(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4635147号
(P4635147)
(45)発行日　平成23年2月16日(2011.2.16)　(24)登録日　平成22年12月3日(2010.12.3)

(51)Int.Cl.　F I
H04L 12/66 (2006.01)　H04L 12/66 B

請求項の数 4　(全 12 頁)

(21)出願番号　特願2005-333199(P2005-333199)
(22)出願日　平成17年11月17日(2005.11.17)
(65)公開番号　特開2007-142767(P2007-142767A)
(43)公開日　平成19年6月7日(2007.6.7)
審査請求日　平成20年6月23日(2008.6.23)

特許法第３０条第１項適用　２００５年５月１８日　社団法人情報処理学会発行の「情報処理学会シンポジウムシリーズＶｏｌ．２００５，Ｎｏ．５　先進的計算基盤システムシンポジウム　ＳＡＣＳＩＳ　２００５　論文集」に発表

(73)特許権者　504171134
国立大学法人　筑波大学
茨城県つくば市天王台一丁目１番１
(73)特許権者　301021533
独立行政法人産業技術総合研究所
東京都千代田区霞が関１－３－１
(74)代理人　100082669
弁理士　福田　賢三
(74)代理人　100095337
弁理士　福田　伸一
(74)代理人　100061642
弁理士　福田　武通
(72)発明者　山口　喜教
茨城県つくば市天王台一丁目１番１　国立大学法人筑波大学内

最終頁に続く

(54)【発明の名称】パターンマッチング装置、その形成方法、それを用いたネットワーク不正侵入検知装置の動作方法、およびそれを用いた侵入防止システムの動作方法

(57)【特許請求の範囲】
【請求項１】
複数の入力信号の積をとる演算回路と、前記演算回路の演算結果を予め決められた時間保持する保持回路と、からなる単位ステートマシンを複数備えるＮＦＡステートマシンと、
伝送された符号と、探索する符号と、の比較を行なう比較器と、
を含み、
前記の演算回路は、初段では予め決められた論理値の出力、あるいは、それ以降の段では前段の単位ステートマシンの出力と、上記の比較器の出力との積をとり、予め決められた段から探索結果を出力するものであって、
複数の単位ステートマシンが出力端まで直列接続された少なくともひとつの構成Ａと、上記の直列接続の中間点から分岐し、他の出力端まで接続された構成Ｂと、をもち、
上記の分岐点の位置を、該分岐点の前段では、構成Ａと構成Ｂとの行なう探索が共通の探索であるように定めたことを特徴とするパターンマッチング装置。
【請求項２】
再構成可能な半導体集積回路上のステートマシンを用いたパターンマッチング装置の形成方法で、
１）検査ルールからNFAを生成して、ルール中のマッチングパターンそれぞれを集約したNFAを再生成するステップと、
２）生成したNFA中に存在する重複ステートを抽出して、仮のパターンマッチング回路を

