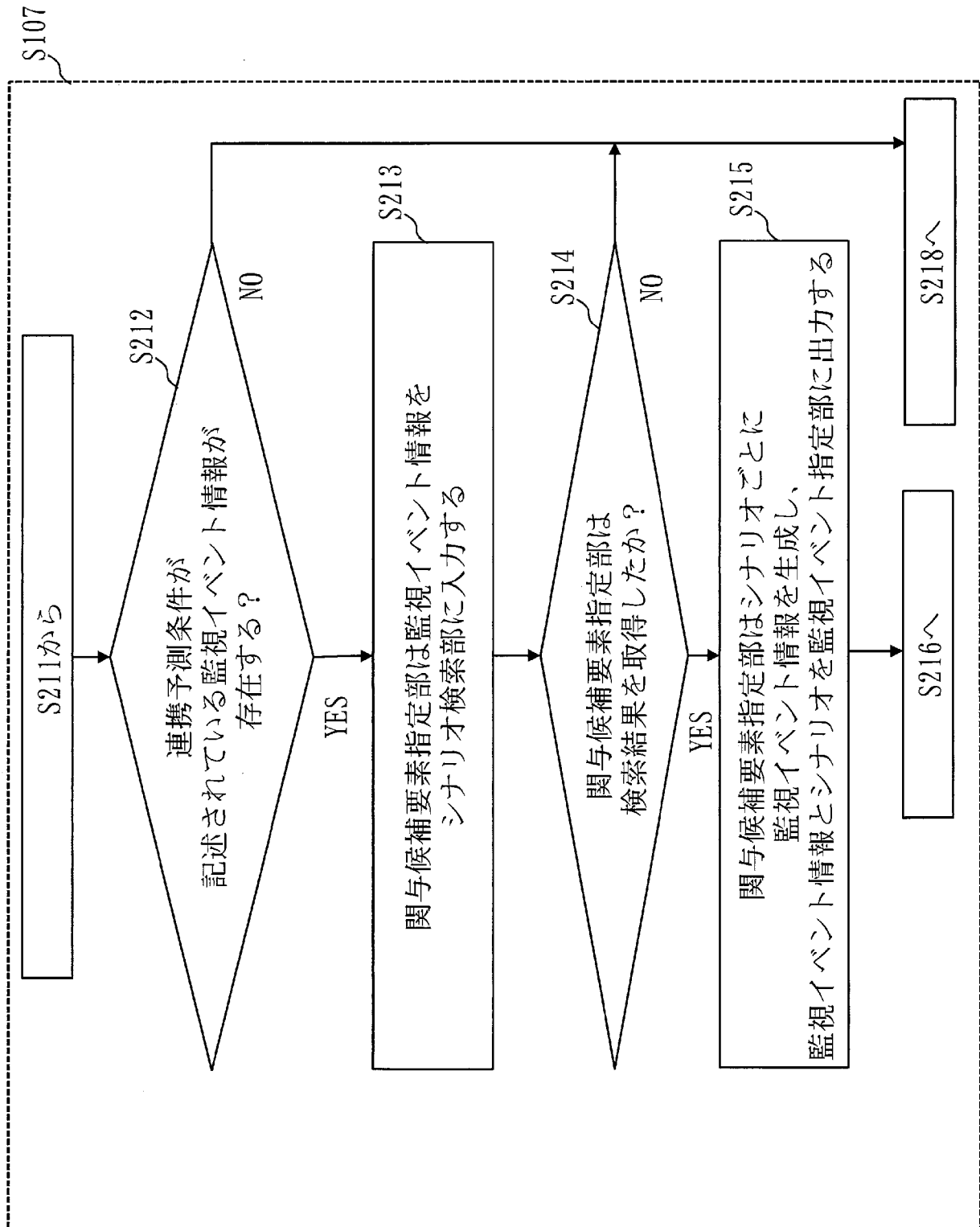
[図12]



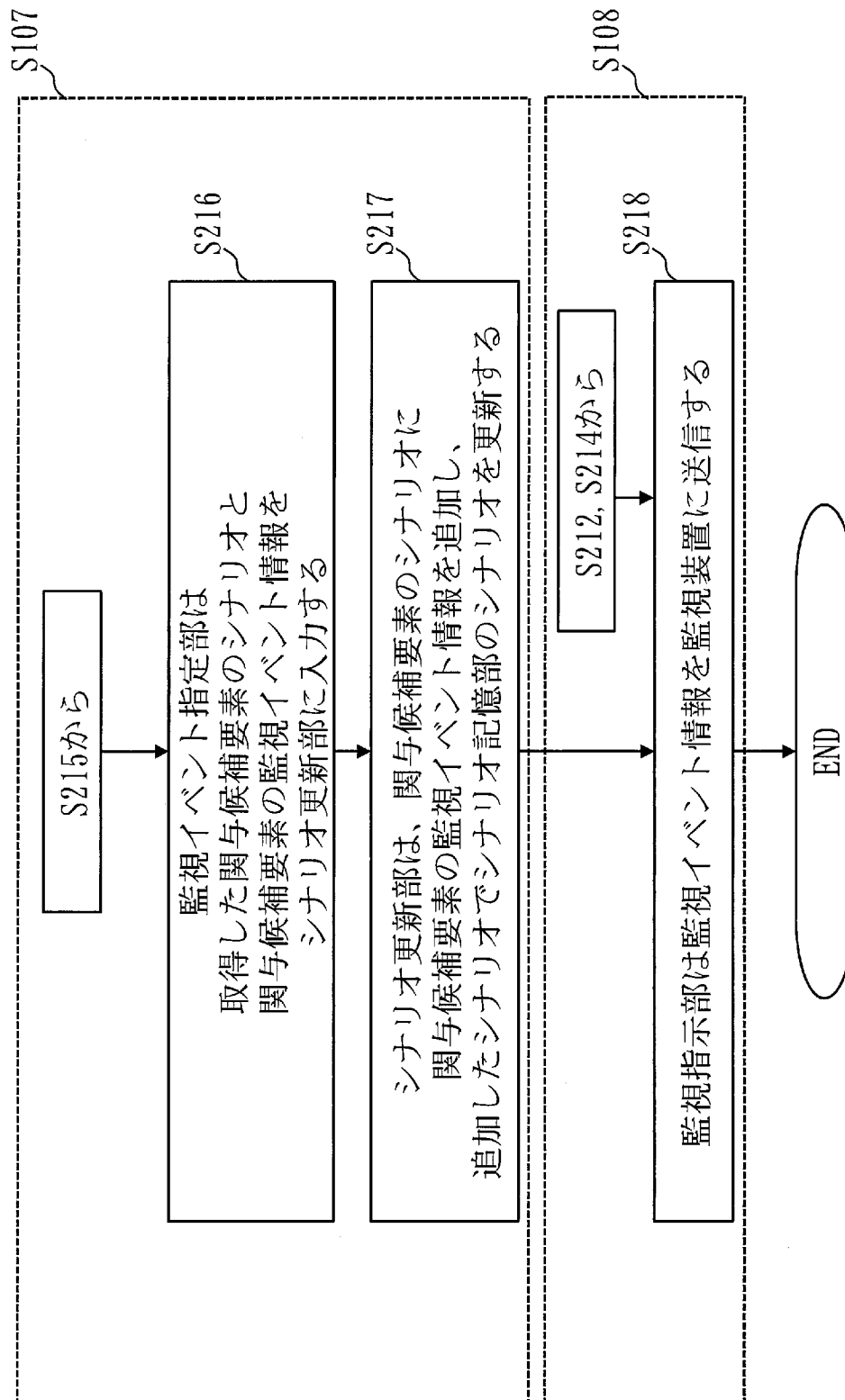
[図13]



