(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
2014 年 4 月 3 日(03.04.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/050424 A1

(51) 国際特許分類:
G06F 21/56 (2013.01)

(21) 国際出願番号: PCT/JP2013/073198

(22) 国際出願日: 2013 年 8 月 29 日(29.08.2013)

(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 2012-211291 2012 年 9 月 25 日(25.09.2012) 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: 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　ＮＴＡ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, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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.

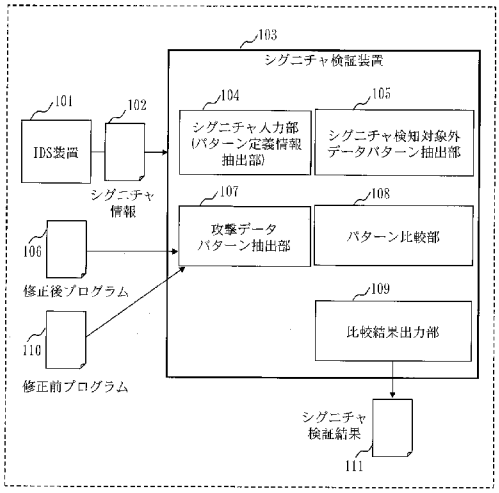
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,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

WO 2014/050424 A1

(54) **Title**: SIGNATURE VERIFICATION DEVICE, SIGNATURE VERIFICATION METHOD, AND PROGRAM

(54) 発明の名称 : シグニチャ検証装置及びシグニチャ検証方法及びプログラム



101 IDS device
102 Signature information
103 Signature verification device
104 Signature input unit (pattern definition information extraction unit)
105 Signature detection excluded data pattern extraction unit
106 Program after correction
107 Attack data pattern extraction unit
108 Pattern comparison unit
109 Comparison result output unit
110 Program before correction
111 Signature verification result

(57) **Abstract**: To determine, without performing an enormous number of verifications, whether or not an attack that cannot be detected using signature information exists. A signature detection excluded data pattern extraction unit (105) performs analysis on signature information (102), and extracts patterns of data not detected using the signature information (102). An attack data pattern extraction unit (107) performs analysis on a target program for which the signature information (102) is applied, and extracts patterns of attack data for attacking the target program. A pattern comparison unit (108) compares the signature detection excluded data patterns that have been extracted by the signature detection excluded data pattern extraction unit (105) with the attack data patterns that have been extracted by the attack data pattern extraction unit (107), and extracts attack data patterns corresponding to the signature detection excluded data patterns as attack data patterns that are not detected using the signature information (102).

(57) 要約:　膨大な数の検証を行わずに、シグニチャ情報で検知できない攻撃が存在するか否かを判別する。シグニチャ検知対象外データパターン抽出部１０５は、シグニチャ情報１０２に対する解析を行い、シグニチャ情報１０２では検知されないデータのパターンを抽出する。攻撃データパターン抽出部１０７は、シグニチャ情報１０２が適用される対象プログラムに対する解析を行い、対象プログラムを攻撃する攻撃データのパターンを抽出する。パターン比較部１０８は、シグニチャ検知対象外データパターン抽出部１０５により抽出されたシグニチャ検知対象外データパターンと攻撃データパターン抽出部１０７により抽出された攻撃データパターンとを比較し、シグニチャ検知対象外データパターンに該当する攻撃データパターンを、シグニチャ情報１０２では検知されない攻撃データパターンとして抽出する。

明　細　書

発明の名称 ：

シグニチャ検証装置及びシグニチャ検証方法及びプログラム

技術分野

[0001] 本発明は、シグニチャ情報（以下、単にシグニチャともいう）を検証する技術に関する。

なお、シグニチャ情報とは、攻撃を行うためのコマンドやデータの特徴が記述された情報である。

背景技術

[0002] 侵入検知装置（Ｉｎｔｒｕｓｉｏｎ Ｄｅｔｅｃｔｉｏｎ Ｓｙｓｔｅｍ：ＩＤＳ）のシグニチャを検証する技術としては、例えば特許文献１にあるように、実際に攻撃を行うプログラムを実行し、プログラムから送信される通信に対して攻撃の検知が行えるか確認する方法が知られている。

先行技術文献

特許文献

[0003] 特許文献1：特開２００７－２４２００２号公報

非特許文献

[0004] 非特許文献1：Ｂｒｕｍｌｅｙ Ｄ．他 Ａｕｔｏｍａｔｉｃ ｐａｔｃｈ－ｂａｓｅｄ ｅｘｐｌｏｉｔ ｇｅｎｅｒａｔｉｏｎ ｉｓ ｐｏｓｓｉｂｌｅ：Ｔｅｃｈｎｉｑｕｅｓ ａｎｄ ｉｍｐｌｉｃａｔｉｏｎｓ．Ｉｎ：Ｐｒｏｃ ｏｆ ｔｈｅ ２００８ ＩＥＥＥ Ｓｙｍｐｏｓｉｕｍ ｏｎ Ｓｅｃｕｒｉｔｙ ａｎｄ Ｐｒｉｖａｃｙ （２００８）

発明の概要

発明が解決しようとする課題

[0005] ＩＤＳは、シグニチャと呼ばれるパターン情報と監視対象ネットワークを流れるトラフィックとを比較し、パターンに合致するトラフィックがネット

ワークを流れた場合に当該トラフィックを攻撃とみなす。

シグニチャは、検知対象とする攻撃ごとに定義されている。

シグニチャに合致する通信が発生した場合に、そのシグニチャが検知対象としている攻撃が発生したとして、ネットワーク管理者に通報が行われる。

[0006] シグニチャは、新たな攻撃が発見される度にＩＤＳの開発元が作成し、定期的、あるいは必要に応じて装置のユーザに配布されるのが一般的である。

但し、そのシグニチャが、検知対象としている攻撃を全て検出できるかどうかの情報については非公開である。

ユーザがシグニチャを検証するには、ユーザが実際に攻撃ツールを入手して攻撃トラフィックを生成してＩＤＳに入力し、検知が行えるかどうかを判定する必要がある。

使用された攻撃ツールの生成するトラフィックが全ての攻撃パターンを網羅していない限り、実際にはシグニチャに検知漏れの可能性があってもユーザは認識することができない。

[0007] 攻撃に利用可能なプログラムの脆弱性に対し、修正が施されたプログラムと修正前のプログラムとを比較して、修正後のプログラムで追加、変更された命令から脆弱性を攻撃するデータを生成する手法として例えば非特許文献１に挙げられる技術が知られている。

このような技術を使用しても、実際にシグニチャが生成される攻撃データ全てに対して検知可能であるかは、実際に生成したデータを使ってＩＤＳで試験するしかなく、攻撃データのバリエーションが膨大である場合、試験が終了しないという課題がある。

[0008] この発明は上記のような課題を解決することを主な目的の１つとしており、膨大な数の検証を行わずに、シグニチャ情報で検知できない攻撃が存在するか否かを判別することを主な目的とする。

課題を解決するための手段

[0009] 本発明に係るシグニチャ検証装置は、

シグニチャ情報に対する解析を行い、前記シグニチャ情報では検知されな

いデータのパターンを抽出するシグニチャ検知対象外データパターン抽出部と、

前記シグニチャ情報が適用される対象プログラムに対する解析を行い、前記対象プログラムを攻撃する攻撃データのパターンを抽出する攻撃データパターン抽出部と、

前記シグニチャ検知対象外データパターン抽出部により抽出されたシグニチャ検知対象外データパターンと前記攻撃データパターン抽出部により抽出された攻撃データパターンとを比較し、シグニチャ検知対象外データパターンに該当する攻撃データパターンを、前記シグニチャ情報では検知されない攻撃データパターンとして抽出するパターン比較部とを有することを特徴とする。

発明の効果

[0010] 本発明によれば、シグニチャ情報に対する解析結果と、シグニチャ情報が適用される対象プログラムに対する解析結果とに基づき、シグニチャ情報では検知されない攻撃データパターンを抽出するため、膨大な数の検証を行わなくても、シグニチャ情報で検知できない攻撃が存在するか否かを判別することができる。

図面の簡単な説明

[0011] [図1]実施の形態１に係るシグニチャ検証装置の構成例を示す図。

[図2]実施の形態１に係るシグニチャ検知対象外データパターン抽出部の動作例を示すフローチャート図。

[図3]実施の形態１に係るシグニチャ検知対象外データパターン抽出例を示す図。

[図4]実施の形態１に係る攻撃データパターン抽出部の動作例を示すフローチャート図。

[図5]実施の形態１に係る正規表現化のための変換テーブルの例を示す図。

[図6]実施の形態１に係るパターン比較部の動作例を示すフローチャート図。

[図7]実施の形態１に係る比較結果出力部の動作例を示すフローチャート図。

[図8]実施の形態２に係るシグニチャ検証装置の構成例を示す図。

[図9]実施の形態２に係る比較結果検証部の動作例を示すフローチャート図。

[図10]実施の形態２に係る「文字列生成」手続きを示すフローチャート図。

[図11]実施の形態１及び２に係るシグニチャ検証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] 実施の形態１.

本実施の形態では、攻撃データのパターンと、シグニチャとを直接比較することにより、膨大な数の検証を行うことなくシグニチャの漏れがあるかどうかを識別する例を説明する。

[0013] 図１は、本実施の形態に係るシグニチャ検証装置１０３の構成例を示す。

[0014] シグニチャ検証装置１０３は、ＩＤＳ装置１０１から取り出されたシグニチャ情報１０２、修正前プログラム１１０及び修正後プログラム１０６を受け取る。

また、シグニチャ検証装置１０３は、シグニチャ情報１０２に記載の検知パターンが、検知対象としている脆弱性攻撃を漏れなく検知できるかどうかを示すシグニチャ検証結果１１１を出力する。

修正前プログラム１１０は、シグニチャ情報１０２が検知対象としている脆弱性攻撃が対象とするプログラムであって、脆弱性に対する修正が行われる前のプログラムである。

修正後プログラム１０６は、修正前プログラム１１０において脆弱性に対する修正が行われた後のプログラムである。

[0015] 本実施の形態ではシグニチャ情報１０２をＩＤＳ装置１０１から取り出す方法を開示しているが、例えばＩＤＳ開発元のウェブサイトからシグネチャ情報１０２を直接ダウンロードするような構成とすることももちろん可能である。

また、本実施の形態では、シグニチャ検証装置１０３は、修正前プログラム１１０、修正後プログラム１０６を入力しているが、その他にも例えば修

正前プログラム及び、修正用の差分情報（いわゆるパッチ）を入力とすることも可能である。

また、プログラムが自由にインターネットからダウンロード可能な場合、シグニチャ検証装置１０３は、定期的にインターネットからプログラムをダウンロードしておくことで、任意の時点での修正前、修正後プログラムを自動で入手することも可能である。

[0016] シグニチャ検証装置１０３は、シグニチャ入力部１０４、シグニチャ検知対象外データパターン抽出部１０５、攻撃データパターン抽出部１０７、パターン比較部１０８、比較結果出力部１０９で構成されている。

[0017] シグニチャ入力部１０４は、シグニチャ情報１０２をシグニチャ検証装置１０３内部に取り込み、シグニチャ情報１０２内に定義されている、検知対象とするデータのパターン定義情報を取り出す。