構成するステップと、
３）上記の仮のパターンマッチング回路における重複ゲートを抽出して、パターンマッチング回路を生成するステップと、
４）また、ヘッダ検査ルールからはヘッダ検査回路を、生成するステップと、
５）ヘッダ－ペイロードルールの対応表から検出判定回路を生成するステップと、
６）生成したパターンマッチング回路とヘッダ検査回路と検出判定回路とを、上記の再構成可能な半導体集積回路に書き込むことを特徴とする請求項１に記載のパターンマッチング装置の形成方法。
【請求項３】
ネットワークインタフェース部と、ネットワークフレーム抽出部と、ヘッダ・ペイロード分離部と、ヘッダ検査部と、パターンマッチング部とに入力するステップと、パターンマッチング部と、検出判定部とを備えるネットワーク不正侵入検知装置の動作方法で、
１）ネットワークインタフェースを通じて入力したネットワークストリームからネットワークフレームを抽出するステップと、
２）ネットワークフレームの種別を解析してヘッダとペイロードに分離するステップと、
３）上記の分離したヘッダとペイロードとを、それぞれヘッダ検査部、パターンマッチング部に入力するステップと、
４）上記のヘッダ検査部、パターンマッチング部で各々検出された結果を、検出判定部でルールに合致するかどうか判断するステップと、
５）上記のルールに合致する場合は、検出結果を整形し外部に出力するステップと、を含み、
上記のパターンマッチング部は請求項１のパターンマッチング装置で構成されていることを特徴とするネットワーク不正侵入検知装置の動作方法。
【請求項４】
ネットワークインタフェース部と、ネットワークフレーム抽出部と、ヘッダ・ペイロード分離部と、ヘッダ検査部と、パターンマッチング部とに入力するステップと、パターンマッチング部と、検出判定部と、フレーム遮断・出力部とを備える侵入防止システムの動作方法で、
侵入防止システムに請求項１に記載のパターンマッチング装置を用いる方法で、
１）ネットワークインタフェースより入力されたネットワークストリームからネットワークフレームを抽出するステップと、
２）ネットワークフレームをヘッダ・ペイロード分離部とディレイ部とにそれぞれ複製して入力するステップと、
３）ヘッダ・ペイロード部によりネットワークフレームの種別を解析してヘッダとペイロードに分離し、それぞれヘッダ検査部、パターンマッチング部に入力するステップと、
４）ヘッダ部、パターンマッチング部で各々検出された結果を検出判定部でルールに合致するかどうか判断するステップと、
５）上記のルールに合致する場合は、選択されたルールをメモリ上に一時的に蓄積するステップと、
６）ディレイ部からネットワークフレームが出力される際に、対応する既に算出した検査結果をメモリより読み出すステップと、
７）上記の検査結果に従ってネットワークフレームを遮断するか出力するか決定するステップと、を含み、
上記のパターンマッチング部は請求項１のパターンマッチング装置で構成されていることを特徴とする侵入防止システムの動作方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、ネットワーク通信におけるパケット処理においてパターンマッチングを用いて文字列や記号列の探索を行う必要のある分野に関している。

【背景技術】
【０００２】
近年ではネットワークにおけるサービスに社会が依存する傾向にあり、ネットワーク上におけるセキュリティの重要性が高まっている。しかし、ネットワークを利用する人口が増加するに従い、ネットワークサービスに対する攻撃や侵入が増加し、サービスに障害をもたらす要因となっている。このネットワークサービスに対する攻撃や侵入を検知し防御を行う起点となる技術が、パターンマッチング技術を用いるＮＩＤＳ（Network Intrusion Detection System）である。ＮＩＤＳでは常時ネットワークの状態を監視し侵入や攻撃の検知を行うため、その処理速度はネットワークのスループットと同じである事が望まれる。ＮＩＤＳの一つに、攻撃・侵入ルールのパターンマッチングによる検知を行うＳＮＯＲＴがあるが、ソフトウェアによるパターンマッチング処理を行っているため、その処理速度は１Ｇｂｐｓに満たない。
【０００３】
パターンマッチング処理用として、ＮＦＡ（Nondeterministic Finite Automaton）によりパターンマッチング回路を再構成可能なデバイスＦＰＧＡ（Field Programmable Gate Array）上に構成し、高速な処理を行う研究が幾つかなされている。ＮＩＤＳでは、新たな攻撃や侵入に従ってマッチングパターンが変更されるためＮＦＡによるパターンマッチングの場合ＡＳＩＣに実装するのは実用的でなく、ＦＰＧＡのような再構成可能なハードウェアがパターンマッチングエンジンとして用いられる。
【０００４】
この従来のＮＦＡによるパターンマッチング回路は、１クロックサイクル当り１バイトを処理するため、その処理性能は１．９６Ｇｂｐｓ（２４５．９７ＭＨｚ、３０６７５文字、FPGA：Xilinx xc2vp100-6　時）程度であった。このＮＦＡによるパターンマッチング回路を１クロック当り複数バイト処理する構成に改変し、処理性能を向上させる研究がなされている。しかし、改変による回路規模の増大は大きく、４バイト処理するＮＦＡ回路は、２５００２文字のマッチングパターンにおいてＦＰＧＡ（Xilinx xc2v-8000）の１００％を使用するものであった。
【０００５】
パターンマッチング回路を実現する方法として、これまでに、非特許文献１に記載されているようなマッチングパターンを表す正規表現からＮＦＡを構成し、これを回路化する方法が知られている。しかし、この方法では、１クロックサイクル当りに処理する入力データ幅が１バイトであったため、高いスループットを得ることが困難であった。また、非特許文献２に記載されているようにＮＦＡより構成したパターンマッチング装置が１クロックサイクルあたりに処理する入力データ幅を拡張し、回路のスループットを向上させる技術も知られている。しかし、この技術では、スループットは向上するものの、データ幅の倍化に伴って回路規模も同様に倍化するため、現実的に適用できるものではなかった。
【０００６】
これら従来の技術では、探索しようとするマッチングパターンが複数ある場合に、それぞれのマッチングパターンに対して独立したステートマシンを生成することによりマッチング回路を構築していた。そのため、マッチングパターン数の増大に比例して回路規模の増大していた。
【０００７】
上記の様に、ネットワークセキュリティシステムのＮＩＤＳは、ネットワークにおける攻撃や侵入を検知するシステムである。ＮＩＤＳで定義ファイルを用いるシグネチャ方式を採るシステムでは、ネットワークパケットと攻撃・侵入パケットデータベースとのパターンマッチング処理が行われている。このパターンマッチング処理をソフトウェアで行うとスループットが数十Ｍｂｐｓ～１Ｇｂｐｓ程度と低速であるため、ハードウェアによるパターンマッチング処理による高速化がなされてきた。
【０００８】
ハードウェアによるパターンマッチング処理のうち、ＮＦＡ（Non-deterministic Fini