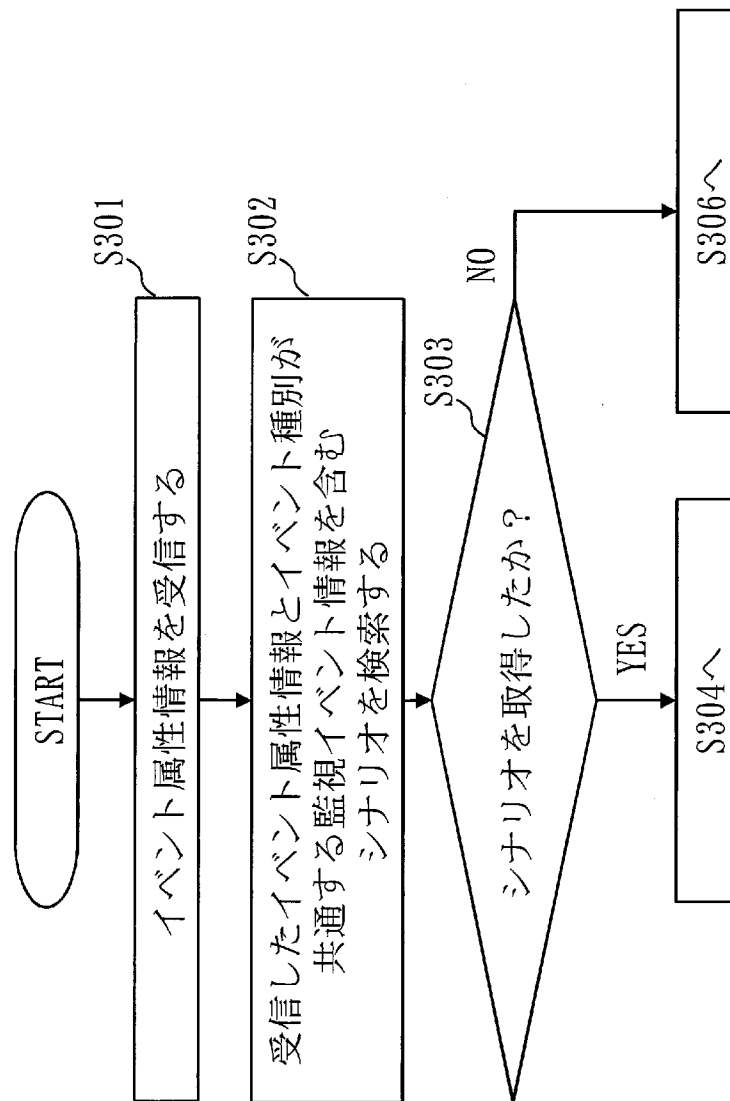
[図14]



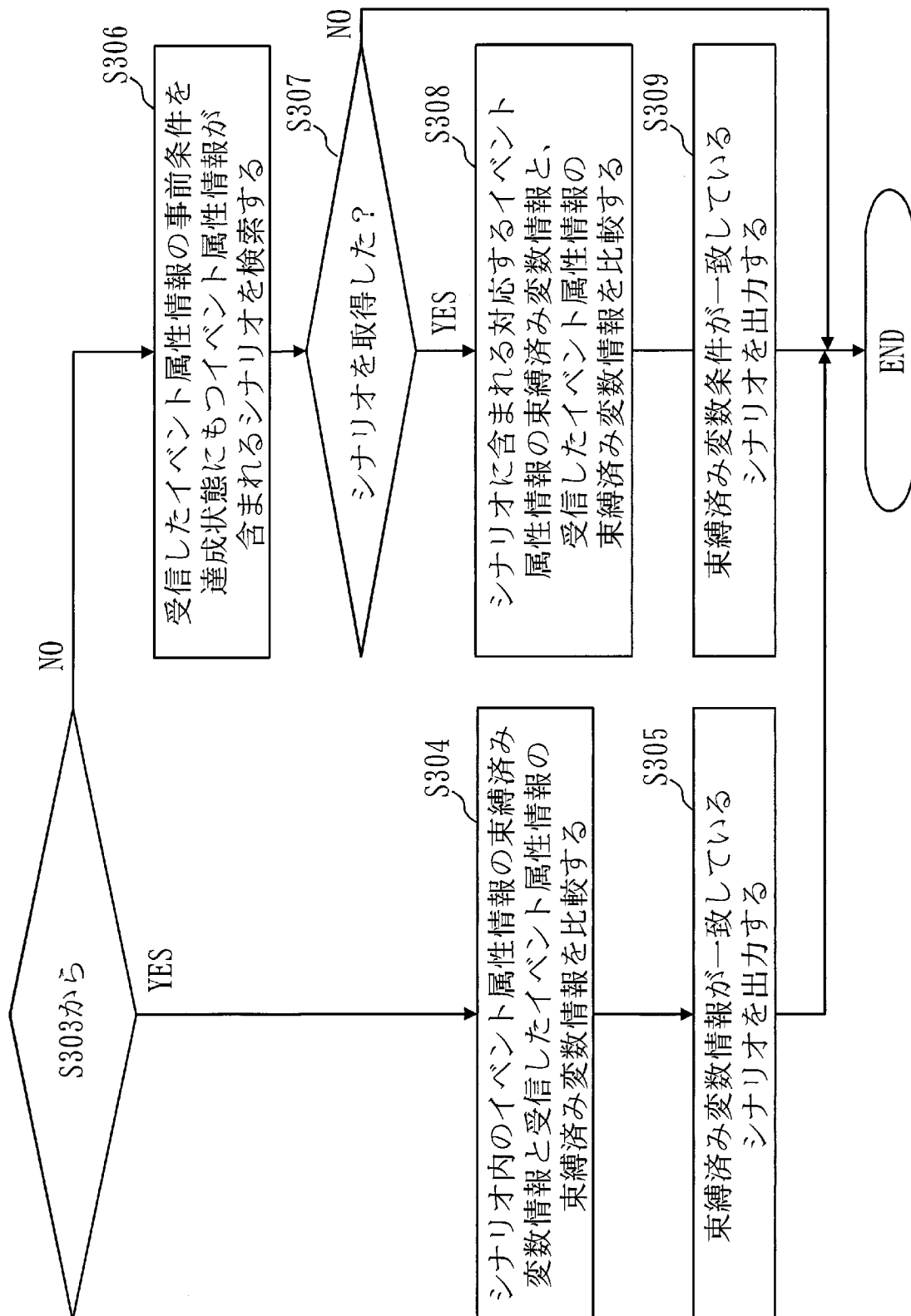
[図15]



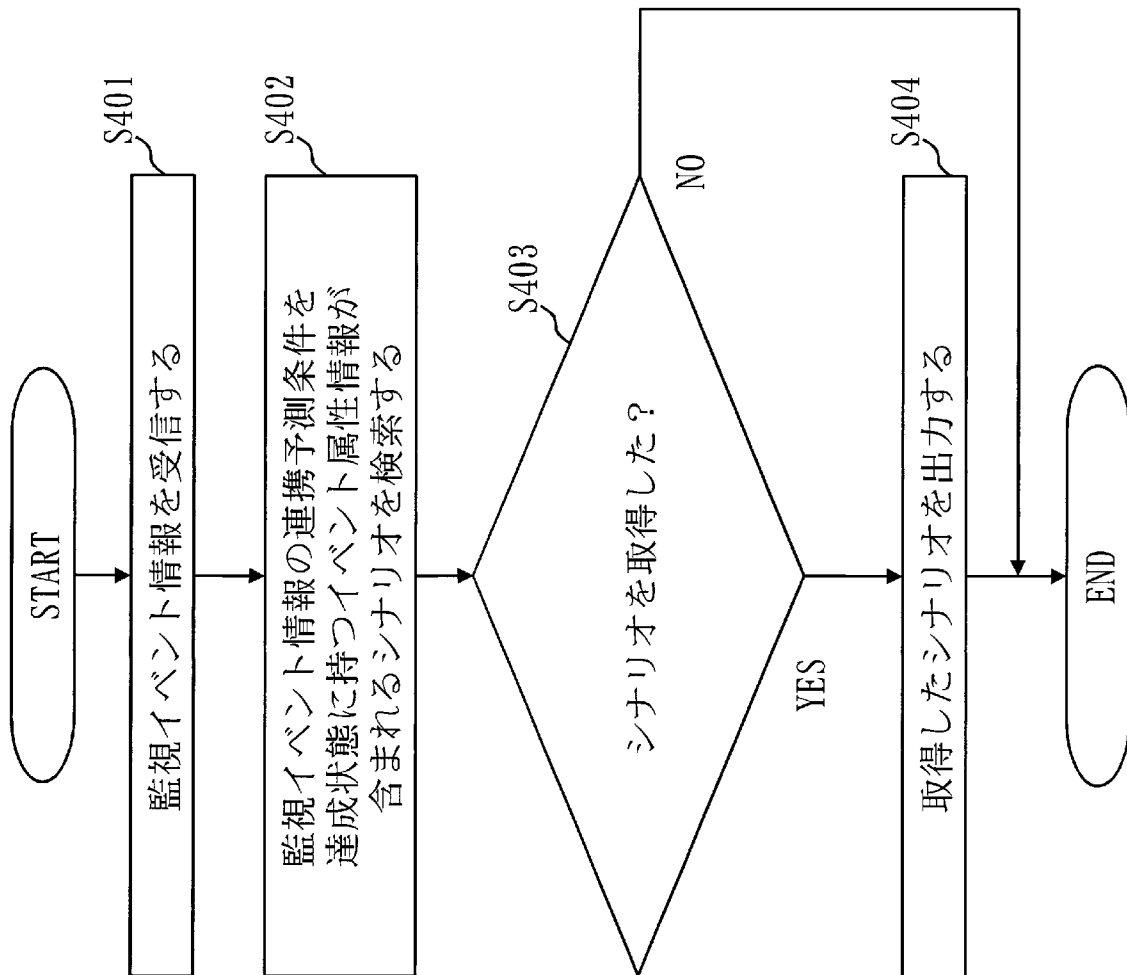
[図16]