つまり、シグニチャ入力部１０４は、シグニチャ情報１０２から、シグニチャ情報１０２が検知の対象とするデータのパターンが定義されるパターン定義情報を抽出する。

シグニチャ入力部１０４は、パターン定義情報抽出部の例に相当する。

[0018] シグニチャ検知対象外データパターン抽出部１０５は、シグニチャ入力部１０４によって取り出されたパターン定義情報を入力し、パターン定義情報では検知されない全てのデータにマッチするパターン（シグニチャ検知対象外データパターン）を抽出する。

つまり、シグニチャ検知対象外データパターン抽出部１０５は、シグニチャ情報１０２から抽出されたパターン定義情報を解析し、パターン定義情報では検知されないデータのパターンをシグニチャ検知対象外データパターンとして抽出する。

[0019] 攻撃データパターン抽出部１０７は、修正前プログラム１１０及び修正後プログラム１０６を入力し、脆弱性に対処するためにプログラムに施された修正内容から、脆弱性を攻撃可能な攻撃データのパターン（攻撃データパターン）を生成する。

つまり、攻撃データパターン抽出部１０７は、シグニチャ情報１０２が適用される対象プログラム（修正前プログラム１１０及び修正後プログラム１０６）に対する解析を行い、対象プログラムを攻撃する攻撃データのパターンを攻撃データパターンとして抽出する。

[0020] パターン比較部１０８は、シグニチャ検知対象外データパターン抽出部１０５によって抽出されたシグニチャ検知対象外データパターンと、攻撃データパターン抽出部１０７によって抽出された攻撃データパターンを比較する。

そして、パターン比較部１０８は、シグニチャ情報１０２で定義されている検知パターンでは検知できない攻撃データのパターンを抽出する。

つまり、パターン比較部１０８は、シグニチャ検知対象外データパターンに該当する攻撃データパターンを、シグニチャ情報１０２では検知されない攻撃データパターンとして抽出する。

[0021] 比較結果出力部１０９は、パターン比較部１０８により抽出された攻撃データのパターンが空かどうか判定し、結果をシグニチャ検証結果１１１として出力する。

[0022] 次に、シグニチャ検証装置１０３の各要素の動作について説明する。

[0023] はじめに、シグニチャ入力部１０４の動作について説明する。

前述の通り、シグニチャ入力部１０４は、入力されたシグニチャ情報１０２から検知対象とするデータのパターン定義情報を取り出す。

パターン定義情報は、一般に正規表現で表される。

シグニチャ情報１０２に含まれる情報の種類や書式はＩＤＳ装置によって変わるが、どのようなＩＤＳのシグニチャ情報であっても検知対象とするデータのパターン定義情報は含まれている。

そのため、分析対象とするシグニチャ情報の書式にあわせて、シグニチャ入力部１０４を構成することは容易であり、ここではシグニチャ入力部１０４の構成を詳しく説明しない。

[0024] 次に、シグニチャ検知対象外データパターン抽出部１０５の動作について

説明する。

前述の通り、シグニチャ検知対象外データパターン抽出部１０５はシグニチャ入力部１０４によって取り出されたパターン定義情報を入力し、パターン定義情報に定義されているパターンでは検知されない全てのデータにマッチするパターン（シグニチャ検知対象外データパターン）を生成する。

[0025] 図２は、シグニチャ検知対象外データパターン抽出部１０５の動作例を示すフローチャートである。

シグニチャ検知対象外データパターン抽出部１０５は、入力としてシグニチャ情報１０２のパターン定義情報を表す正規表現を受け取り、受け取った正規表現を変数Ｓに格納する（Ｓ２０１）。

次にＳ２０２において、シグニチャ検知対象外データパターン抽出部１０５は、Ｓの両端に任意の文字列を受理する正規表現である”．＊”を付加した新たな正規表現Ｓ’を生成する。

その後、Ｓ２０３において、シグニチャ検知対象外データパターン抽出部１０５は、正規表現Ｓ’から、同正規表現にマッチするデータのみを受理可能な有限状態オートマトン（以後オートマトンと略す）を生成し、生成したオートマトンを変数Ａに格納する。

与えられた正規表現にマッチするデータのみを受理可能な有限状態オートマトンの構成方法は広く知られており、例えば参考文献１などに詳しい。

参考文献１：中田育男　コンパイラの構成と最適化　ＩＳＢＮ９７８－４－２５４－１２１３９－１

その後、Ｓ２０４において、シグニチャ検知対象外データパターン抽出部１０５は、変数Ａに格納されたオートマトンの受理状態と、非受理状態を入れ替えることで新たなオートマトンを生成（Ａ’）し、新たなオートマトンを出力してシグニチャ検知対象外データパターン抽出部１０５の処理は終了する。

[0026] 入力されたシグニチャ情報１０２のパターン定義情報に対しどのように処理が行われるかの具体例を図３に示す。

図３においては、符号３０１に示される正規表現（ここでは”ａｂｃ”という文字列にのみマッチする）が入力として与えられたものとする。

先に説明したＳ２０２によって生成された符号３０１の正規表現から、符号３０２の正規表現が生成され、その後Ｓ２０３によってオートマトン３０３が生成される。

[0027] オートマトン３０３の表記について概略を説明する。

符号３０６～３０９の円がオートマトンの各「状態」を表しており、円中の番号が各状態の識別子となっている。

状態間を結ぶ矢印は状態遷移を表している。

例えば符号３１１が示す矢印は、状態２（３０７）の時点で入力文字”ｂ”を受け取った場合、状態３（３０８）へと遷移することを示している。

状態遷移は符号３１０のように、遷移元と遷移先が同じこともある。

状態４（３０９）は、状態の中でも受理状態と呼ばれ、オートマトンがこの状態にいるときに入力が終了すると、入力された文字列はオートマトンに受理されたとみなす。

それ以外の状態は非受理状態であり、これらの状態で入力が終了すると、入力はオートマトンに受理されなかったものとみなされる。

最後に黒丸３０５は、状態１がオートマトンの初期状態であることを示している。

[0028] シグニチャ検知対象外データパターン抽出部１０５は、オートマトン３０３を生成した後、最後にＳ２０４にてオートマトンの受理状態と、非受理状態を入れ替えた新たなオートマトン３０４を生成し、処理結果として出力する。

[0029] 次に、攻撃データパターン抽出部１０７の動作について説明する。

前述の通り、攻撃データパターン抽出部１０７は、修正前プログラム１１０及び修正後プログラム１０６を入力とし、脆弱性に対処するためにプログラムに施された修正内容から、脆弱性を攻撃可能な攻撃データのパターンを生成する。

[0030] 図４は、攻撃データパターン抽出部１０７の動作例を示すフローチャートである。

Ｓ４０１に示すとおり、攻撃データパターン抽出部１０７は、修正前プログラム１１０及び修正後プログラム１０６を入力として呼び出され、それぞれを変数Ｐ、Ｐ’に格納する。

次にＳ４０２において、攻撃データパターン抽出部１０７は、脆弱性を攻撃するデータに関する制約条件を算出し、算出した制約条件を変数Ｃへ代入する。

制約条件の算出は、例えば非特許文献１で示しているように、Ｐ、Ｐ’を比較し、脆弱性への対策として追加された入力データ検査処理を抽出し、データの入力から同検査処理に到達するまでに行われる（既存の）入力データ検査の検査条件と、新たに追加された入力データ検査の検査条件を組み合わせることで算出することが可能である。

Ｓ４０２で生成される制約条件は、例えば以下のようなものになる。

（入力文字列長＜１００）∨（１００≦入力文字列長∧入力文字列内に“ｍｏｄｅ＝ＬＯＮＧ”を含む）

[0031] 次に、Ｓ４０３において、攻撃データパターン抽出部１０７は、生成された制約条件を加法標準形に変形し、変形後の制約条件を変数Ｃ’に格納する。

加法標準形とは論理式を連言節の選言として表現したものであり、任意の論理式をこの形式に変形することが可能である。

[0032] 次に、Ｓ４０４からＳ４１６で、攻撃データパターン抽出部１０７は、Ｃ’から同条件（加法標準形に変形した制約条件）を満たす文字列の「文法」を生成する。

文法は文脈自由文法として表される。

文脈自由文法とは、全ての生成規則の左辺が１個の非終端記号のみで構成されている文法である。

まず、攻撃データパターン抽出部１０７は、Ｓ４０４で生成規則を一つも

含まない空の文法を生成し、Ｓ４０５で開始記号Ｓを与えることで、最終的な出力となる文法Ｇを初期化する。

次に、攻撃データパターン抽出部１０７は、Ｓ４０７からＳ４１５のループにおいて、制約条件Ｃ’中の各連言節に対応する制約条件を満たした（部分的な）文法を生成する。

まず、攻撃データパターン抽出部１０７は、Ｓ４０８において、変数Ｘを任意の文字列を受理する文法で初期化する。

このような条件を満たす文法としては、例えば以下のような文法を与えることが可能である（εは空を表す記号）。

Ｘ：：＝ε

Ｘ：：＝任意の１文字　Ｘ

[0033] 次に、Ｓ４１０～Ｓ４１３に示すループにおいて、攻撃データパターン抽出部１０７は、ｎ番目の連言節に含まれる全ての制約条件を満たす文法規則を生成する。

まず、Ｓ４１１において、攻撃データパターン抽出部１０７は、Ｃ’のｎ番目の連言節に含まれる各リテラル（原子論理式及びその否定）を取り出し、取り出された条件を対応するオートマトンに変換し、オートマトンを変数Ｒへ代入する。

変換は図５のような変換テーブルを用いて行う。

変換テーブルは、変換対象とする条件に対し、対応するオートマトンを生成するための方法を定義したテーブルである。

変換テーブルは変換対象とする条件を記述したカラム５０２と対応するオートマトンの生成方法を定義したカラム５０３で構成されている。

Ｓ４１１において、例えば“入力文字列長＜１００”というリテラルに対しては、条件カラム５０２が検索され、レコード５０４がマッチする。

その結果、符号５０６に示されるようなオートマトンが生成される。

ただし、条件５０４の文言中Ｎと表記されている部分は、この例の場合１００になる。

リテラルがある原子論理式の否定であった場合には、条件５０５にマッチするため、同原子論理式に対応するオートマトンが生成され、その後同オートマトンの受理・非受理状態の反転が行われる。

次に、Ｓ４１２において文法Ｘとオートマトンを引数として手続き「ＩＮＴＥＲＳＥＣＴ」が呼び出される。

「ＩＮＴＥＲＳＥＣＴ」は、文法Ｘとオートマトンがともに受理する文字列が満たす文法を生成する処理であり、そのアルゴリズムとしては、例えば参考文献２に示されるような方法を適用可能である。

参考文献２：Ｄ．Ｍｅｌｓｋｉ ａｎｄ Ｔ．Ｒｅｐｓ．Ｉｎｔｅｒｃｏｎｖｅｒｔｉｂｉｌｉｔｙ ｏｆ Ｓｅｔ Ｃｏｎｓｔｒａｉｎｔｓ ａｎｄ Ｃｏｎｔｅｘｔ－Ｆｒｅｅ Ｌａｎｇｕａｇｅ Ｒｅａｃｈａｂｉｌｉｔｙ．Ｉｎ Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ｔｈｅ １９９７ ＡＣＭ ＳＩＧＰＬＡＮ Ｓｙｍｐｏｓｉｕｍ ｏｎ Ｐａｒｔｉａｌ Ｅｖａｌｕａｔｉｏｎ ａｎｄ Ｓｅｍａｎｔｉｃｓ－ｂａｓｅｄ Ｐｒｏｇｒａｍ Ｍａｎｉｐｕｌａｔｉｏｎ、ｐａｇｅｓ ７４－８９