te Automaton）によってパターンマッチング装置を構成する方法が存在する。このパターンマッチング装置で、例えば、文字列「ａｂｂ」を検出する場合の構築手順を図１に示す。

【０００９】

通常は、探索を受ける情報を、探索を容易にするために正規表現（通常の文字と、メタキャラクタと呼ばれる特別な意味を持った記号を組み合わせた表記）に変換しておく。また、探索しようとする文字列や記号列を変換して得られるマッチングパターンを示す正規表現からＮＦＡステートマシンを生成する。このＮＦＡステートマシン中のステート１つに１状態を保持するステートマシンを割り当ててパターンマッチング装置を構築する。

【００１０】

このような従来の技術では、パターンマッチング装置の処理データ幅を増やすと回路規模が大幅に増大してしまう、という問題があった。さらに、探索するマッチングパターンの数を増やすと回路規模が比例して増大してしまう、という問題もあった。これは、探索するマッチングパターンが複数ある場合に、それぞれのマッチングパターンに対して独立したＮＦＡを生成してパターンマッチング装置を構築していたためである。

【００１１】

従来の技術によるパターンマッチング装置の構成を図２に示す。図２に示すパターンマッチング装置の処理するバイト幅は４バイトである。この装置は、入力されたデータを１バイト毎に比較する比較器部と各々のマッチングパターンに対応したステートマシン部より構成される。

【００１２】

【非特許文献１】Reetinder Sidhu, Viktor K. Prasanna, "Fast Regular Expression Matching using FPGAs",Proceedings of IEEE FCCM 2001, Apr 2001.

【非特許文献２】Christopher R. Clark, David E. Schimmel "Scalable Pattern Matching for High Speed Networks", FCCM2004, pp.249 -257, Apr 20 -23, 2004, Napa, California.