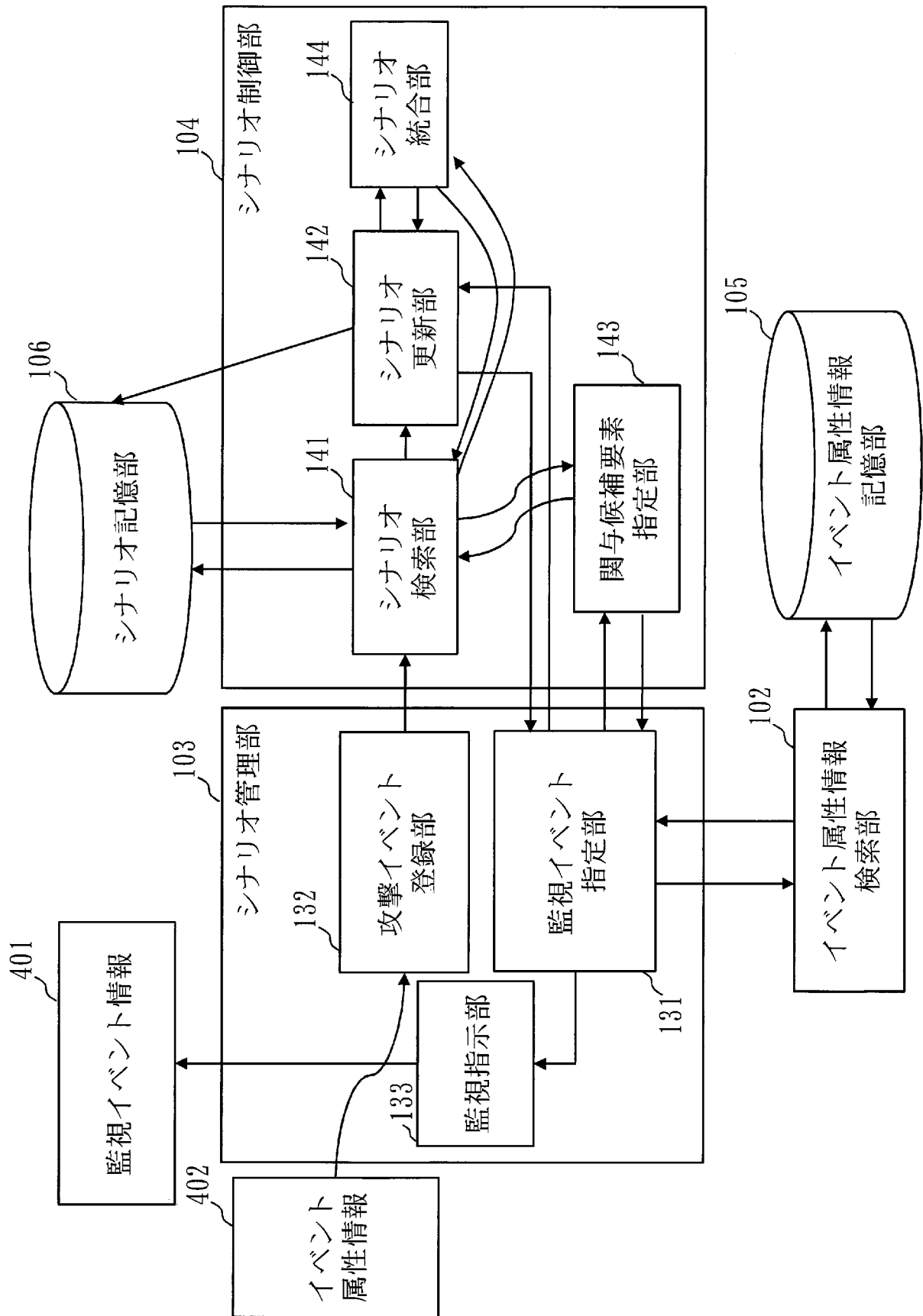
[図17]



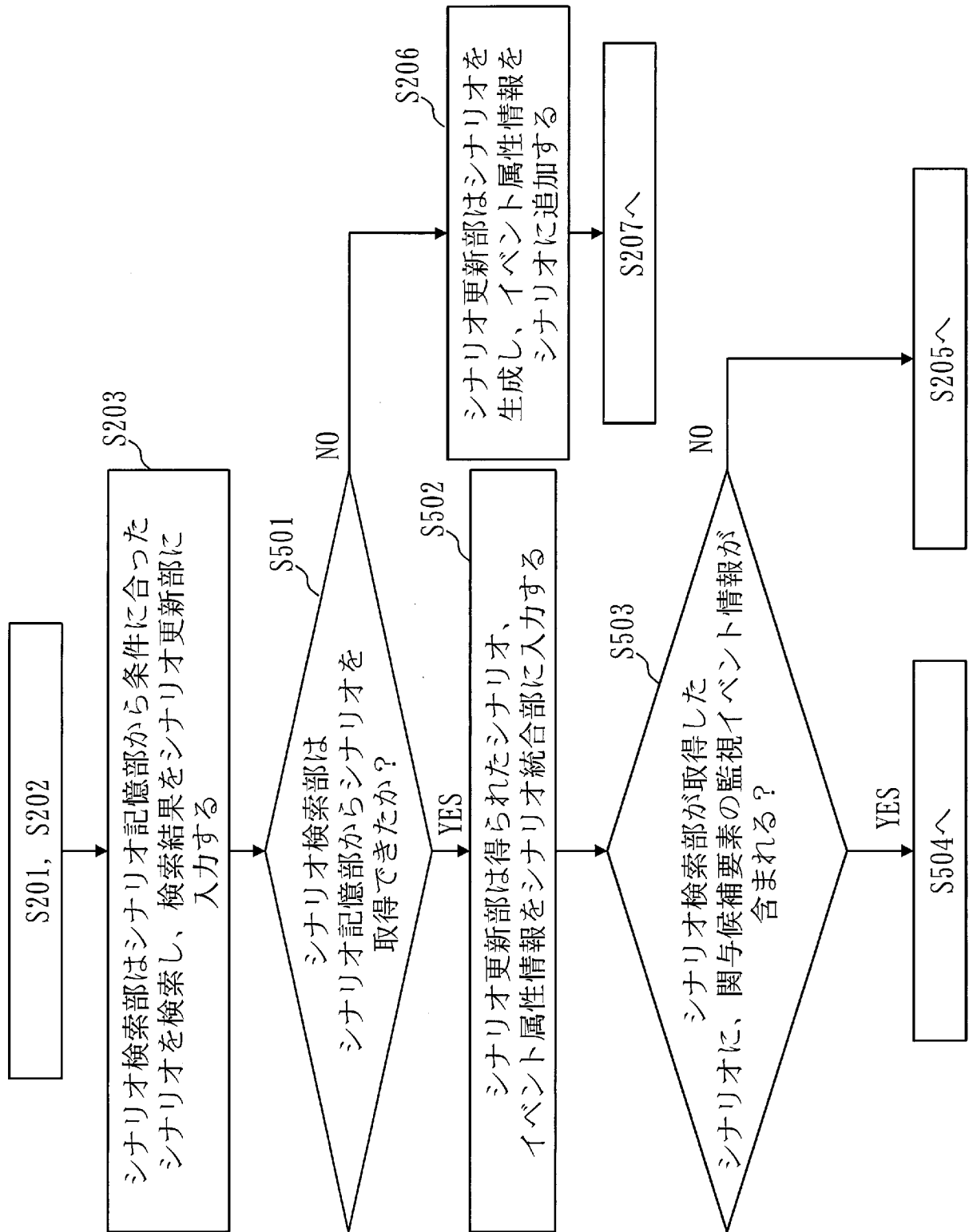
[図18]