[0034] Ｓ４１０にてループを終了した時点で、文法Ｘには、Ｃ’中のｎ番目の連言節内の全てのリテラルとのＩＮＴＥＲＳＥＣＴをとった文法が格納されている。

攻撃データパターン抽出部１０７は、Ｓ４１４にてこの文法を文法Ｇに登録する。

登録はまず、攻撃データパターン抽出部１０７が、文法Ｘ内の全ての非終端記号を、文法Ｇ内で使用済みの非終端記号と異なる名前に変更し、全ての生成規則を文法Ｇに追加する。

その後、攻撃データパターン抽出部１０７は、文法Ｇの開始記号Ｓの生成規則としてＳ：：＝Ｘの開始記号を追加する。

その後、外側のループＳ４０７に戻り、攻撃データパターン抽出部１０７は、次の連言節に対して同様の処理を行う。

以上の処理を行うことで、最終的に文法Ｇには、制約Ｃで示された制約条

件を満たし得る全ての文字列を表す文法が格納されるため、攻撃データパターン抽出部１０７は、Ｓ４１６にて同文法を処理結果として出力する。

[0035] 次に、パターン比較部１０８の動作例について説明する。

前述の通り、パターン比較部１０８は、シグニチャ検知対象外データパターン抽出部１０５によって算出された検知対象外データのパターンと、攻撃データパターン抽出部１０７によって算出された攻撃データパターンを比較する。

そして、パターン比較部１０８は、シグニチャ情報１０２で定義されている検知パターンでは検知できない攻撃データのパターンを算出する。

[0036] 図６はパターン比較部１０８の動作例を示すフローチャートである。

パターン比較部１０８は攻撃データパターンと、シグニチャ検知対象外データパターンを入力として呼び出され、攻撃データパターンと、シグニチャ検知対象外データパターンをそれぞれ変数Ｇ及びＳに格納する（Ｓ６０１）。

次に、Ｓ６０２において、ＧとＳを引数として「ＩＮＴＥＲＳＥＣＴ」手続きが呼び出される。

その結果、文法Ｇと正規表現Ｓの両方を満たす文字列の文法、つまり攻撃データであり、かつシグニチャでは検知されないデータが満たす文法が算出される。

算出された文法は変数Ｘに代入され、パターン比較部１０８の処理結果として返される（Ｓ６０３）。

[0037] 最後に、比較結果出力部１０９の動作例について説明する。

前述の通り、比較結果出力部１０９は、パターン比較部１０８により算出された攻撃データのパターンが空かどうか判定し、結果をシグニチャ検証結果１１１として出力する。

[0038] 図７は、比較結果出力部１０９の動作例を示すフローチャートである。

比較結果出力部１０９は、パターン比較部１０８の処理結果として出力されたパターン比較結果を示す文法を入力として呼び出され、パターン比較結

果を示す文法を変数Ｇに格納する（Ｓ７０１）。

次にＳ７０２において、入力された文法Ｇ内に格納されている生成規則の有無について検査が行われる。

もし、文法Ｇ内に生成規則が一つも存在していなければ、全ての攻撃データがシグニチャによって検知されることを表しており、比較結果出力部１０９は、Ｓ７０３にてシグニチャに漏れが無い旨をシグニチャ検証結果１１１として出力し、処理を終了する。

一方、文法Ｇ内に生成規則が一つでも存在していたならば、その文法に従ったデータを生成することでシグニチャに検知されること無く攻撃が可能である。

このため、比較結果出力部１０９は、Ｓ７０４にてシグニチャに漏れがあることを示すシグニチャ検証結果１１１を出力し処理を終了する。

[0039] 以上に示したように、シグニチャ検証結果１１１には最低限、シグニチャに漏れがあるかどうかを示す情報が出力されるが、その他の補足情報を出力することももちろん可能である。

例えばシグニチャに漏れがあると判断した場合に、文法Ｇの内容をあわせて出力し、ユーザが実際にその文法に従ったデータを生成し、ＩＤＳの試験を行えるようにすることも考えられる。

[0040] 以上のように、シグニチャ情報と攻撃データのパターン情報から、シグニチャが検知対象とする脆弱性攻撃に対し漏れなく検知が行えるかを、実際にＩＤＳを動作させることなく、短時間で検証できるという効果がある。

[0041] さらに、脆弱性修正前後のプログラムの差分から生成される攻撃データに対する制約条件を加法標準形に変換し、各連言節から、攻撃データが満たすべき文法を生成することで、シグニチャ検証に必要となる攻撃データのパターンを自動生成できるという効果がある。

[0042] さらに、シグニチャのパターン情報から、シグニチャでは検知できないデータのパターンを算出し、同パターンと脆弱性を攻撃するデータのパターンとを比較することで、シグニチャと攻撃データパターンとの比較を自動で行

うことができるという効果がある。

[0043] さらに、パターン同士の比較において、「ＩＮＴＥＲＳＥＣＴ」手続きを使用することで、シグニチャに漏れがある場合に、どのような攻撃データが実際に検知から漏れてしまうのかをユーザに提示することができるという効果がある。

[0044] さらに、検証結果を比較結果出力部によって表示することで、シグニチャの検証結果を利用者が容易に確認できるという効果がある。

[0045] さらに、シグニチャ情報をＩＤＳ開発元のウェブサイトから直接ダウンロードすることで、検証装置とＩＤＳとが直接接続されていなくても検証可能になるという効果がある。

[0046] さらに、定期的にプログラムをインターネットからダウンロードしておくことで、修正前プログラム１１０、修正後プログラム１０６をユーザの作業無しに利用可能になるという効果がある。

[0047] 本実施の形態では、

以下の要素で構成され、シグニチャ情報に対し、シグニチャ検証結果を出力するシグニチャ検証装置を説明した。

シグニチャ情報を装置内部に取り込み、検知対象とするデータのパターン定義情報を取り出すシグニチャ入力部、

シグニチャでは検知されない全てのデータにマッチするパターンを生成するシグニチャ検知対象外データパターン抽出部、

脆弱性を攻撃可能な攻撃データのパターンを生成する攻撃データパターン抽出部、

シグニチャ検知対象外データパターンと攻撃データパターンを比較することで、シグニチャでは検知できない攻撃データのパターンを算出するパターン比較部、

パターン比較部により算出された攻撃データのパターンを出力する比較結果出力部。

[0048] また、本実施の形態では、

攻撃データパターン抽出部が、脆弱性修正前のプログラムと脆弱性修正後のプログラムとの差分から生成される攻撃データに対する制約条件を加法標準形に変換し、各連言節から、攻撃データが満たすべき文法を生成することを説明した。

[0049] また、本実施の形態では、

シグニチャ検知対象外データパターン抽出部が、シグニチャのパターン情報から、オートマトンを生成し、オートマトンの受理・非受理状態を反転させることでシグニチャでは検知できないデータのパターンを算出することを説明した。

[0050] また、本実施の形態では、

パターン比較部において、シグニチャ検知対象外データパターンと脆弱性を攻撃するデータのパターンとの交差（ＩＮＴＥＲＳＥＣＴ）をとることで、シグニチャと攻撃データパターンとの比較を行うことを説明した。

[0051] また、本実施の形態では、

比較結果出力部が、シグニチャに漏れがある場合に、どのような攻撃データが実際に検知から漏れてしまうのかをユーザに提示することを説明した。

[0052] また、本実施の形態では、

シグニチャ入力部が、シグニチャ情報をＩＤＳ開発元のウェブサイトから直接ダウンロードすることを説明した。

[0053] また、本実施の形態では、

攻撃データパターン抽出部が、定期的にプログラムをインターネットからダウンロードしておくことを説明した。

[0054] 実施の形態２．

以上の実施の形態１では、パターン比較部１０８の結果を比較結果出力部１０９がそのまま出力するものであったが、攻撃データパターン抽出部１０７が本来攻撃とはならないデータも包含したパターンを抽出する場合を考慮した実施の形態を示す。

[0055] 本実施の形態の構成例を図８に示す。

本実施の形態に係るシグニチャ検証装置８０３は、実施の形態１と同様に、ＩＤＳ装置８０１から取得されたシグニチャ情報８０２、シグニチャ情報８０２が検知対象とした攻撃が標的としている脆弱性に対し、修正を施す前後のプログラム（修正前プログラム８１１及び修正後プログラム８０６）とを入力とし、シグニチャ検証結果８１２を出力する。

シグニチャ検証装置８０３は、実施の形態１とは異なり、その構成要素に比較結果検証部８０９が追加されている。

その他の要素（シグニチャ入力部８０４、シグニチャ検知対象外データパターン抽出部８０５、攻撃データパターン抽出部８０７、パターン比較部８０８及び比較結果出力部８１０）については、実施の形態１と同様である。

比較結果検証部８０９は、パターン比較部８０８によって算出された、シグニチャ情報８０２で検知されない攻撃データの文法情報を元に、実際に攻撃データ（パターン対応データ）を生成し、生成した攻撃データを修正前プログラム８１１に入力する。

そして、比較結果検証部８０９は、パターン比較結果によって生成された文法情報が本当に攻撃となるデータのパターンを示しているかを検証する。

[0056] 図９は、比較結果検証部８０９の動作例を示すフローチャートである。

[0057] 比較結果検証部８０９は、パターン比較部８０８が算出した文法と、修正前プログラム８１１を入力として呼び出される（Ｓ９０１）。

以下ではそれぞれを文法Ｇ、修正前プログラムＰとして説明する。

比較結果検証部８０９は、Ｓ９０２では文法Ｇの開始記号を変数Ｓに代入し、次にＳ９０３で手続き「文字列生成」を文法Ｇ、変数Ｓを引数として呼び出す。

具体的な処理手順については後述するが、手続き「文字列生成」は文法Ｇにおいて、非終端記号Ｓとして受理可能な全ての文字列を生成する。

手続き「文字列生成」の実行結果は文字列のリストとして変数ＩＮに格納される。

次に、Ｓ９０５からＳ９０９で示されるループで、比較結果検証部８０９

は、ＩＮに格納された各文字列を実際にプログラムＰへ入力し、攻撃データとなる文字列が含まれているかどうかを判別する。

文字列が攻撃データかどうかの判別はＳ９０８で行う。

Ｓ９０８では、比較結果検証部８０９は、データを入力後のプログラムＰの挙動を監視し、メモリアクセス違反等により、プログラムがクラッシュ（異常終了）するかどうかを検査する。

クラッシュしたかどうかの判定は、対象プログラムにデバッガを接続した上で、デバッガが対象プログラムを実行することで容易に行うことができる。

もし修正前プログラムＰがクラッシュした場合、比較結果検証部８０９は、入力したデータは攻撃データであったとみなし、判定結果として変数ｒｅｓｕｌｔにＴＲＵＥを格納してループを終了する。