【発明の開示】

【発明が解決しようとする課題】

【００１３】

従来の技術では、パターンマッチング装置の処理データ幅を増やすと回路規模が大幅に増大してしまう問題があった。さらに、探索するマッチングパターンの数を増やすと回路規模が比例して増大してしまう問題もあった。

【発明の効果】

【００１４】

本発明のパターンマッチング装置の構成を採ることにより、パターンマッチング装置の回路規模の増大を抑制しつつ入力データ幅を拡張することが可能である。これにより、ＮＩＤＳ（Network Intrusion Detection System：ネットワーク不正侵入検知システム）に使用されるマッチングパターン全てに対応しつつ高いスループットを持つパターンマッチング装置を１つのＦＰＧＡ（Field Programmable Gate Array：再構成可能な半導体集積回路）デバイス上に搭載することができる。

【課題を解決するための手段】

【００１５】

従来、複数のマッチングパターンそれぞれからステートマシンを生成していたが、本発明では、このステートマシンの数を集約するものである。このため、本発明のパターンマッチング装置では、複数の入力信号の積をとる演算回路と、前記演算回路の演算結果を予め決められた時間保持する保持回路と、からなる単位ステートマシンを複数備えるＮＦＡステートマシンと、伝送された符号と、検索する符号と、の比較を行なう比較器と、を含み、前記の演算回路は、初段では予め決められた論理値の出力、あるいは、それ以降の段では前段の単位ステートマシンの出力と、上記の比較器の出力との積をとり、予め決められた段から検索結果を出力するものであって、複数の単位ステートマシンが出力端まで直

列接続された少なくともひとつの構成Ａと、上記の直列接続の中間点から分岐し、他の出力端まで接続された構成Ｂと、をもち、上記の分岐点の位置を、該分岐点の前段では、構成Ａと構成Ｂとの行なう検索が共通の検索であるように定める。

【００１６】

また、ステートマシンを再構成可能な半導体集積回路上に構成して、上記のパターンマッチング装置を形成する方法は、攻撃あるいは侵入パケットを検出するルールを入力するステップと、ネットワークフレーム中のヘッダを検査するルールと、ペイロードを検査するルール（マッチングパターン）と、ヘッダルールとペイロードルールとを対応付ける表と、を分離するステップと、の後に、

１）検査ルールからＮＦＡを生成して、ルール中のマッチングパターンそれぞれを集約したＮＦＡを再生成するステップと、

２）生成したＮＦＡ中に存在する重複ステートを抽出して、仮のパターンマッチング回路を構成するステップと、

３）上記の仮のパターンマッチング回路における重複ゲートを抽出して、パターンマッチング回路を生成するステップと、

４）また、ヘッダ検査ルールからはヘッダ検査回路を、生成するステップと、

５）ヘッダーペイロードルールの対応表から検出判定回路を生成するステップと、

６）生成したパターンマッチング回路とヘッダ検査回路と検出判定回路とを、上記の再構成可能な半導体集積回路に書き込む、というものである。

【００１７】

また、本発明は、ネットワークインタフェース部と、ネットワークフレーム抽出部と、ヘッダとペイロード分離部と、ヘッダ検査部と、パターンマッチング部とに入力するステップと、パターンマッチング部と、検出判定部とを備えるネットワーク不正侵入検知装置の動作方法で、

１）ネットワークインタフェースを通じて入力したネットワークストリームからネットワークフレームを抽出するステップと、

２）ネットワークフレームの種別を解析してヘッダとペイロードに分離するステップと、

３）上記の分離したヘッダとペイロードとを、それぞれヘッダ検査部、パターンマッチング部に入力するステップと、

４）上記のヘッダ検査部、パターンマッチング部で各々検出された結果を、検出判定部でルールに合致するかどうか判断するステップと、

５）上記のルールに合致する場合は、検出結果を整形し外部に出力するステップと、を含み、上記のパターンマッチング部は請求項１のパターンマッチング装置で構成したものである。

【００１８】

また、本発明は、ネットワークインタフェース部と、ネットワークフレーム抽出部と、ヘッダ・ペイロード分離部と、ヘッダ検査部と、パターンマッチング部とに入力するステップと、パターンマッチング部と、検出判定部と、フレーム遮断・出力部とを備える侵入防止システムの動作方法で、