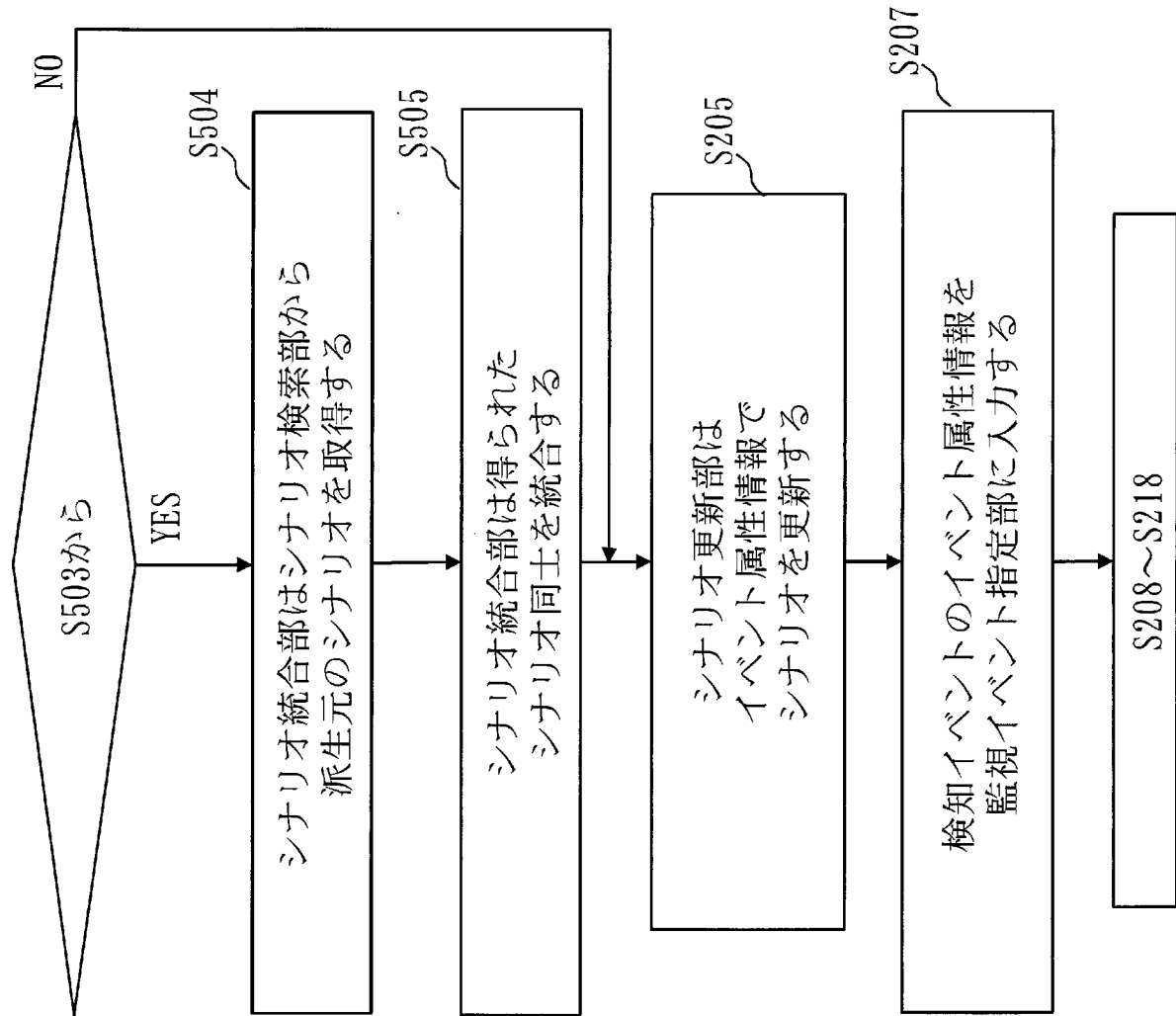
[図19]



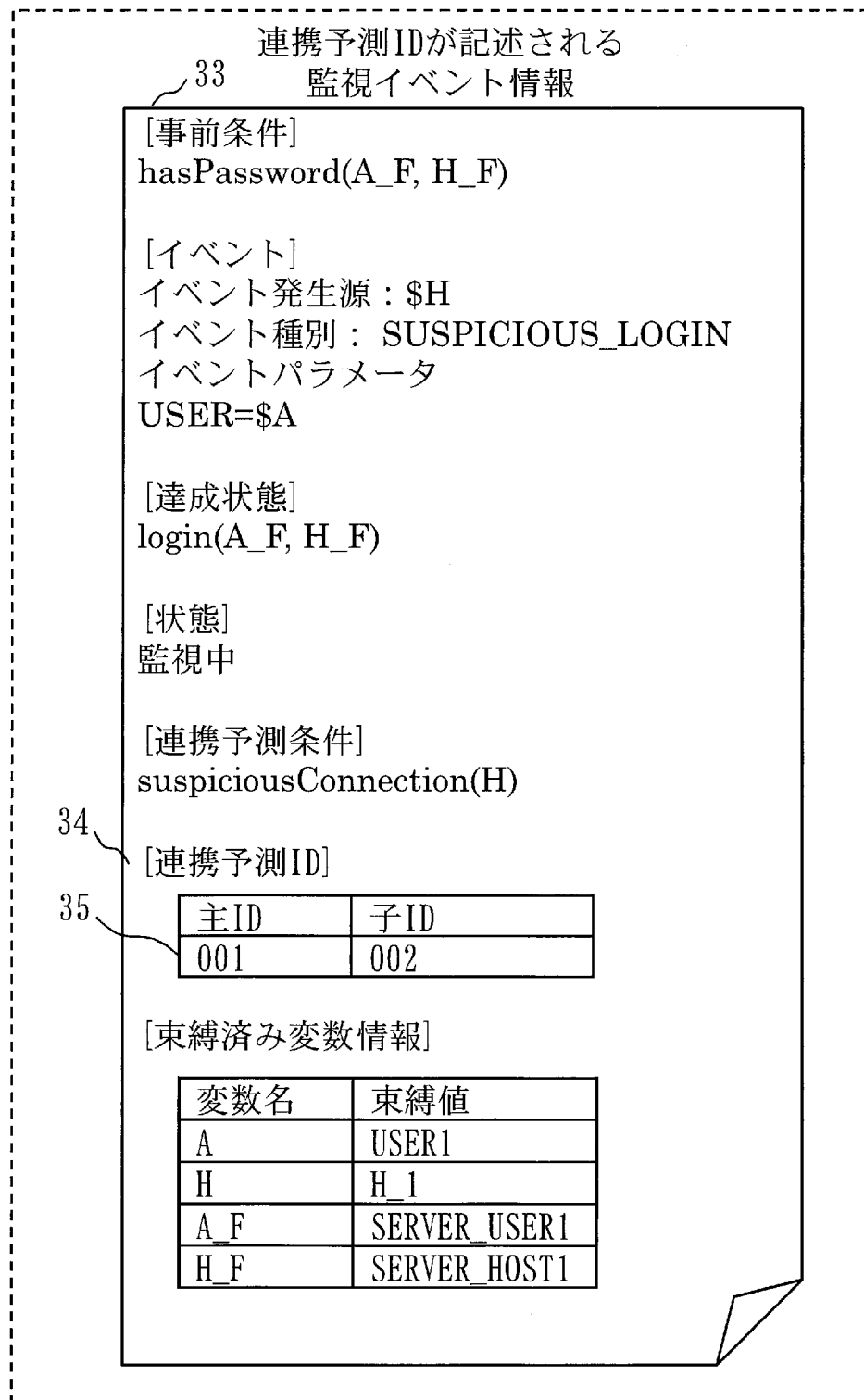
[図20]



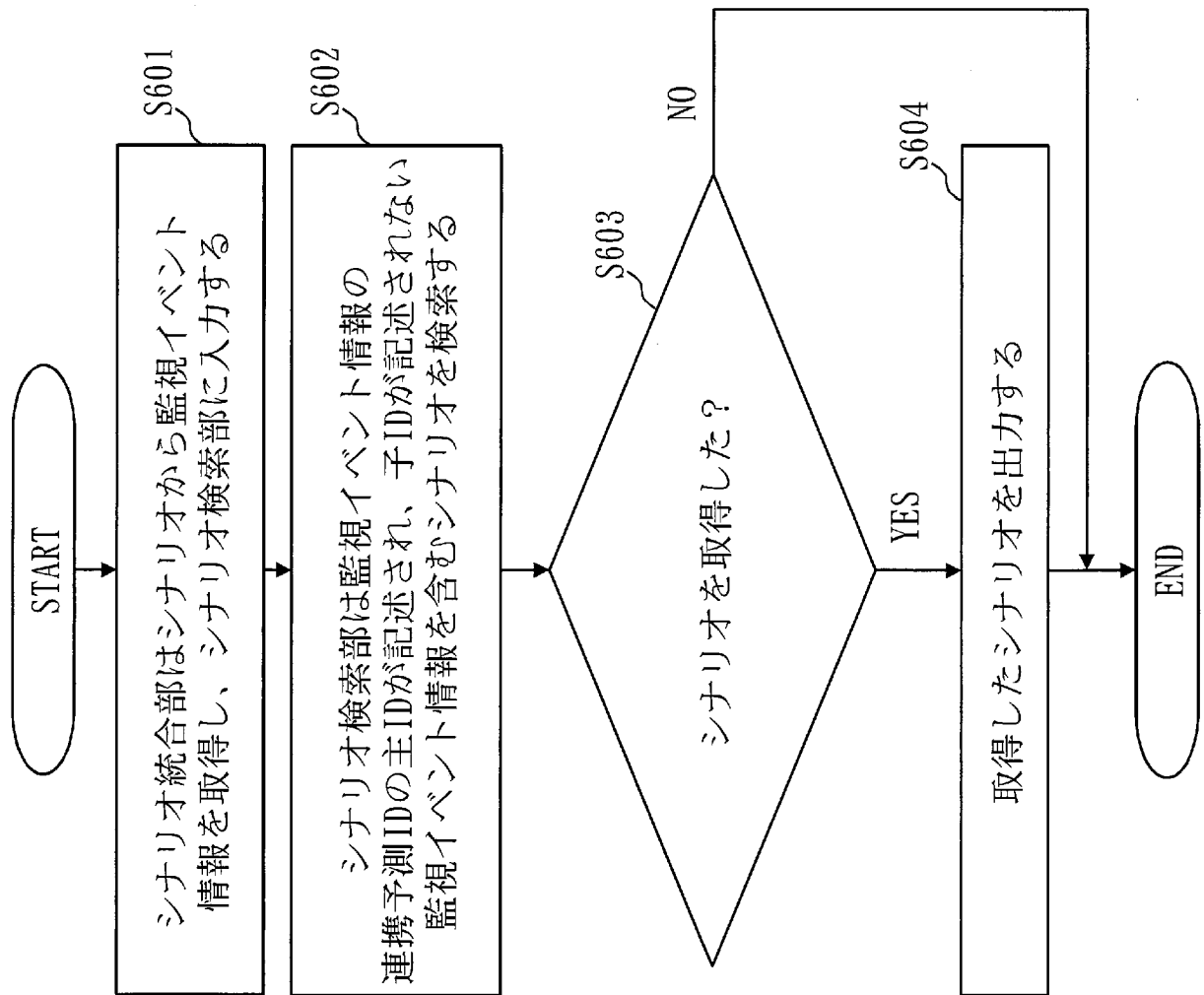
[図21]