ＩＮに格納された全ての文字列においてＰがクラッシュしなければ、比較結果検証部８０９は、変数ｒｅｓｕｌｔにＦＡＬＳＥを格納してループを終了する。

最後に、比較結果検証部８０９は、変数ｒｅｓｕｌｔの内容を、比較結果検証部８０９の処理結果として出力する。

比較結果検証部８０９の処理結果がＴＲＵＥだった場合、文法Ｇを入力として比較結果出力部８１０が呼び出される。

ＦＡＬＳＥだった場合、文法Ｇに格納されている全ての生成規則が削除されてから比較結果出力部８１０が呼び出される。

[0058] 次に、手続き「文字列生成」の動作について説明する。

図１０は、手続き「文字列生成」の動作を示すフローチャートである。

手続き「文字列生成」では、文法Ｇ及び文字列生成の対象となる非終端記号Ｓが引数として呼び出される（Ｓ１００１）。

まずＳ１００２において、ワークリストWが生成され、ワークリストWに、文法Ｇ内で定義された非終端記号Ｓに関する全ての生成規則の右辺にある記号列が格納される。

例えば、文法Ｇ内にＳ：：＝ＸＹ、Ｓ：：＝ＢＣという二つの生成規則が存在した場合には、（Ｘ、Ｙ）、（Ｂ、Ｃ）という二つの右辺値がワークリストＷに格納される。

次に生成された文字列を格納するリストＬが作成される（Ｓ１００３）。

その後、ワークリストＷが空になるまでＳ１００４～Ｓ１００９までのループが実行される。

まずＳ１００５ではワークリストＷの先頭の要素を取り出され、取り出された先頭の要素が変数Ｒに格納される。

その際、ワークリストＷの先頭要素が取り除かれる。

次に変数Ｒの先頭から非終端記号が検索され、最初に見つかった非終端記号Ｎを境界として、変数Ｒが終端記号列ＴＳ、Ｎ、残りの記号列ＲＳに分割される（Ｓ１００６）。

Ｓ１００７で、Ｓ１００６での非終端記号の検索結果が評価され、もし非終端記号Ｎが見つかっていなかった場合には、変数Ｒ内の記号列は全て終端記号であるため、各記号が表す文字が連結されて文字列が作成され、作成された文字列がリストＬに追加される。

もし、Ｓ１００６において非終端記号Ｎが見つかった場合には、文法Ｇから非終端記号Ｎに関する全ての生成規則が取り出され、各生成規則の右辺の記号列（仮にＮＳとする）を使用して、ＴＳ　ＮＳ　ＲＳ　となる記号列が生成され、生成された記号列がワークリストＷに追加される（Ｓ１００９）。

Ｓ１００８もしくはＳ１００９実施後、再びループの先頭Ｓ１００４に戻る。

最終的に、ワークリストＷが空になったら、リストＬが手続き「文字列生成」の処理結果として出力される（Ｓ１０１０）。

[0059] 本実施の形態では、文字列生成手続きでは与えられた非終端記号を満たす全ての文字列が出力されるが、生成される文字列の上限数を制限することも可能であるし、生成される文字列の上限数をユーザが指定できるようにする

ことも容易である。

また、本実施の形態では、Ｓ９０８で表されるようにプログラムのクラッシュを攻撃の成否判定条件として用いているが、本実施の形態で示した以外にもクラッシュの検出方法としては以下が考えられ、いずれを用いることも可能である。

・対象プログラム実行後に、ＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）上でのアプリケーション実行エラー記録を確認する

・ユーザが対象プログラムの動作画面等を確認し、クラッシュしたかどうかをシグニチャ検証装置に入力する

[0060] 以上のように、本実施の形態では、パターン比較部により出力された文法情報をもとに攻撃データを生成し、実際に攻撃データを修正前プログラムへ入力して修正前プログラムの動作を監視し、攻撃データパターン抽出部の生成した攻撃データのパターンのうち、無害なパターンを除外する。

これにより、本実施の形態では、シグニチャによって無害なパターンが検出されない旨を警告する検証結果が出力されることを防止できるという効果がある。

[0061] さらに、文字列生成手続きにおいて上限数を制限することで、検証を無限に実施することを防ぐことができるという効果がある。

[0062] さらに、文字列生成の上限数をユーザが指定可能とすることで、ユーザの判断に基づき、処理時間を調整することが可能となるという効果がある。

[0063] さらに、ＯＳ上のアプリケーション実行エラー記録を確認するというクラッシュ判定を行うことで、デバッガ接続によって動作が変わってしまうプログラムに対しても検証できるという効果がある。

[0064] さらに、ユーザが動作画面等を確認し、確認結果をシグニチャ検証装置に入力するというクラッシュ判定を行うことで、ＯＳ上にデバッグ機能やアプリケーション実行エラー記録機能が無い場合にも本検証装置を実現することができるという効果がある。

[0065] 本実施の形態では、

実施の形態１に示したシグニチャ検証装置に、さらに比較結果検証部を設けることを説明した。

[0066] また、本実施の形態では、

生成する攻撃データ数の上限をユーザが指定できることを説明した。

[0067] また、本実施の形態では、

比較結果検証部が、ＯＳ上のアプリケーション実行エラー記録を確認することでプログラムのクラッシュを判定することを説明した。

[0068] また、本実施の形態では、

比較結果検証部が、ユーザが対象プログラムの動作画面等を確認してクラッシュしたかどうかを判定した結果を入力するためのインタフェースを備えていることを説明した。

[0069] 最後に、実施の形態１及び２に示したシグニチャ検証装置１０３、シグニチャ検証装置８０３のハードウェア構成例を図１１を参照して説明する。

シグニチャ検証装置１０３、シグニチャ検証装置８０３はコンピュータであり、シグニチャ検証装置１０３、シグニチャ検証装置８０３の各要素をプログラムで実現することができる。

シグニチャ検証装置１０３、シグニチャ検証装置８０３のハードウェア構成としては、バスに、演算装置９０１、外部記憶装置９０２、主記憶装置９０３、通信装置９０４、入出力装置９０５が接続されている。

[0070] 演算装置９０１は、プログラムを実行するＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）である。

外部記憶装置９０２は、例えばＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）やフラッシュメモリ、ハードディスク装置である。

主記憶装置９０３は、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）である。

通信装置９０４は、例えば、シグニチャ入力部１０４がＩＤＳ装置１０１からシグニチャ情報１０２を受信する際（シグニチャ入力部８０４がＩＤＳ装置８０１からシグニチャ情報８０２を受信する際）に用いられる。

入出力装置９０５は、例えばマウス、キーボード、ディスプレイ装置等であり、修正前プログラム１１０及び修正後プログラム１０６の入力、修正前プログラム８１１及び修正後プログラム８０６の入力、シグニチャ検証結果１１１の出力、シグニチャ検証結果８１２の出力に用いられる。

[0071] プログラムは、通常は外部記憶装置９０２に記憶されており、主記憶装置９０３にロードされた状態で、順次演算装置９０１に読み込まれ、実行される。

プログラムは、図１及び図８に示す「～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。

更に、外部記憶装置９０２にはＯＳも記憶されており、ＯＳの少なくとも一部が主記憶装置９０３にロードされ、演算装置９０１はＯＳを実行しながら、図１及び図８に示す「～部」の機能を実現するプログラムを実行する。

また、実施の形態１及び２の説明において、「～の判断」、「～の判定」、「～の抽出」、「～の検知」、「～の算出」、「～の比較」、「～の検証」、「～の設定」、「～の登録」、「～の選択」、「～の生成」、「～の入力」、「～の出力」等として説明している処理の結果を示す情報やデータや信号値や変数値が主記憶装置９０３にファイルとして記憶されている。

また、シグニチャ情報１０２、シグニチャ情報８０２、修正前プログラム１１０、修正前プログラム８１１、修正後プログラム１０６、修正後プログラム８０６が主記憶装置９０３に記憶される。

また、暗号鍵・復号鍵や乱数値やパラメータが、主記憶装置９０３にファイルとして記憶されてもよい。

[0072] なお、図１１の構成は、あくまでもシグニチャ検証装置１０３、シグニチャ検証装置８０３のハードウェア構成の一例を示すものであり、シグニチャ検証装置１０３、シグニチャ検証装置８０３のハードウェア構成は図１１に記載の構成に限らず、他の構成であってもよい。

[0073] また、実施の形態１及び２に示す手順により、本発明に係るシグニチャ検証方法を実現可能である。

符号の説明

[0074] １０１　ＩＤＳ装置、１０２　シグニチャ情報、１０３　シグニチャ検証装置、１０４　シグニチャ入力部、１０５　シグニチャ検知対象外データパターン抽出部、１０６　修正後プログラム、１０７　攻撃データパターン抽出部、１０８　パターン比較部、１０９　比較結果出力部、１１０　修正前プログラム、１１１　シグニチャ検証結果、８０１　ＩＤＳ装置、８０２　シグニチャ情報、８０３　シグニチャ検証装置、８０４　シグニチャ入力部、８０５　シグニチャ検知対象外データパターン抽出部、８０６　修正後プログラム、８０７　攻撃データパターン抽出部、８０８　パターン比較部、８０９　比較結果検証部、８１０　比較結果出力部、８１１　修正前プログラム、８１２　シグニチャ検証結果。

請求の範囲

[請求項1] シグニチャ情報に対する解析を行い、前記シグニチャ情報では検知されないデータのパターンを抽出するシグニチャ検知対象外データパターン抽出部と、

前記シグニチャ情報が適用される対象プログラムに対する解析を行い、前記対象プログラムを攻撃する攻撃データのパターンを抽出する攻撃データパターン抽出部と、

前記シグニチャ検知対象外データパターン抽出部により抽出されたシグニチャ検知対象外データパターンと前記攻撃データパターン抽出部により抽出された攻撃データパターンとを比較し、シグニチャ検知対象外データパターンに該当する攻撃データパターンを、前記シグニチャ情報では検知されない攻撃データパターンとして抽出するパターン比較部とを有することを特徴とするシグニチャ検証装置。

[請求項2] 前記攻撃データパターン抽出部は、

脆弱性に対する修正が行われる前の対象プログラムと、脆弱性に対する修正が行われた後の対象プログラムとの差分から、攻撃データの制約条件を生成し、

生成した制約条件を加法標準形に変換し、加法標準形に変換後の制約条件の各連言節から、攻撃データのパターンを抽出することを特徴とする請求項１に記載のシグニチャ検証装置。

[請求項3] 前記シグニチャ検証装置は、更に、

前記シグニチャ情報から、前記シグニチャ情報が検知の対象とするデータのパターンが定義されるパターン定義情報を抽出するパターン定義情報抽出部を有し、

前記シグニチャ検知対象外データパターン抽出部は、

前記パターン定義情報で定義されているパターンを表すオートマトンを生成し、

生成したオートマトンにおける受理状態及び非受理状態を反転させ

て、前記シグニチャ情報では検知されないデータのパターンを抽出することを特徴とする請求項１又は２に記載のシグニチャ検証装置。

［請求項4］ 前記パターン比較部は、

前記シグニチャ検知対象外データパターンと前記攻撃データパターンとの交差（ＩＮＴＥＲＳＥＣＴ）をとることで、前記シグニチャ検知対象外データパターンと前記攻撃データパターンとを比較することを特徴とする請求項１～３のいずれかに記載のシグニチャ検証装置。

［請求項5］ 前記シグニチャ検証装置は、更に、

前記パターン比較部により抽出された攻撃データパターンを、前記シグニチャ検証装置の利用者に提示する比較結果出力部を有することを特徴とする請求項１～４のいずれかに記載のシグニチャ検証装置。