侵入防止システムに請求項１に記載のパターンマッチング装置を用いる方法で、

１）ネットワークインタフェースより入力されたネットワークストリームからネットワークフレームを抽出するステップと、

２）ネットワークフレームをヘッダ・ペイロード分離部とディレイ部とにそれぞれ複製して入力するステップと、

３）ヘッダ・ペイロード部によりネットワークフレームの種別を解析してヘッダとペイロードに分離し、それぞれヘッダ検査部、パターンマッチング部に入力するステップと、

４）ヘッダ部、パターンマッチング部で各々検出された結果を検出判定部でルールに合致するかどうか判断するステップと、

５）上記のルールに合致する場合は、選択されたルールをメモリ上に一時的に蓄積するステップと、

６）ディレイ部からネットワークフレームが出力される際に、対応する既に算出した検査結果をメモリより読み出すステップと、
７）上記の検査結果に従ってネットワークフレームを遮断するか出力するか決定するステップと、を含み、
上記のパターンマッチング部は上記のパターンマッチング装置で構成したものである。
【発明を実施するための最良の形態】
【００１９】
以下に、この発明の実施の形態を図面に基づいて詳細に説明する。
【実施例１】
【００２０】
上記のように、従来は複数のマッチングパターンそれぞれからステートマシンを生成していたが、本発明では、このステートマシンを集約するものである。さらに、ステートマシンのステート遷移条件を生成するＡＮＤゲート２、パターン検出信号を生成するＯＲゲート３をステートマシン１の回路と独立させる。一例として、図３に本発明の技術によるパターンマッチング装置の構成を示す。前記構成は、入力されたデータを１バイト毎に比較する比較器部、ＡＮＤゲート群、マッチングパターン全てを含んだ１つのステートマシン、ＯＲゲート群より成る。図３の単位ステートマシンＡ、Ｂ、Ｃでは、単位ステートマシンＡを共有して、ＡとＢの、あるいはＡとＣの単位ステートマシンの直列接続と同様の結果が得られる。
【００２１】
このようにステートマシンを集約することで、ステートマシン中で同じ状態を表すステートが抽出可能となる。重複したステートを共有・削減することにより回路規模の削減を図る。さらに、ステート遷移条件を生成するＡＮＤ群中にも同じ条件を表すＡＮＤゲートが抽出でき、これも共有・削減することにより一層の回路規模の削減を図る。
【００２２】
また、一例として、図４に同じ状態を表すステートの削減方法を示す。図４（１）、（２）は、それぞれ、従来の場合と本発明の場合、である。マッチングパターン間で接頭パターンが同じであれば、その接頭パターンを表すステートは重複しており、共有が可能である。図では「ａｂｃ」「ａｂｂ」の２つのマッチングパターンを例として挙げているが、「ａｂｃ」「ａｂｂ」は「ａｂ」が同じであるため、このパターンを表すステートが共有されている。
【００２３】
次に、一例として、図５に同じステート遷移条件を生成するＡＮＤゲートの削減方法を示す。例として、処理するデータ幅が４バイトであるパターンマッチング装置において、マッチングパターン「ａｂｃ」「ｂｂｃ」を検出するステートマシンのステート遷移に必要な条件を示す。点線で囲まれた条件は同じ遷移条件を表しており、該当するＡＮＤゲートを共有あるいは削減することができる。
【００２４】
上記の共有あるいは削減により、回路規模を従来の回路構成と比べて半分以下に削減することが可能であり、１つのデバイス上にＮＩＤＳで必要とされるパターンマッチング回路を構築することが現実的となる。また、回路規模の大幅な削減により低消費電力効果が期待できる。
【００２５】
一般に、ＮＦＡによるパターンマッチング装置を構成する際、処理データ幅を増大しスループットの向上を図ると、回路規模が大幅に増大する。しかし、マッチングパターンからＮＦＡベースのパターンマッチング装置を構成する際、上記の様に、各々のパターンから生成されるステートマシンを１つのステートマシンに集約して共有可能なステート等を抽出することにより、処理データ幅を増大しつつ回路規模増大の抑制を行うことができる。
【実施例２】