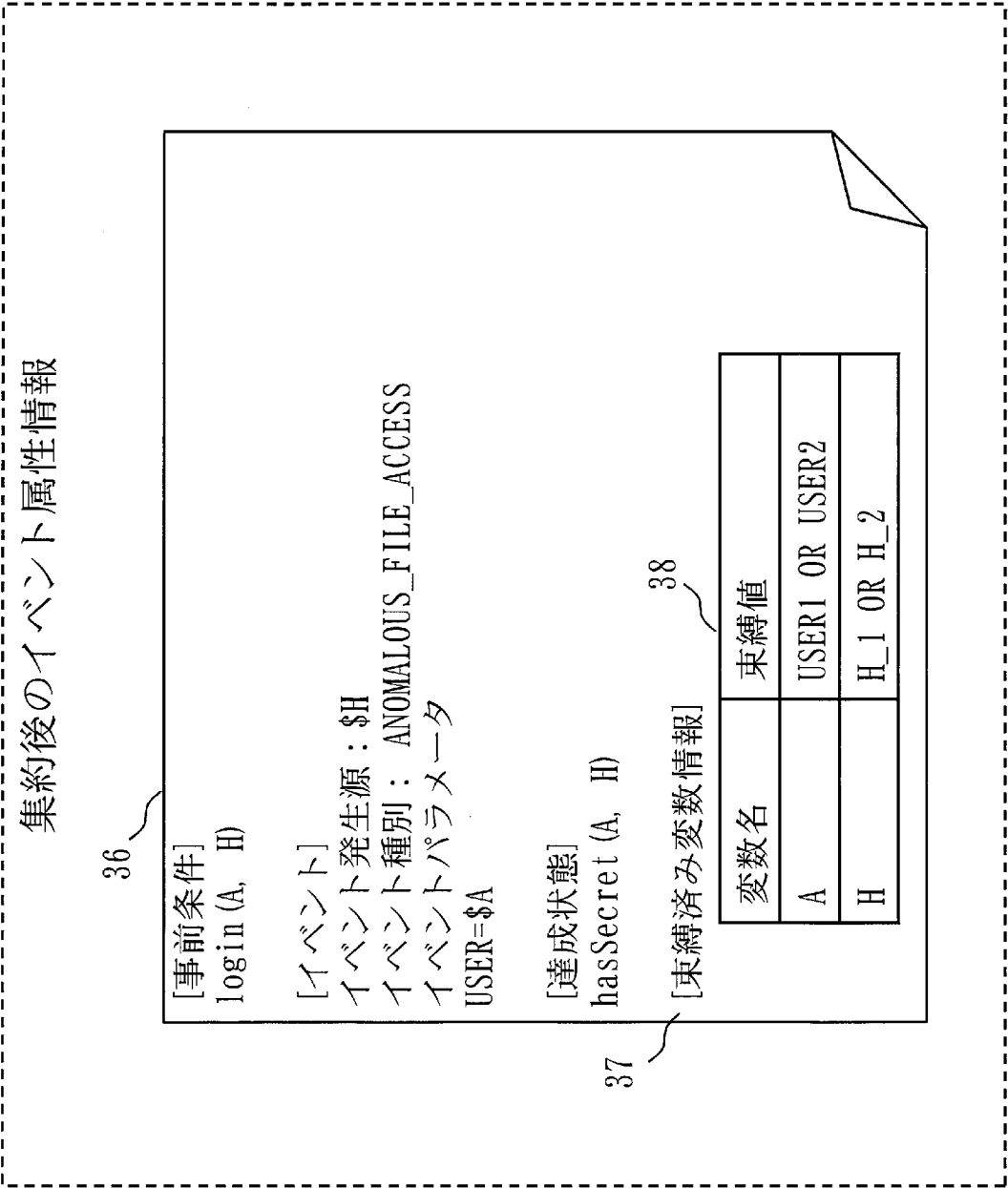
[図22]



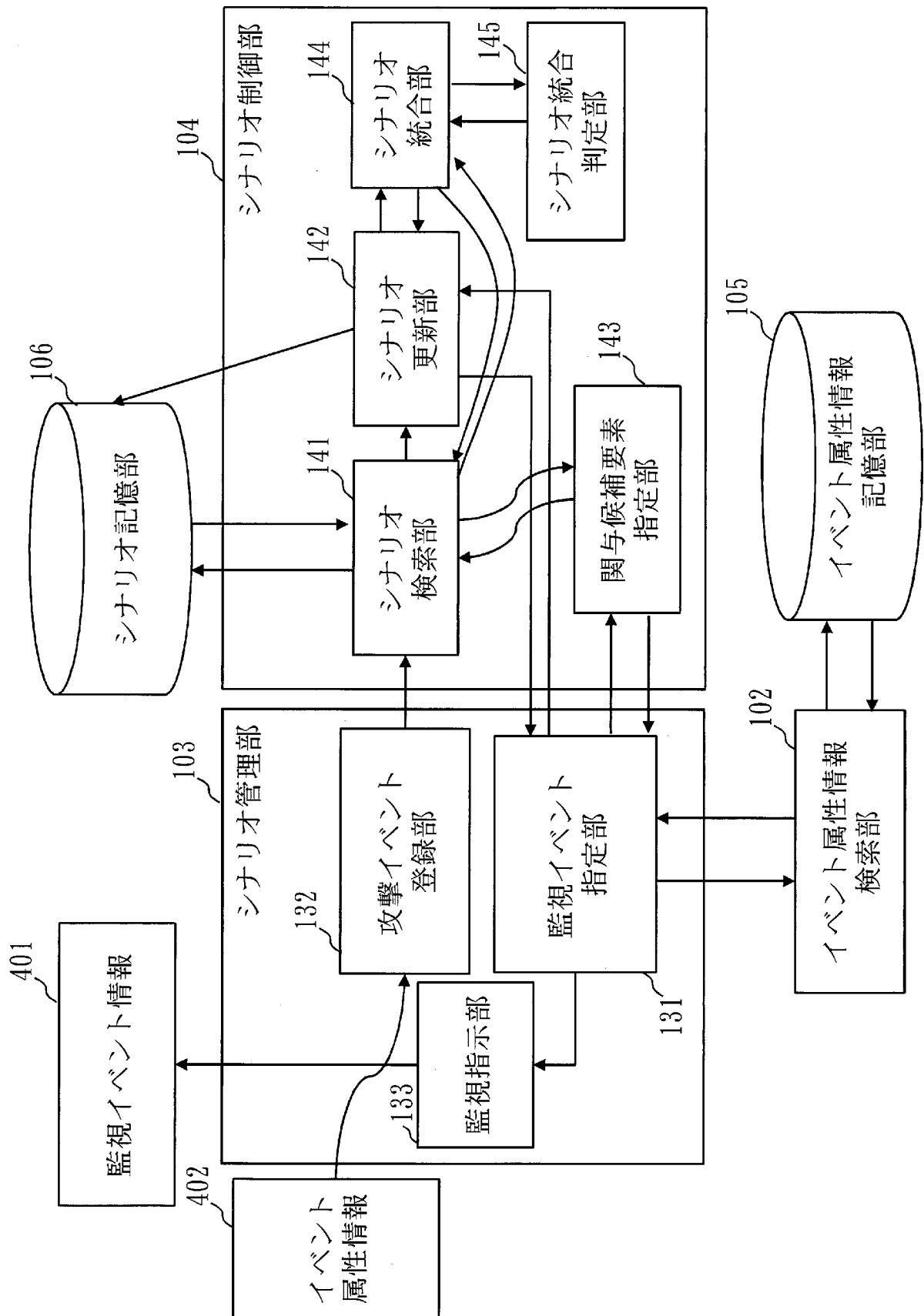
[図23]