［請求項6］ 前記シグニチャ検証装置は、更に、

前記パターン比較部により抽出された攻撃データパターンによって前記対象プログラムが攻撃されるか否かを検証する比較結果検証部を有し、

前記比較結果出力部は、

前記対象プログラムが攻撃されると前記比較結果検証部により判断された攻撃データパターンを選択して、前記シグニチャ検証装置の利用者に提示することを特徴とする請求項５に記載のシグニチャ検証装置。

［請求項7］ 前記比較結果検証部は、

前記パターン比較部により抽出された攻撃データパターンに対応するデータをパターン対応データとして生成し、生成したパターン対応データを前記対象プログラムに適用し、

前記パターン対応データによって前記対象プログラムが攻撃されるか否かを検証することを特徴とする請求項６に記載のシグニチャ検証装置。

［請求項8］ 前記比較結果検証部は、

前記対象プログラムが異常終了した場合に、前記パターン対応データによって前記対象プログラムが攻撃されたと判断することを特徴とする請求項７に記載のシグニチャ検証装置。

[請求項9] 前記比較結果検証部は、

前記対象プログラムの挙動の監視、前記対象プログラムを動作させるＯＳ（Ｏｐｅｒａｔｉｎｇ　Ｓｙｓｔｅｍ）における記録、前記シグニチャ検証装置の利用者による指定の少なくともいずれかにより、前記対象プログラムの異常終了を検知することを特徴とする請求項８に記載のシグニチャ検証装置。

[請求項10] 前記比較結果検証部は、

前記シグニチャ検証装置の利用者により指定された個数分のパターン対応データを生成し、生成した各パターン対応データを前記対象プログラムに適用することを特徴とする請求項７～９のいずれかに記載のシグニチャ検証装置。

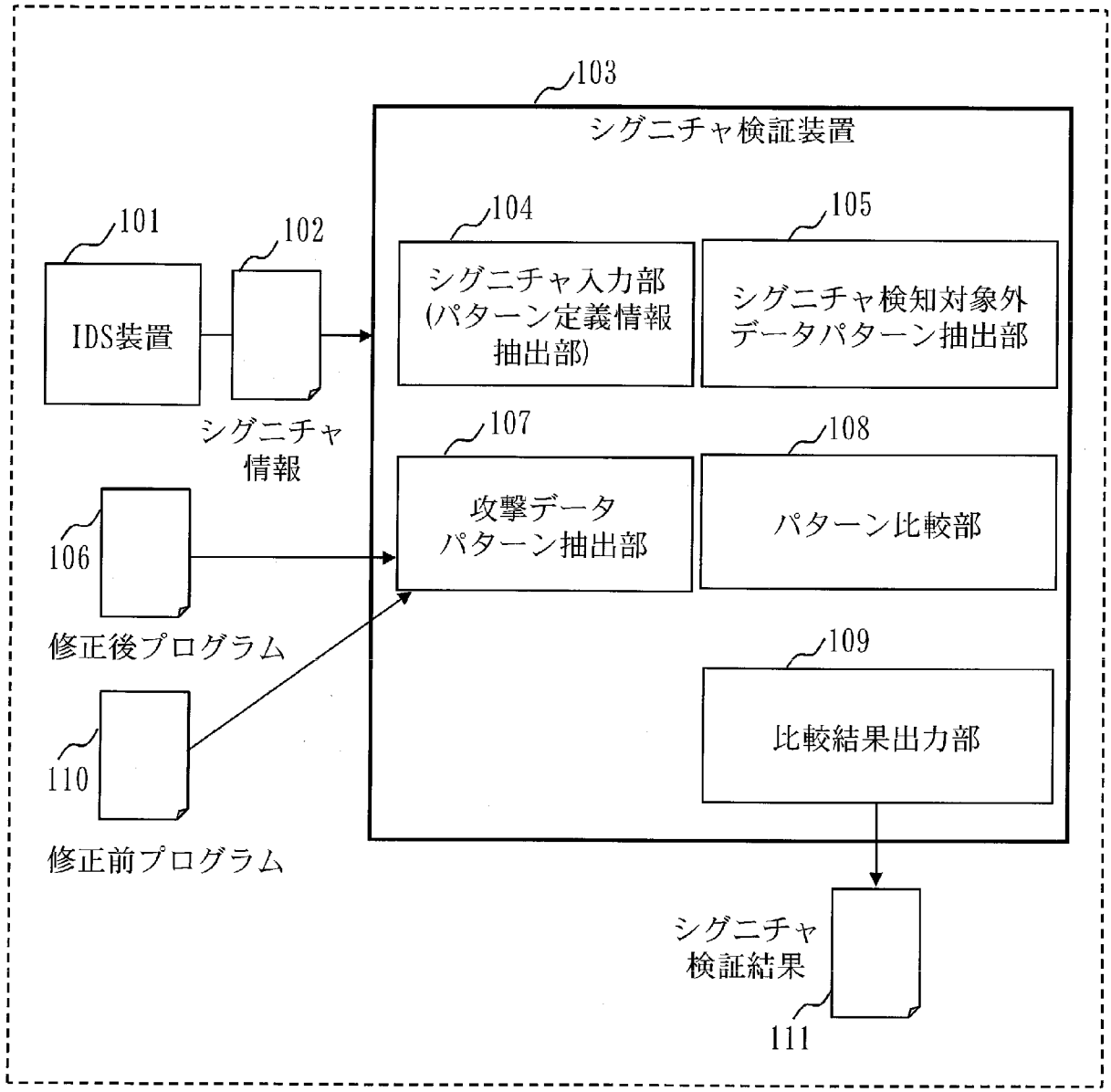
[請求項11] コンピュータが、シグニチャ情報に対する解析を行い、前記シグニチャ情報では検知されないデータのパターンをシグニチャ検知対象外データパターンとして抽出し、

前記コンピュータが、前記シグニチャ情報が適用される対象プログラムに対する解析を行い、前記対象プログラムを攻撃する攻撃データのパターンを攻撃データパターンとして抽出し、

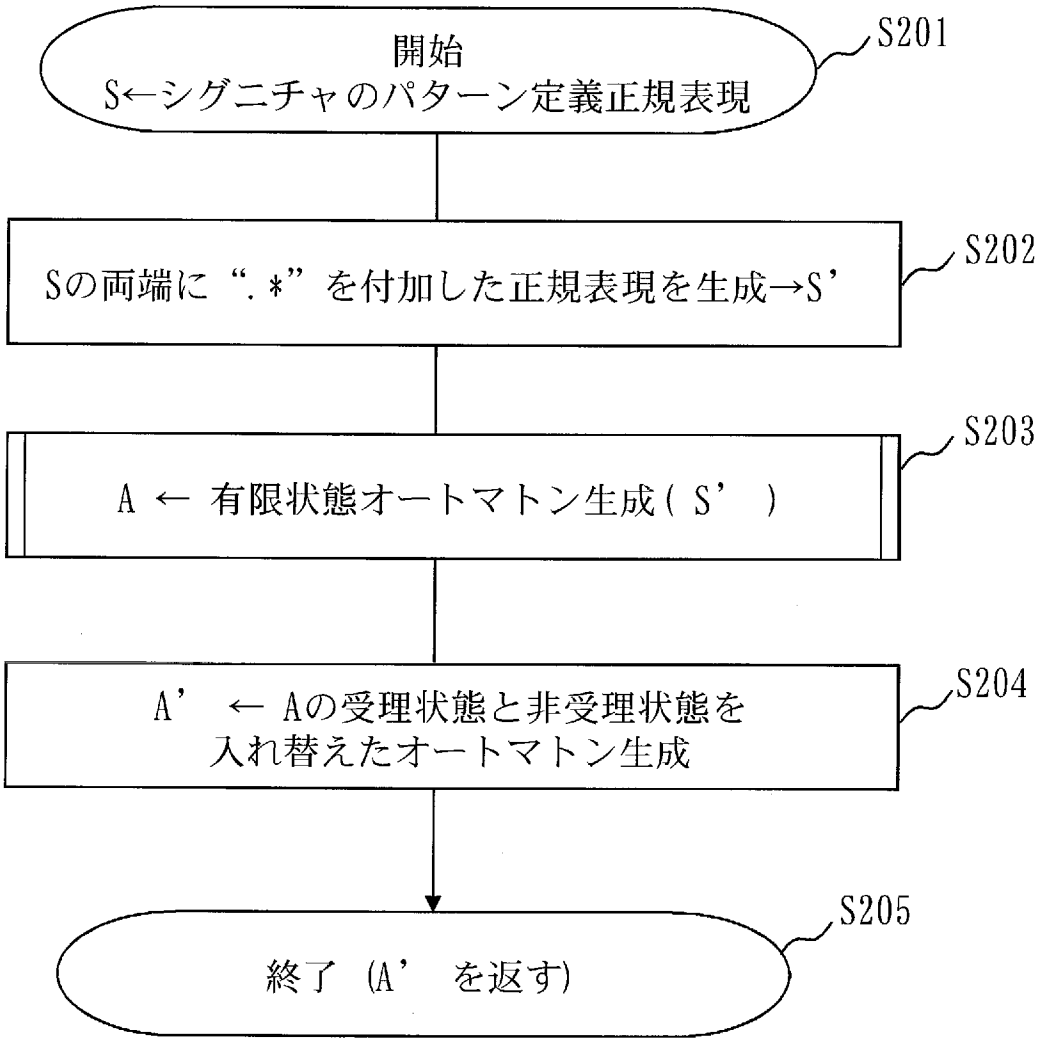
前記コンピュータが、シグニチャ検知対象外データパターンと攻撃データパターンとを比較し、シグニチャ検知対象外データパターンに該当する攻撃データパターンを、前記シグニチャ情報では検知されない攻撃データパターンとして抽出することを特徴とするシグニチャ検証方法。