【００２６】
次に、再構成可能な半導体集積回路をパターンマッチング回路に用いて、ステートマシンを自動生成する装置の動作方法を説明する。この装置のブロック図を図９に示す。この装置は、検出すべきネットワークフレームを特定するためのルールをルール解析部５に入力すると、分離部６でネットワークフレーム中のヘッダを検査するルール、ペイロードを検査するルール、そしてヘッダルールとペイロードルールに対応して３つに分離される。分離された信号の１つはヘッダ検査回路生成部８を通り、半導体集積回路のソースコードの一部を出力する。また、他の１つは、ＮＦＡ生成部７、重複ステート・重複ゲート抽出部９、パターンマッチング回路生成部１１を通り、半導体集積回路のソースコードの一部を出力する。ここでは、自動的にイーサネット（登録商標）フレームのヘッダに対するルールとペイロードに対するマッチングパターンを抽出し、ヘッダ検査回路、パターンマッチング回路、ルール検出判定回路を生成する。残りの信号は、検出判定回路生成部１０で処理され半導体集積回路のソースコードの一部を出力する。これらのソースコードを用いて再構成部１２で半導体集積回路の再構成を行なう。
【００２７】
上記のパターンマッチング回路を自動生成する装置をシグネチャ方式のＮＩＤＳに適用する場合を以下で説明する。一般に、シグネチャ方式のＮＩＤＳでは、攻撃や侵入を検出するためのルールを定義し、このルールを元に検出処理を行う。本ソフトウェアは攻撃・侵入パケットを検出するルールから、検出処理する回路を自動生成する装置である。本ソフトウェアの処理手順を図６に示す。本装置は、
１）攻撃あるいは侵入パケットを検出するルールを入力すると、
２）ネットワークフレーム中のヘッダを検査するルールとペイロードを検査するルール（マッチングパターン）、そしてヘッダルールとペイロードルールを対応付ける表の３つに分離する。
３）ペイロード検査ルールからはＮＦＡを生成し、ルール中のマッチングパターンそれぞれを集約したＮＦＡを再生成する。
４）そして、生成したＮＦＡ中に存在する重複ステートを抽出し、
５）仮のパターンマッチング回路を構成後、
６）さらに重複ゲートを抽出して、パターンマッチング回路を生成する。
７）また、ヘッダ検査ルールからはヘッダ検査回路、ヘッダ－ペイロードルールの対応表からは検出判定回路を生成する。
本装置では、入力した攻撃・侵入ルールからサブセットのルールを生成し回路化することもできる。また、回路が処理するデータ幅を指定することができ、容易に高いスループットを持つ回路を生成することもできる。
【実施例３】
【００２８】
次に、本発明をＮＩＤＳ（ネットワーク不正侵入検知）装置に適用する場合について説明する。これは、あらかじめ設定されたマッチングパターンに従ってネットワークフレームを検査することで、攻撃や侵入を検出する装置である。ＮＩＤＳ装置の構成を図７に示す。本装置は、
１）まずネットワークＩＦ（インタフェース）より入力されたネットワークストリームからネットワークフレームを抽出する。
２）そして、ネットワークフレームの種別を解析してヘッダとペイロードに分離し、
３）それぞれヘッダ検査部、パターンマッチング部に入力する。
４）ヘッダ部、パターンマッチング部で各々検出された結果を検出判定部でルールに合致するかどうか判断する。
５）１つのネットワークフレームが複数のルールに合致する場合は、プライオリティエンコーダにより重要なルールが選択される。最後に結果を整形し外部に出力する。
【００２９】
本装置により、ネットワーク上の攻撃や侵入をネットワークのワイヤスピードで検査す