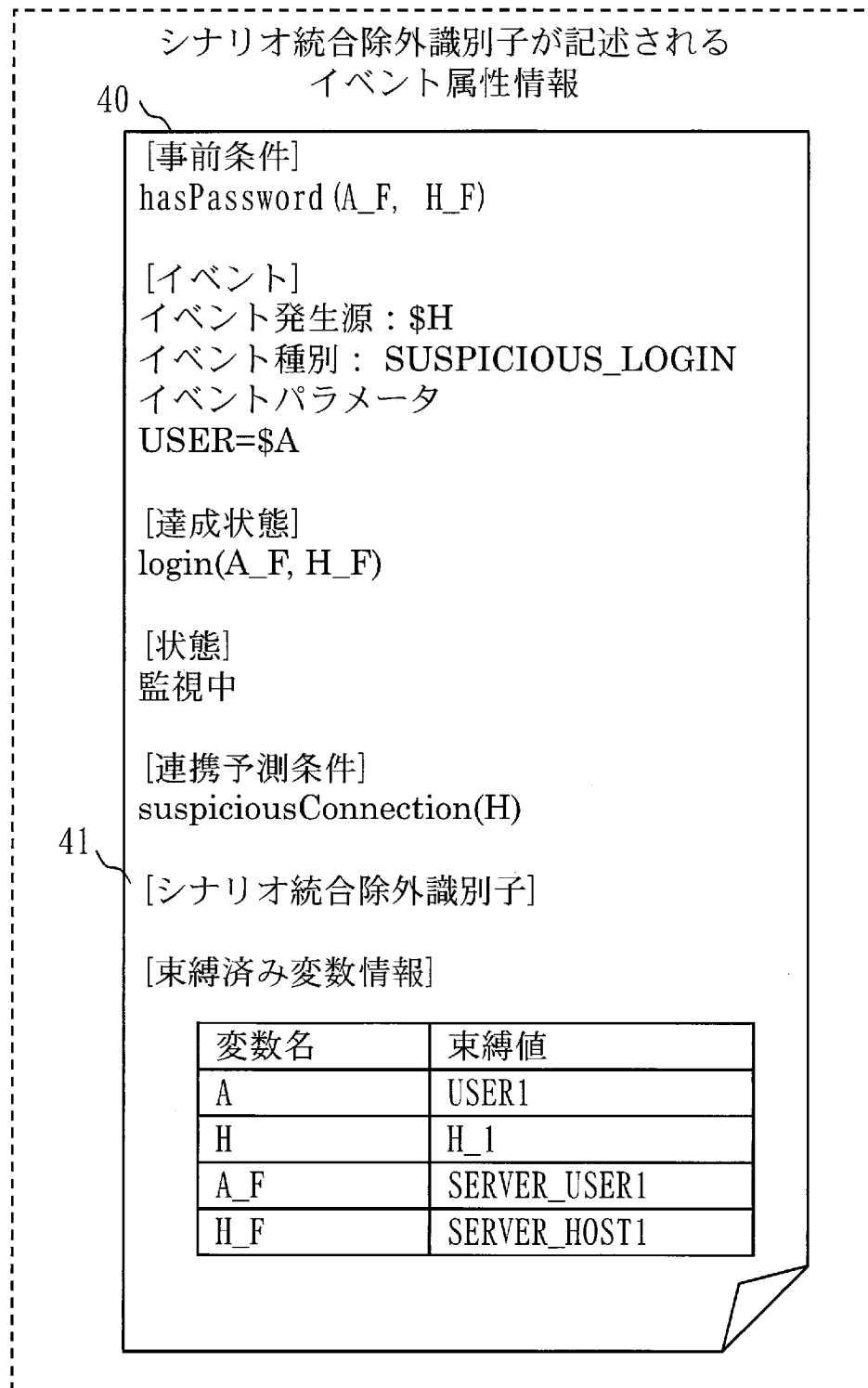
[図24]



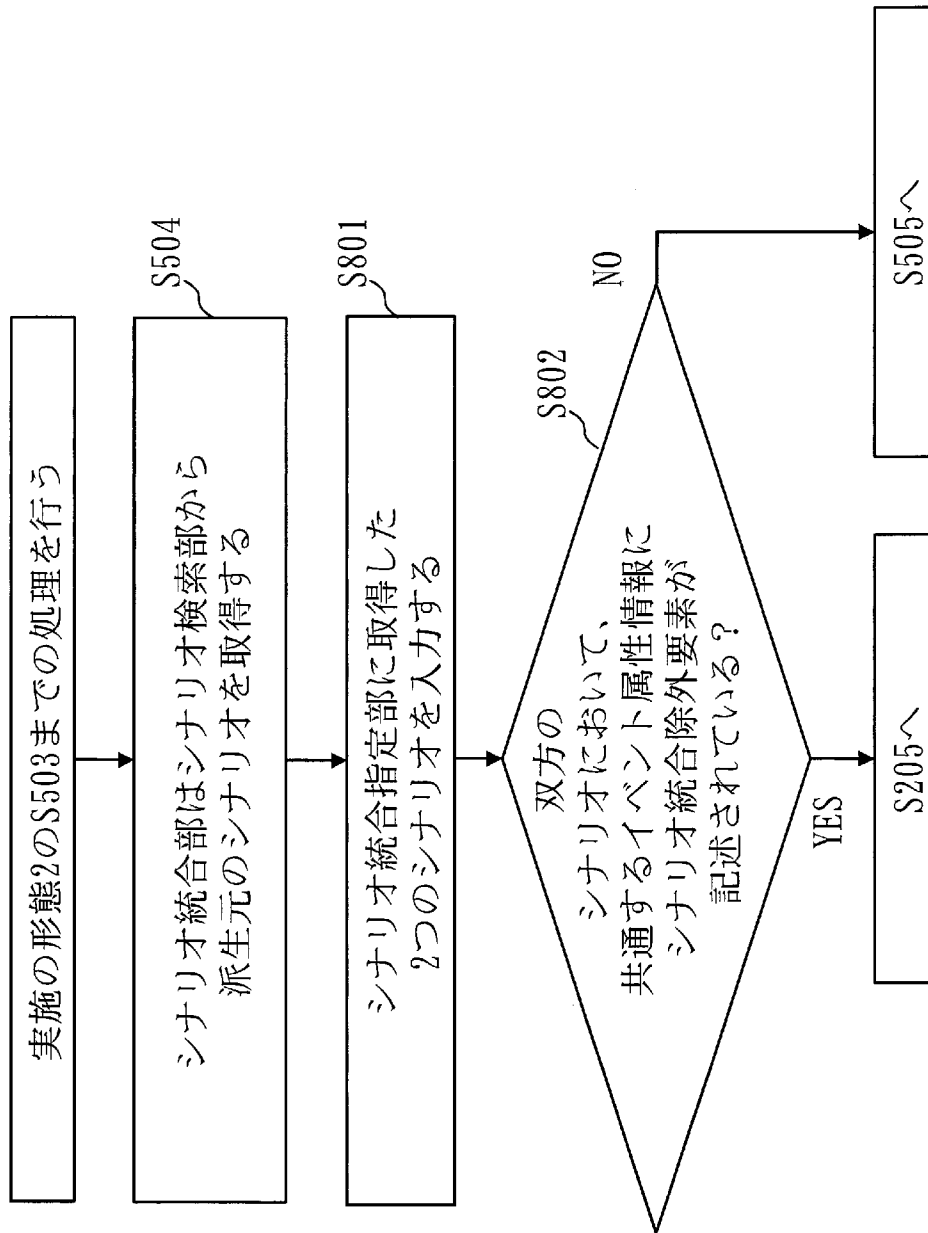
[図25]