[請求項12] コンピュータを請求項１に記載されたシグネチャ検証装置として機能させることを特徴とするプログラム。

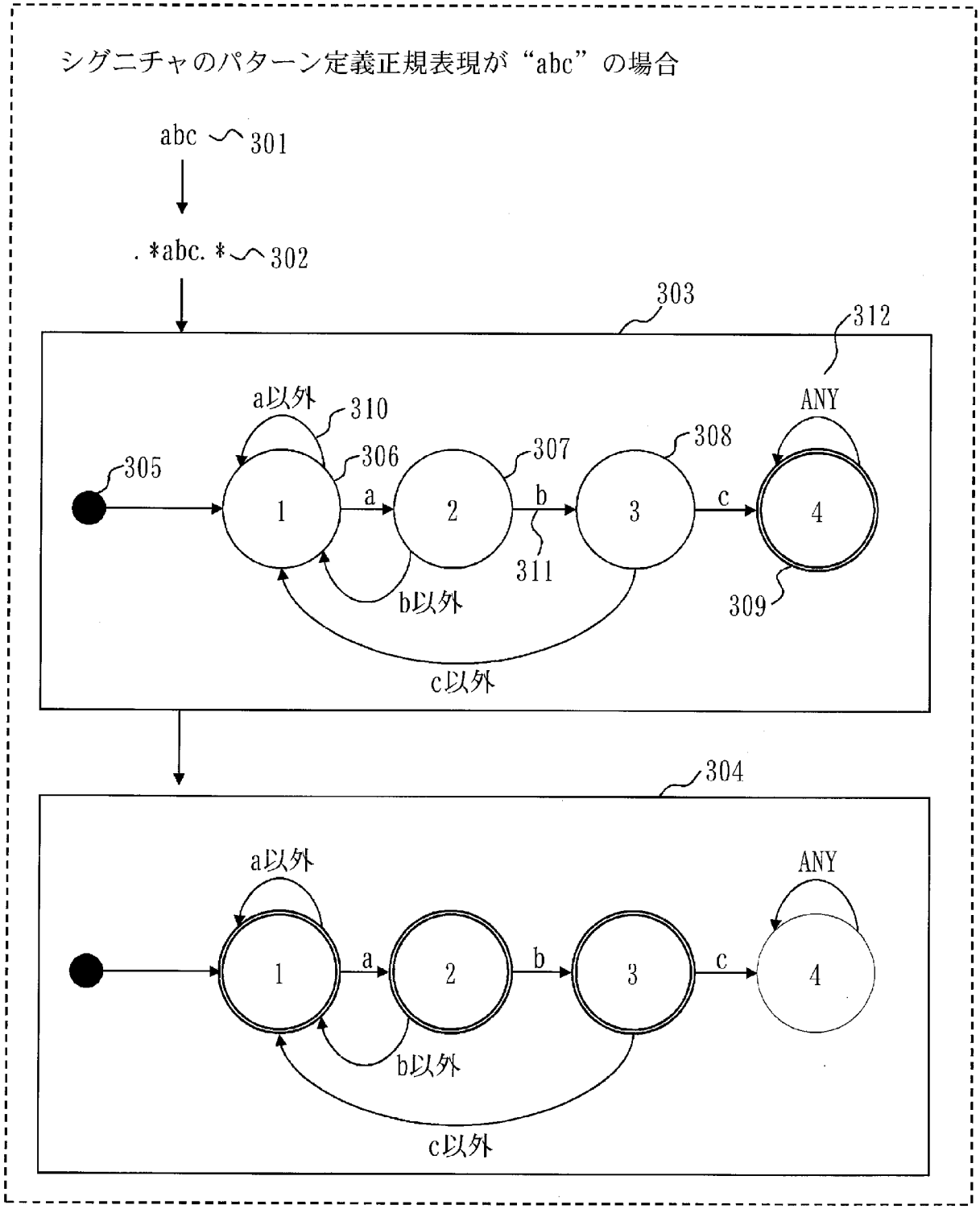
[図1]


103
シグニチャ検証装置
101
IDS装置
102
シグニチャ情報
104
シグニチャ入力部(パターン定義情報抽出部)
105
シグニチャ検知対象外データパターン抽出部
107
攻撃データパターン抽出部
108
パターン比較部
106
修正後プログラム
109
比較結果出力部
110
修正前プログラム
シグニチャ検証結果
111

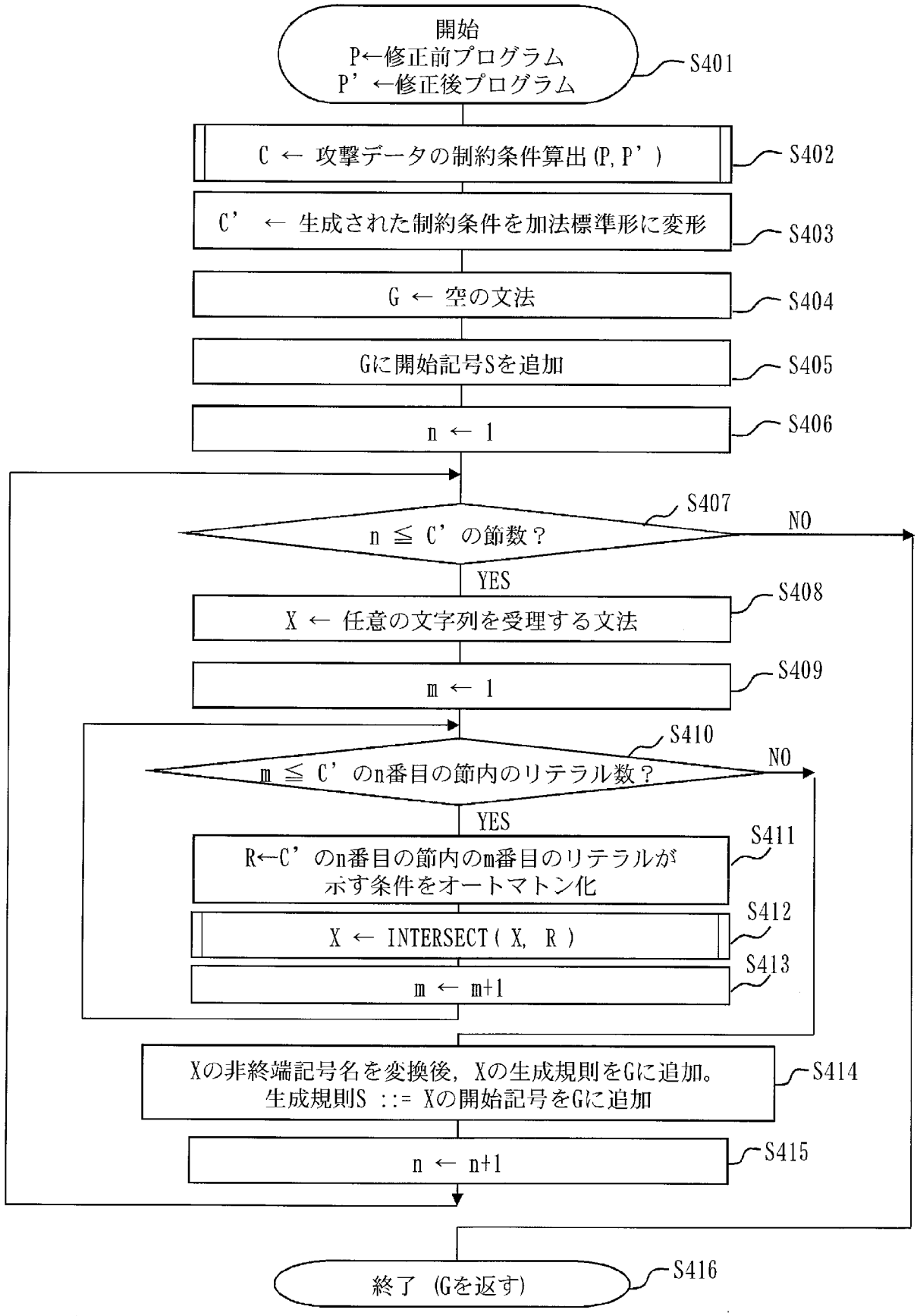
[図2]


開始
S←シグニチャのパターン定義正規表現
S201
Sの両端に“.*”を付加した正規表現を生成→S’
S202
A ← 有限状態オートマトン生成(S’)
S203
A’ ← Aの受理状態と非受理状態を
入れ替えたオートマトン生成
S204
終了 (A’ を返す)
S205

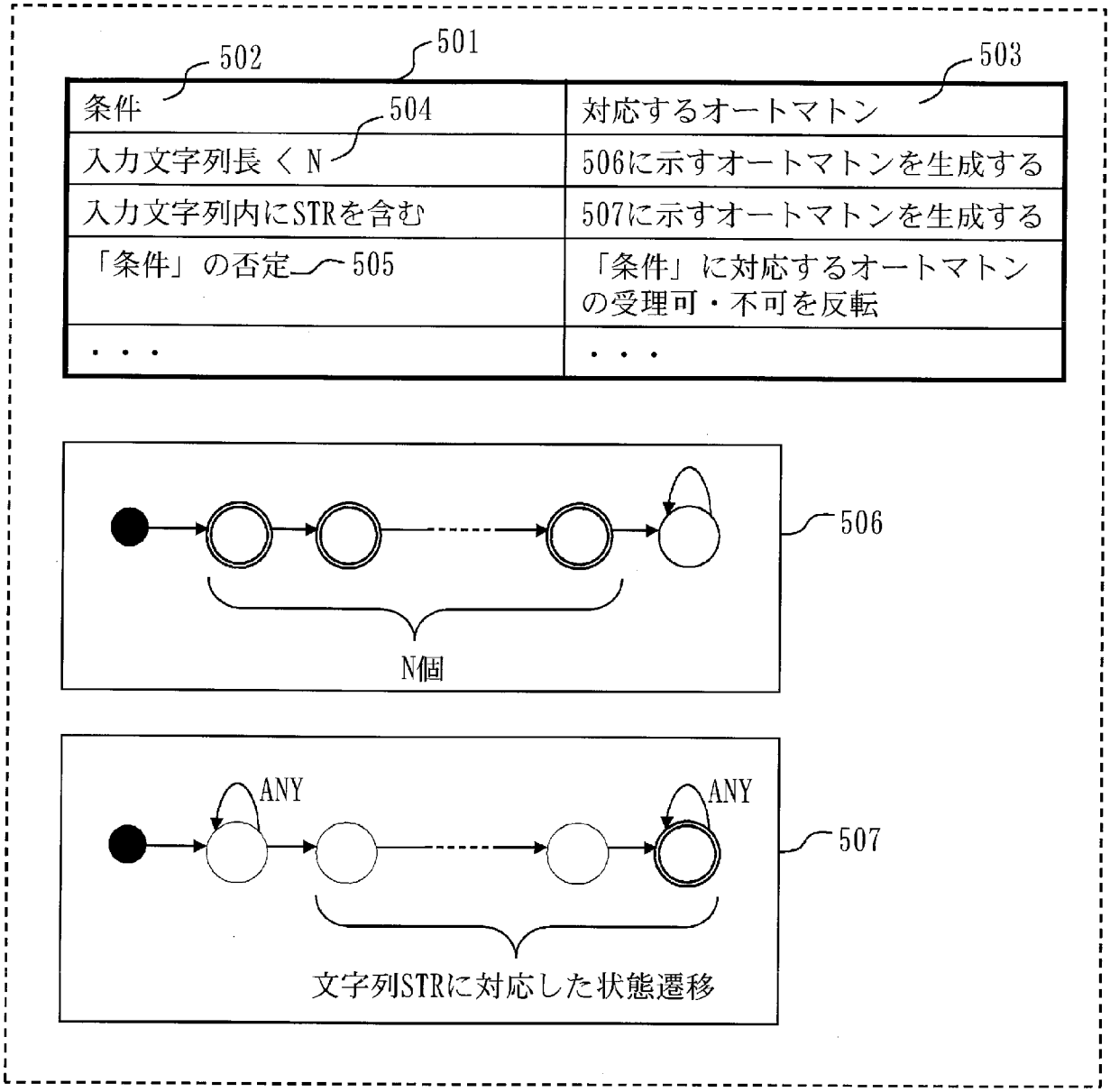
[図3]


シグニチャのパターン定義正規表現が“abc”の場合
abc
301
.*abc.*
302
303
312
a以外
310
306
307
308
ANY
305
1
a
2
b
3
c
4
311
b以外
309
c以外
304
a以外
ANY
1
a
2
b
3
c
4
b以外
c以外