ることができる。また、本装置を構成する、パターンマッチング、ヘッダ検査、検出判定の回路は実施例（１）で示した装置により生成される。

【実施例４】

【００３０】

次に、本発明をＩＰＳ（Intrusion Protection System：侵入防止システム）装置に適用する場合について説明する。これは、あらかじめ設定されたマッチングパターンに従ってネットワークフレームを検査することで攻撃や侵入を検出し、さらに有害なネットワークフレームは遮断する装置である。ＩＰＳ装置の構成を図７に示す。

【００３１】

１）本装置は、まずネットワークＩＦ（インタフェース）より入力されたネットワークストリームからネットワークフレームを抽出する。

２）ネットワークフレームはヘッダ・ペイロード分離部とディレイ部にそれぞれ複製されて入力される。

３）そして、ヘッダ・ペイロード部によりネットワークフレームの種別を解析してヘッダとペイロードに分離し、

４）それぞれヘッダ検査部、パターンマッチング部に入力する。

５）ヘッダ部、パターンマッチング部で各々検出された結果を検出判定部でルールに合致するかどうか判断する。１つのネットワークフレームが複数のルールに合致する場合は、プライオリティエンコーダにより重要なルールが選択される。選択されたルールはメモリ上に一時的に蓄積される。

６）最後に、ディレイ部からネットワークフレームが出力される際に、対応する既に算出した検査結果をメモリより読み出される。

７）このとき、検査結果に従ってネットワークフレームを遮断するか出力するか決定する。

【００３２】

本装置により、ネットワーク上の攻撃や侵入をネットワークのワイヤスピードで検査することができるほか、危険なネットワークフレームを遮断することができる。本装置を構成する、パターンマッチング、ヘッダ検査、検出判定の回路は実施例(1)で示した装置により生成される。

【産業上の利用可能性】

【００３３】

本発明のパターンマッチング装置の使用目的は、ネットワークのセキュリティの向上に限定される理由はなく、データベースの検索にも用いることができる。また、文字や記号に限定する理由もなく、アナログ信号であっても、符号化した後の情報を用いて探索を行なうことができる。