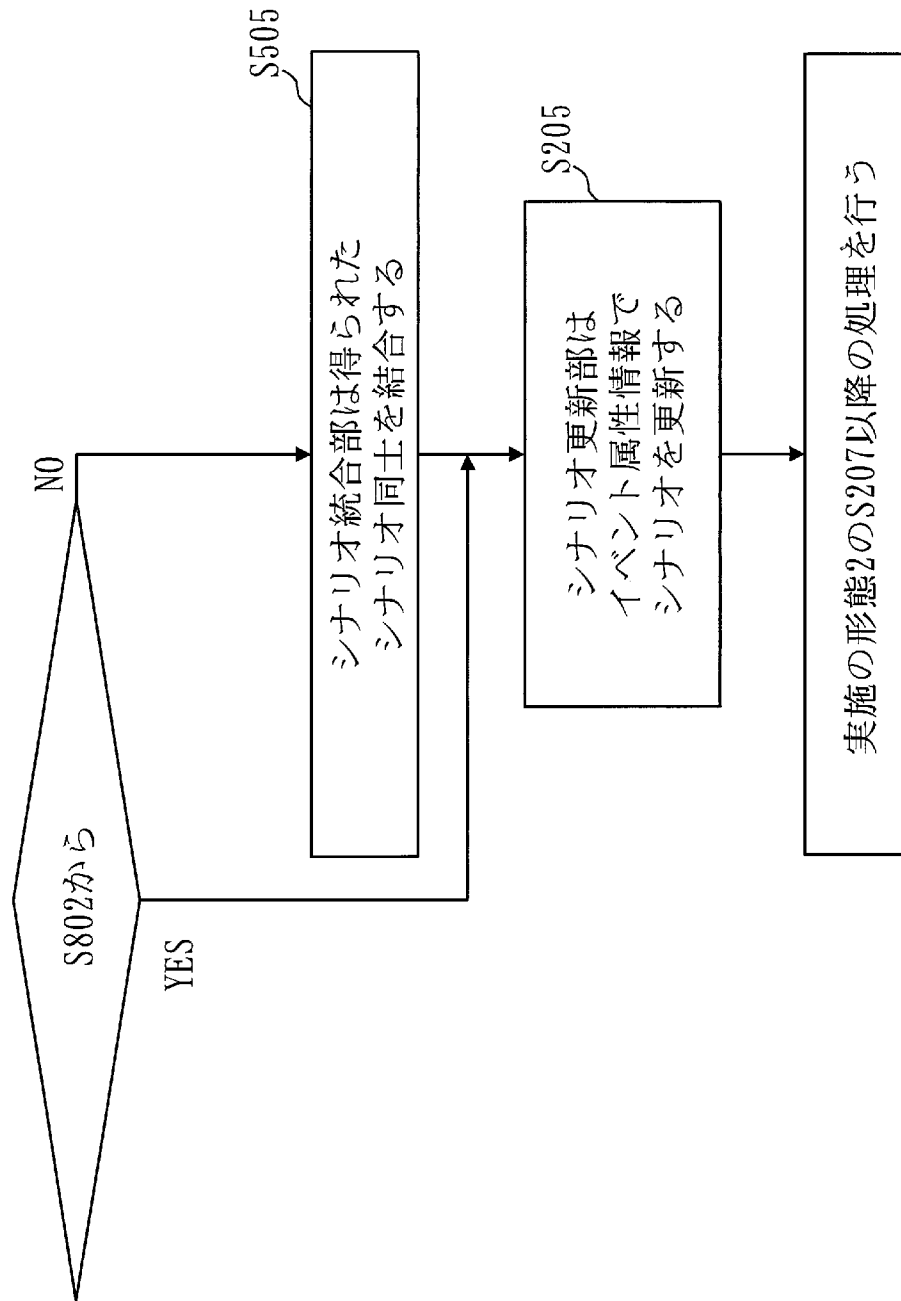
[図26]



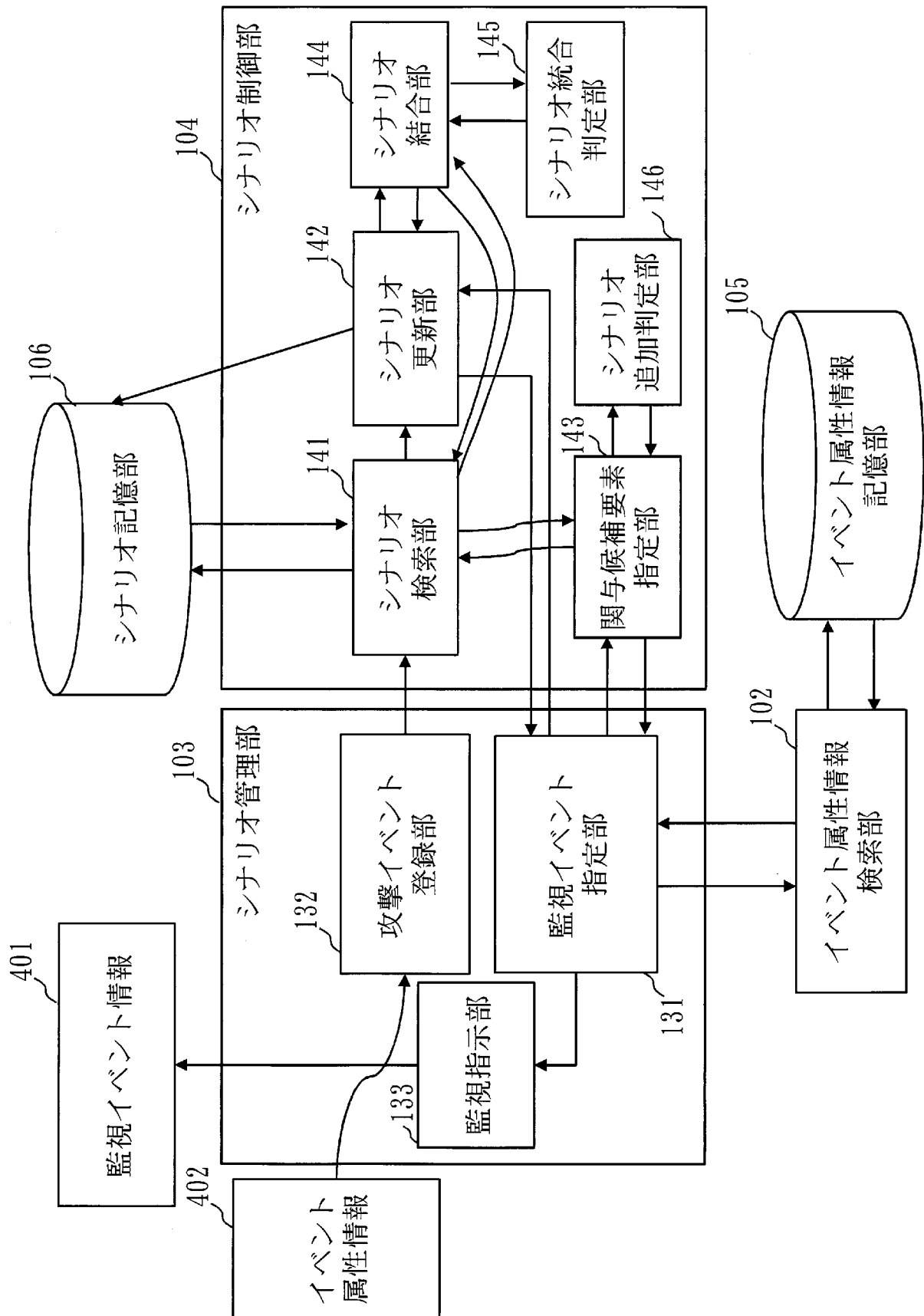
[図27]



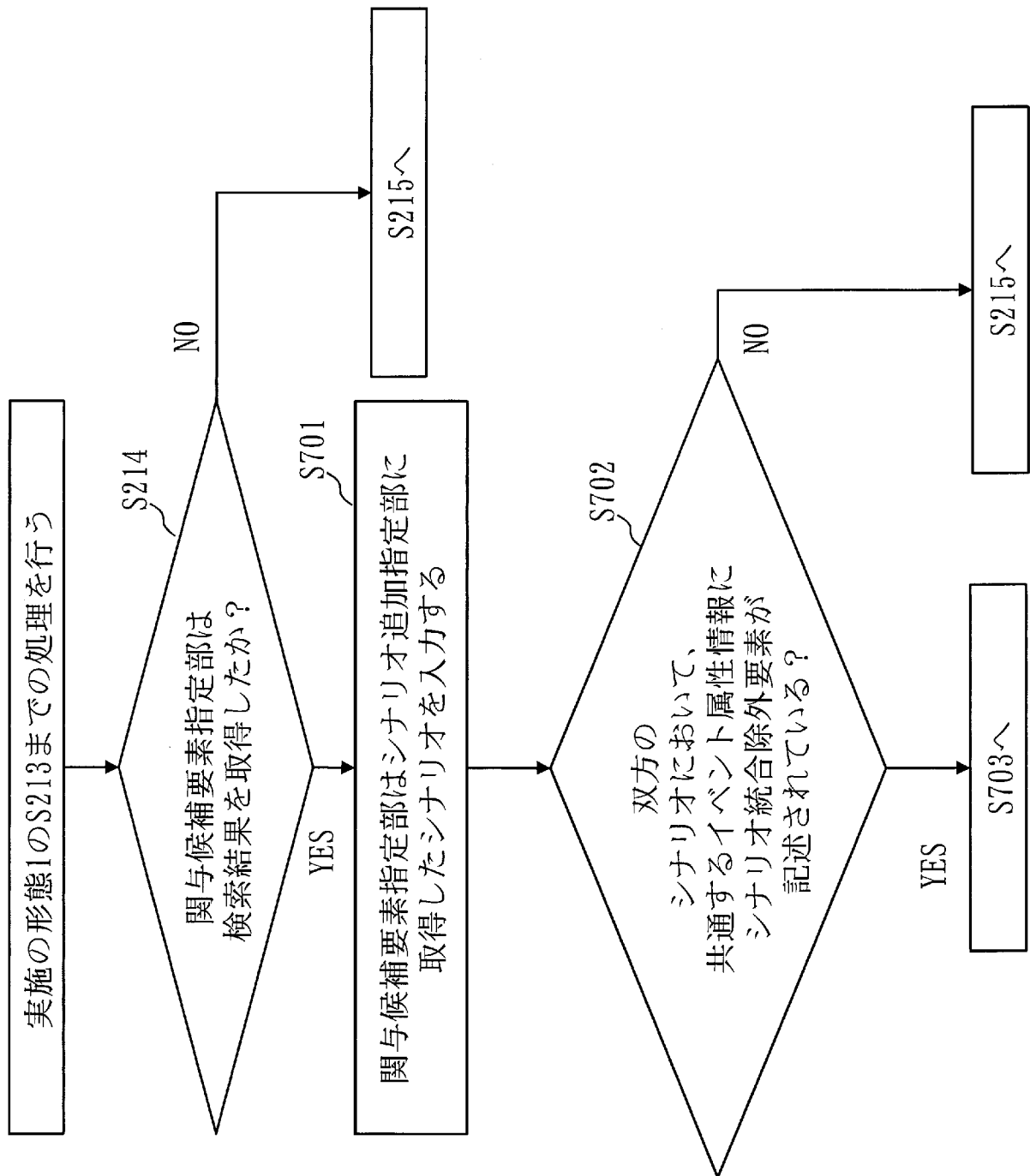
[図28]