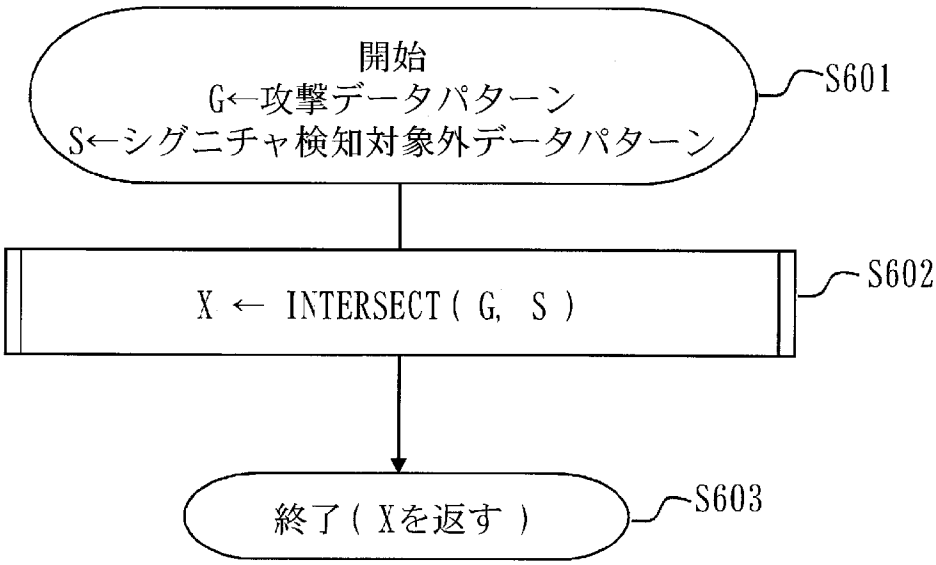
[図4]


開始
P←修正前プログラム
P'←修正後プログラム
S401
C ← 攻撃データの制約条件算出(P, P')
S402
C' ← 生成された制約条件を加法標準形に変形
S403
G ← 空の文法
S404
Gに開始記号Sを追加
S405
n ← 1
S406
n ≦ C'の節数？
S407
NO
YES
X ← 任意の文字列を受理する文法
S408
m ← 1
S409
m ≦ C'のn番目の節内のリテラル数？
S410
NO
YES
R←C'のn番目の節内のm番目のリテラルが示す条件をオートマトン化
S411
X ← INTERSECT(X, R)
S412
m ← m+1
S413
Xの非終端記号名を変換後，Xの生成規則をGに追加。
生成規則S ::= Xの開始記号をGに追加
S414
n ← n+1
S415
終了 (Gを返す)
S416

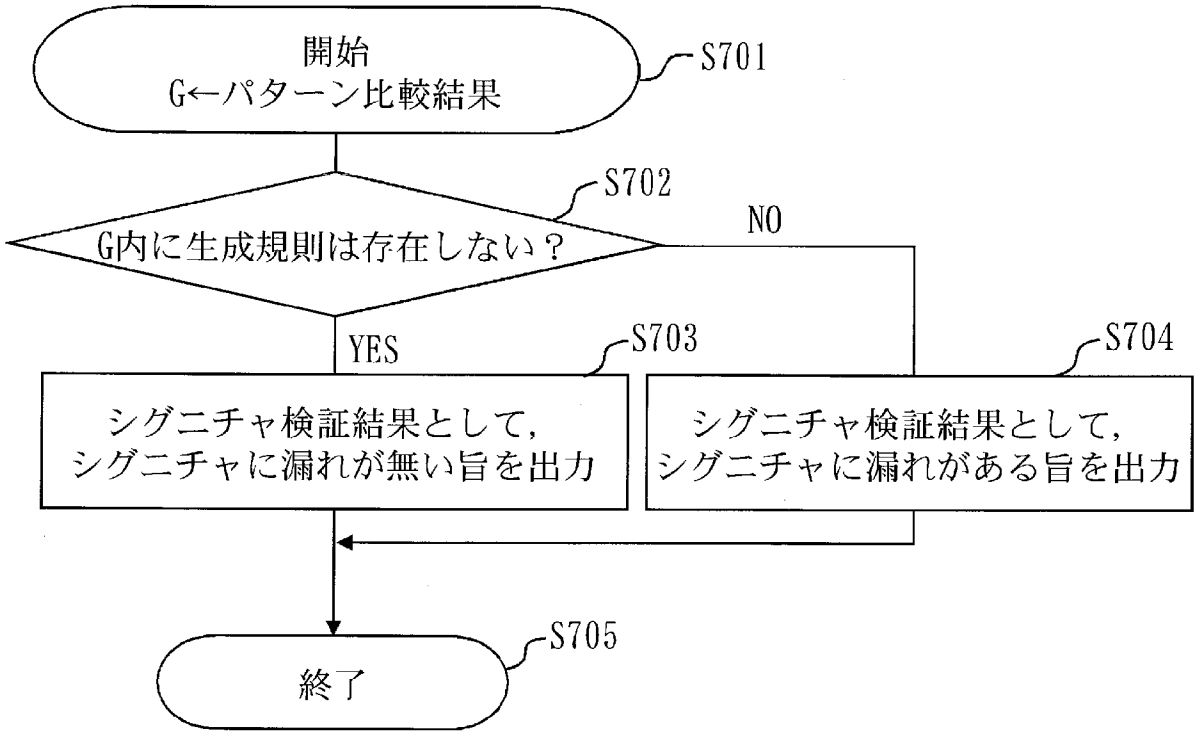
[図5]


501
502
503
504
505
506
507
条件
対応するオートマトン
入力文字列長 < N
506に示すオートマトンを生成する
入力文字列内にSTRを含む
507に示すオートマトンを生成する
「条件」の否定
「条件」に対応するオートマトンの受理可・不可を反転
・・・
・・・
N個
ANY
ANY
文字列STRに対応した状態遷移

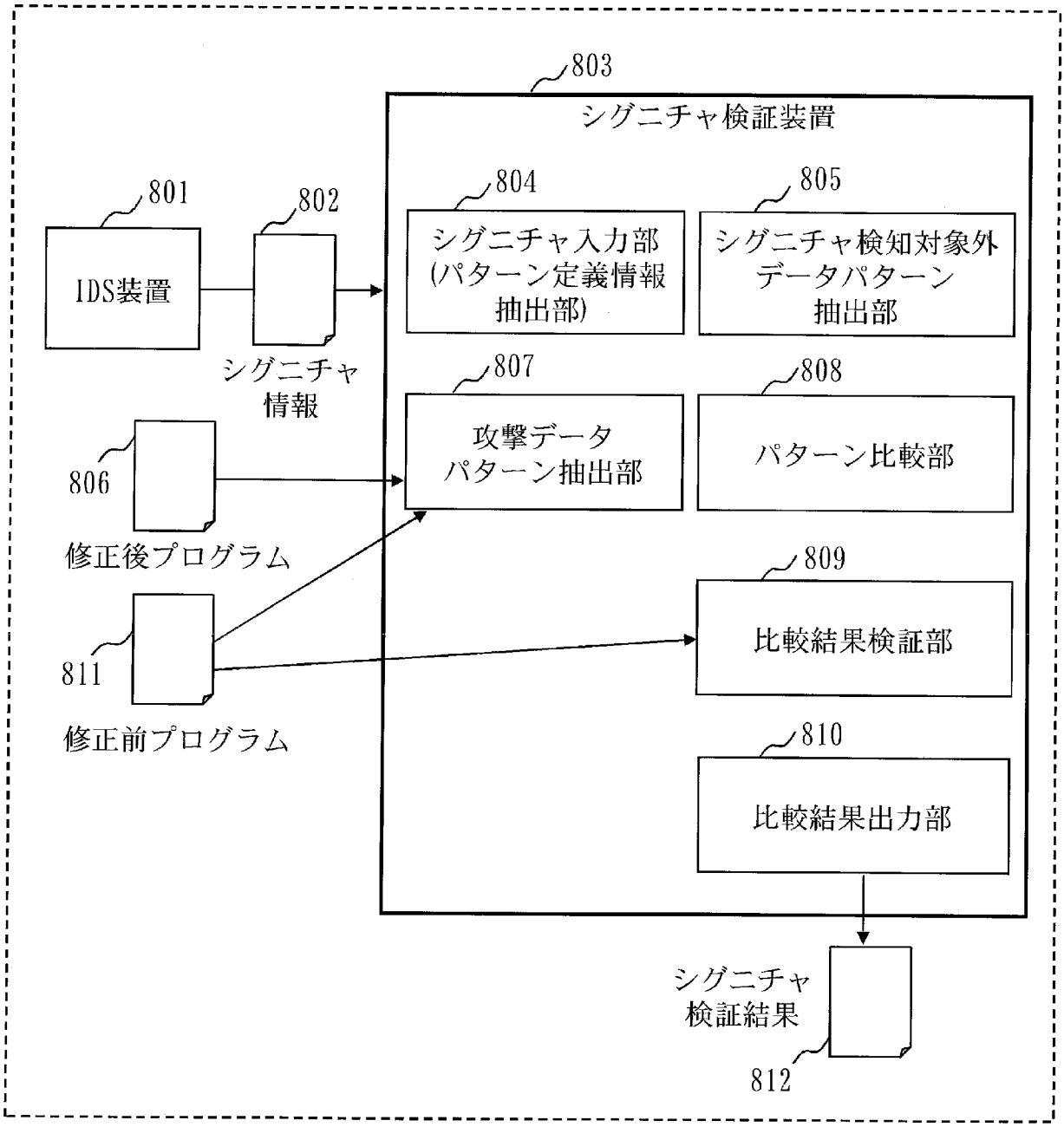
[図6]


開始
G←攻撃データパターン
S←シグニチャ検知対象外データパターン
S601
X ← INTERSECT (G, S)
S602
終了 (Xを返す)
S603

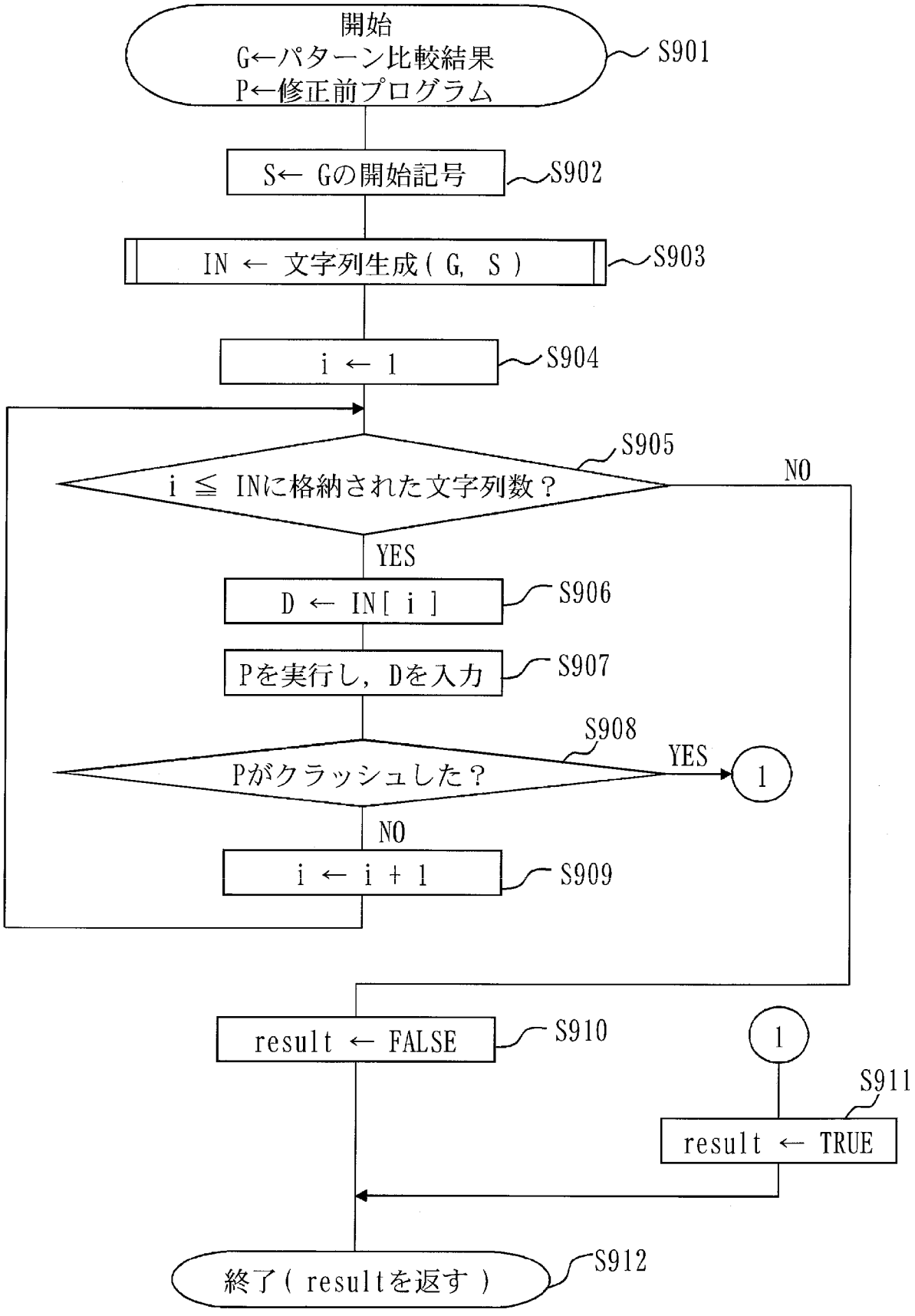
[図7]


開始
G←パターン比較結果
S701
S702
G内に生成規則は存在しない？
NO
YES
S703
シグニチャ検証結果として，
シグニチャに漏れが無い旨を出力
S704
シグニチャ検証結果として，
シグニチャに漏れがある旨を出力
S705
終了

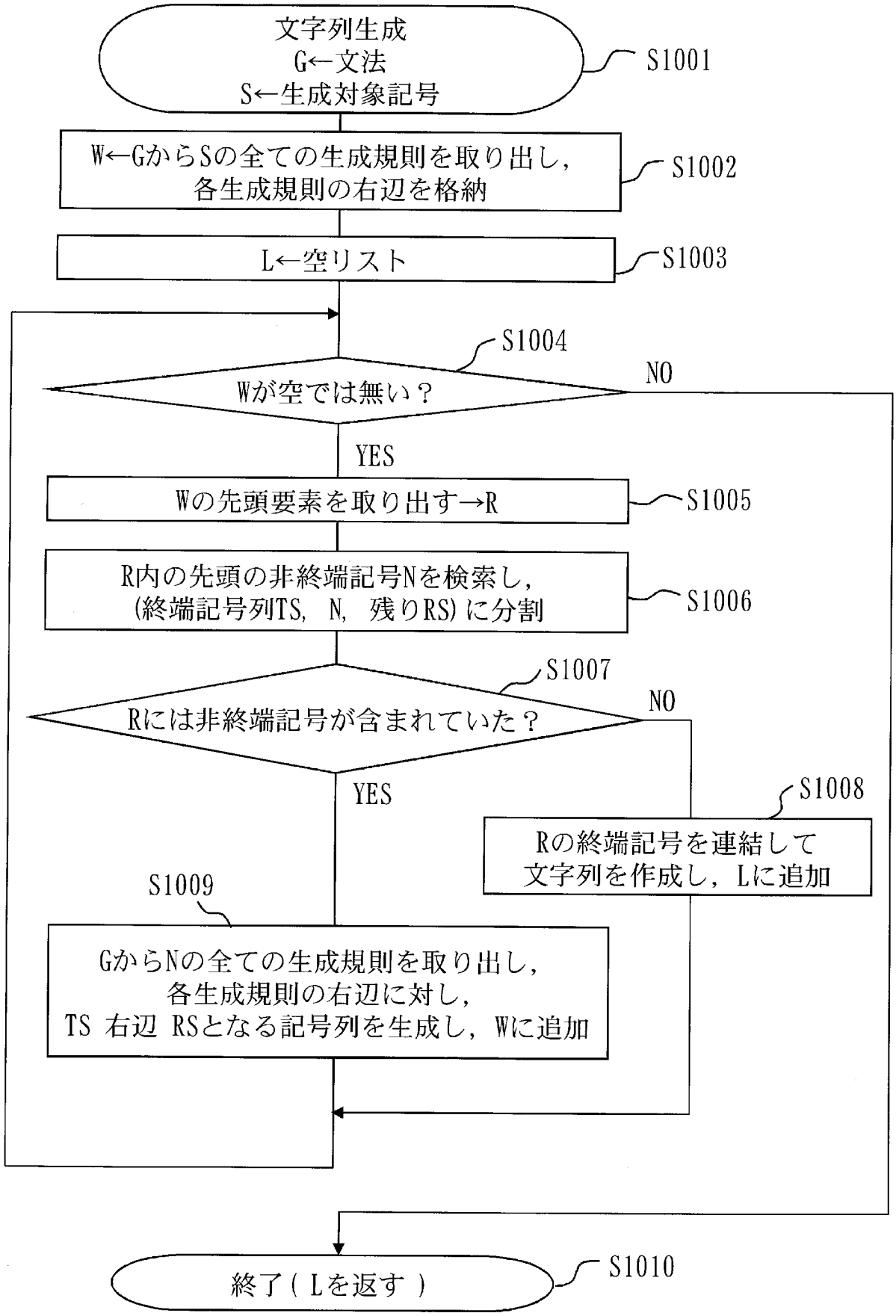
[図8]


803
シグニチャ検証装置
801
IDS装置
802
シグニチャ
情報
804
シグニチャ入力部
(パターン定義情報
抽出部)
805
シグニチャ検知対象外
データパターン
抽出部
807
攻撃データ
パターン抽出部
808
パターン比較部
806
修正後プログラム
809
比較結果検証部
811
修正前プログラム
810
比較結果出力部
シグニチャ
検証結果
812

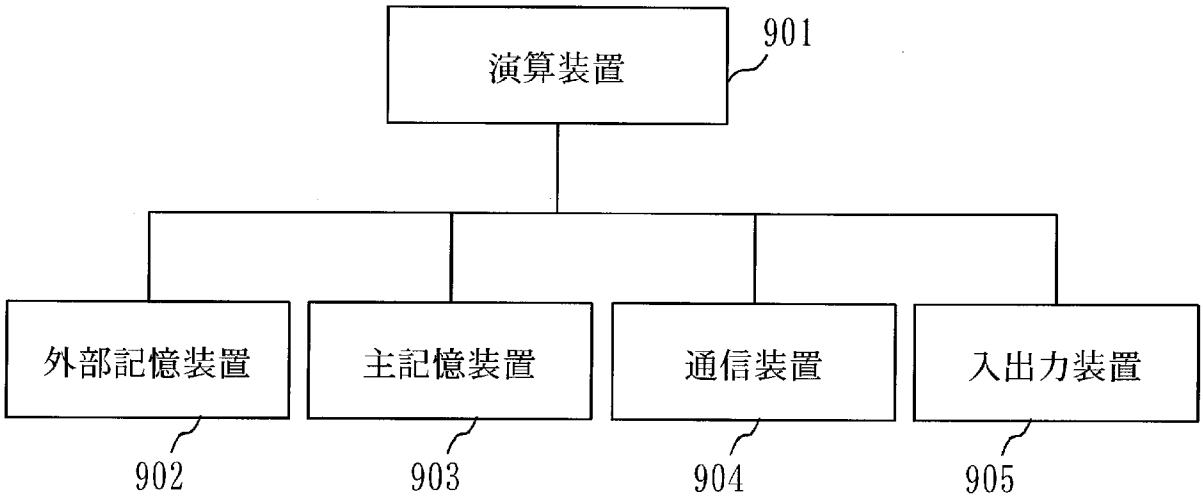
[図9]


開始
G←パターン比較結果
P←修正前プログラム
S901
S← Gの開始記号
S902
IN ← 文字列生成(G, S)
S903
i ← 1
S904
S905
i ≦ INに格納された文字列数？
NO
YES
D ← IN[i]
S906
Pを実行し，Dを入力
S907
S908
Pがクラッシュした？
YES
1
NO
i ← i + 1
S909
result ← FALSE
S910
1
S911
result ← TRUE
終了(resultを返す)
S912

[図10]


文字列生成
G←文法
S←生成対象記号
S1001
W←GからSの全ての生成規則を取り出し，
各生成規則の右辺を格納
S1002
L←空リスト
S1003
S1004
Wが空では無い？
NO
YES
Wの先頭要素を取り出す→R
S1005
R内の先頭の非終端記号Nを検索し，
(終端記号列TS，N，残りRS) に分割
S1006
S1007
Rには非終端記号が含まれていた？
NO
YES
S1008
Rの終端記号を連結して
文字列を作成し，Lに追加
S1009
GからNの全ての生成規則を取り出し，
各生成規則の右辺に対し，
TS 右辺 RSとなる記号列を生成し，Wに追加
終了（Lを返す）
S1010

[図11]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/073198

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/56(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)
G06F21/56

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 1996-2013
Kokai Jitsuyo Shinan Koho 1971-2013 Toroku Jitsuyo Shinan Koho 1994-2013

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 2007-242002 A (Mitsubishi Electric Corp.), 20 September 2007 (20.09.2007), paragraphs [0010] to [0040]; fig. 1 to 11 (Family: none)	1-12
A	BRUMLEY et al., Automatic Patch-Based Exploit Generation is Possible: Techniques and Implications:, 2008 IEEE Symposium on Security and Privvacy, 2008, p.143-157	1-12
A	Hiroki KUZUNO, Toyoo TAKATA, "Probabilistic Automata for Anomaly Detection", IPSJ Symposium Series, vol.2004, no.11, Computer Security Symposium 2004, 20 October 2004 (20.10.2004), pages 91 to 96	1-12

☐ 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
26 November, 2013 (26.11.13)	03 December, 2013 (03.12.13)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１３／０７３１９８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/56(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.　G06F21/56

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	１９７１－２０１３年
日本国実用新案登録公報	１９９６－２０１３年
日本国登録実用新案公報	１９９４－２０１３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 2007-242002 A（三菱電機株式会社） 2007.09.20，段落００１０－００４０，図１－１１ （ファミリーなし）	1-12
A	BRUMLEY et al., Automatic Patch-Based Exploit Generation is Possible: Techniques and Implications:, 2008 IEEE Symposium on Security and Privvacy, 2008, p.143-157	1-12

☑　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
２６．１１．２０１３	０３．１２．２０１３

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　４０９２
木村　励
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　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	葛野 弘樹，高田 豊雄，確率オートマトンを用いた異常検知手法，情報処理学会シンポジウムシリーズ Vol.2004，No.11，コンピュータセキュリティシンポジウム2004，2004.10.20，p.91-96	1-12