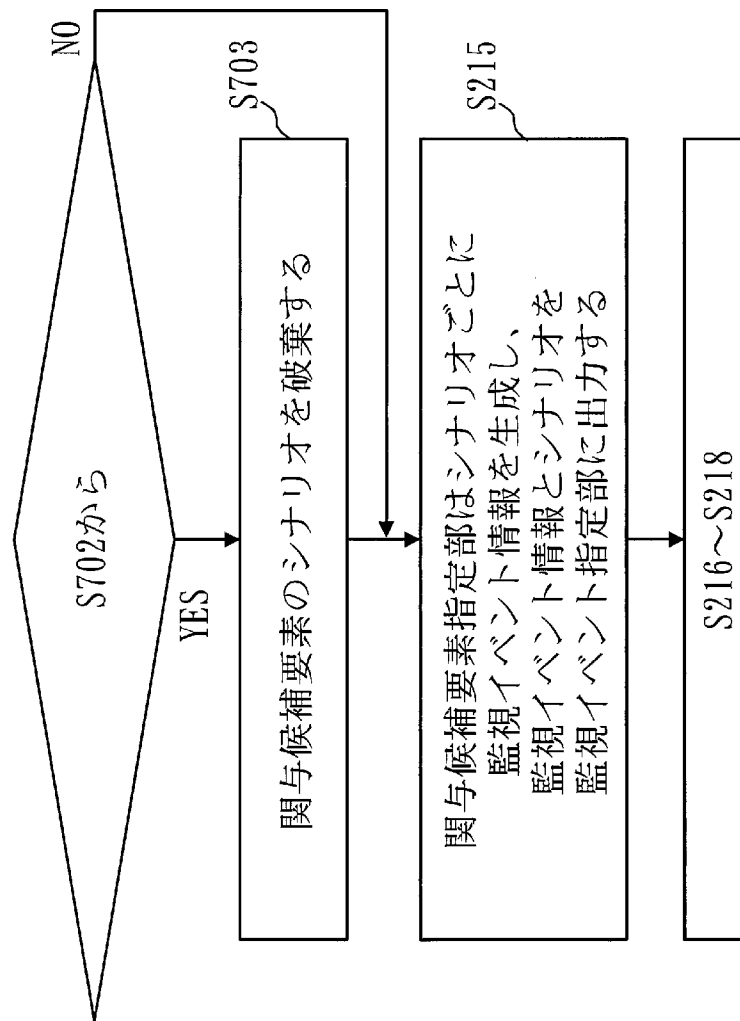
[図29]



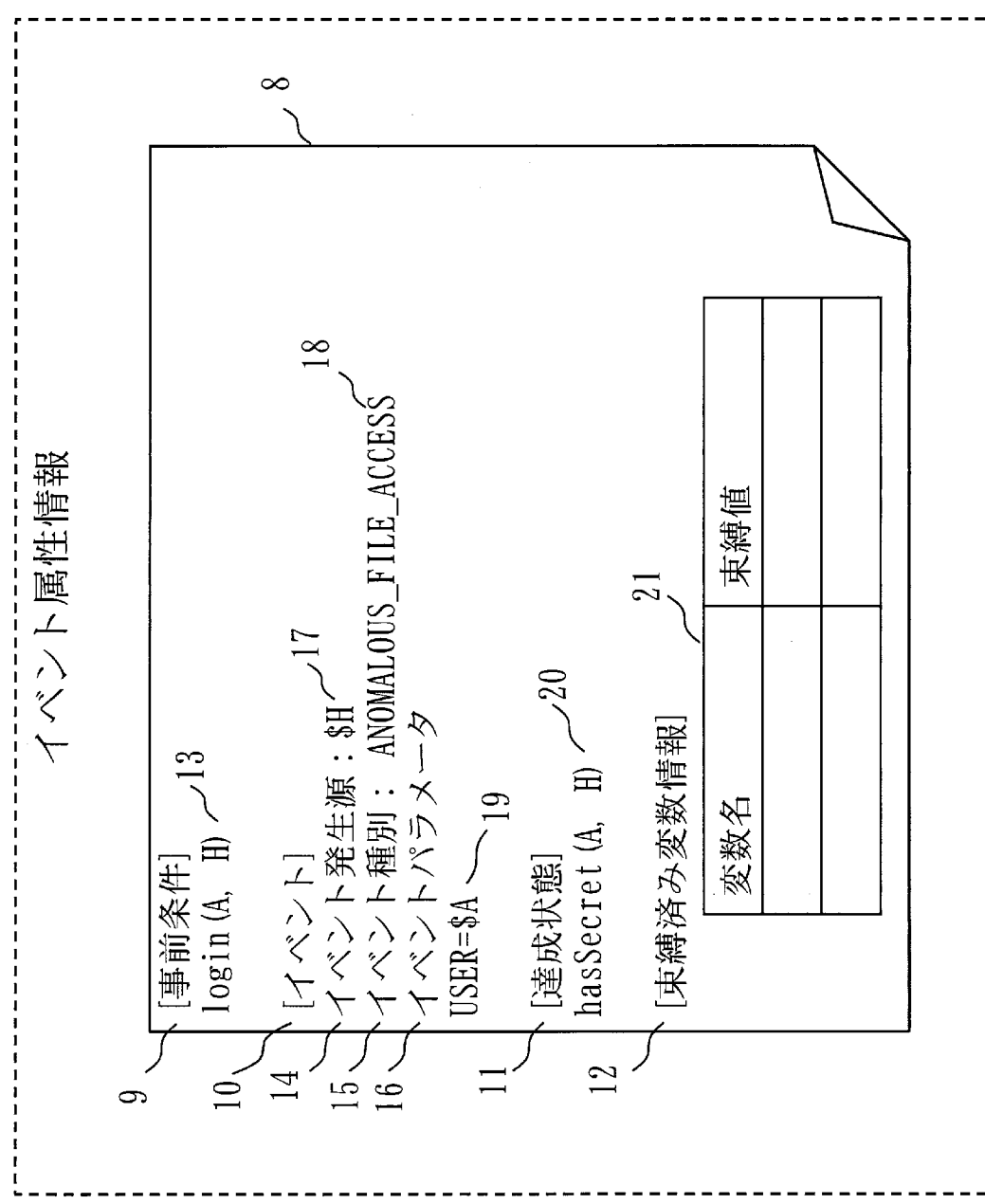
[図30]



[図31]



[図32]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2015/084931

A. CLASSIFICATION OF SUBJECT MATTER

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)

G06F21/55

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

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2016

Kokai Jitsuyo Shinan Koho 1971-2016 Toroku Jitsuyo Shinan Koho 1994-2016

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	WO 2015/059791 A1 (Mitsubishi Electric Corp.), 30 April 2015 (30.04.2015), abstract (Family: none)	1-11

☐ 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

15 February 2016 (15.02.16)

Date of mailing of the international search report

23 February 2016 (23.02.16)

Name and mailing address of the ISA/

Japan Patent Office

3-4-3, Kasumigaseki, Chiyoda-ku,

Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））

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（I P C））

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	1971-2016年
日本国実用新案登録公報	1996-2016年
日本国登録実用新案公報	1994-2016年

国際調査で利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	WO 2015/059791 A1（三菱電機株式会社）2015. 04. 30, [要約]（ファミリーなし）	1-11

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

15. 02. 2016

国際調査報告の発送日

23. 02. 2016

国際調査機関の名称及びあて先

日本国特許庁（I S A/J P）

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）

平井 誠

電話番号 03-3581-1101 内線 3546

5 S

9071