【図面の簡単な説明】

【００３４】

【図１】文字列「ａｂｂ」を検出するパターンマッチング装置の構築手順を説明するためのブロック図である。

【図２】従来のパターンマッチング装置のブロック図である。

【図３】本発明を用いたパターンマッチング装置のブロック図である。

【図４】同じ状態を表すステートの削減を示す模式図である。

【図５】同じステート遷移条件を生成するANDゲートの削減を示す模式図である。

【図６】パターンマッチング装置を自動生成する装置の処理手順を示す図である。

【図７】ＮＩＤＳ装置のブロック図である。

【図８】ＩＰＳ装置のブロック図である。

【図９】パターンマッチング装置を自動生成する装置のブロック図である。

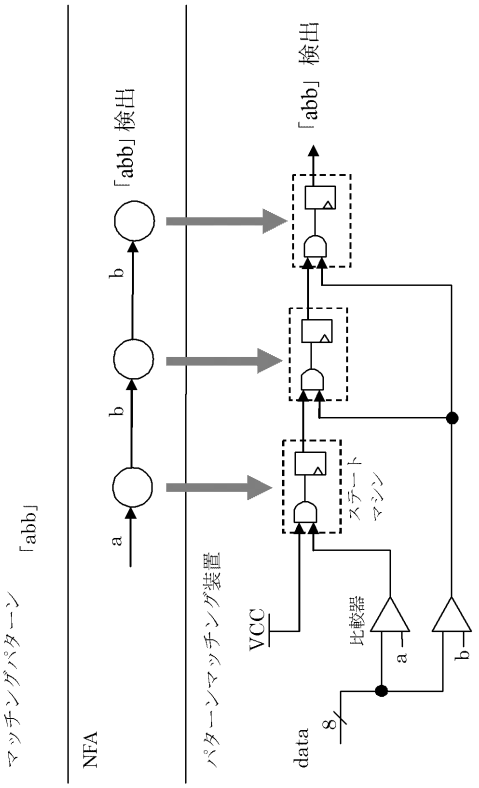
【符号の説明】

【００３５】

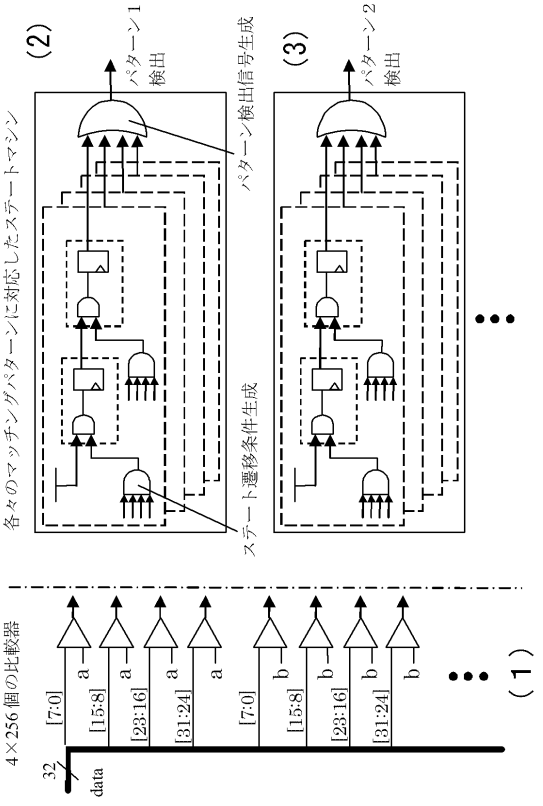
１　ステートマシン

２　ＡＮＤゲート
３　ＯＲゲート
４　単位ステートマシン
５　ルール解析部
６　分離部
７　ＮＦＡ生成部
８　ヘッダ検査回路生成部
９　重複ステート・重複ゲート抽出部
１０　検出判定回路生成部
１１　パターンマッチング回路生成部
１２　再構成部

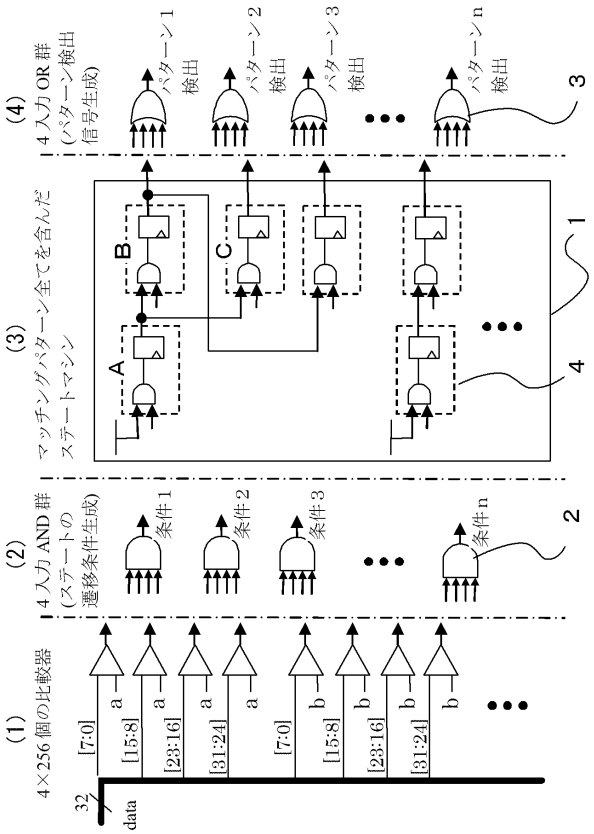
【図１】



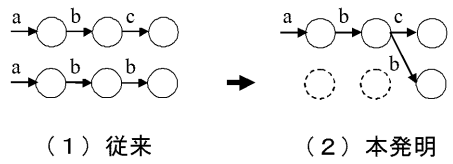
【図２】



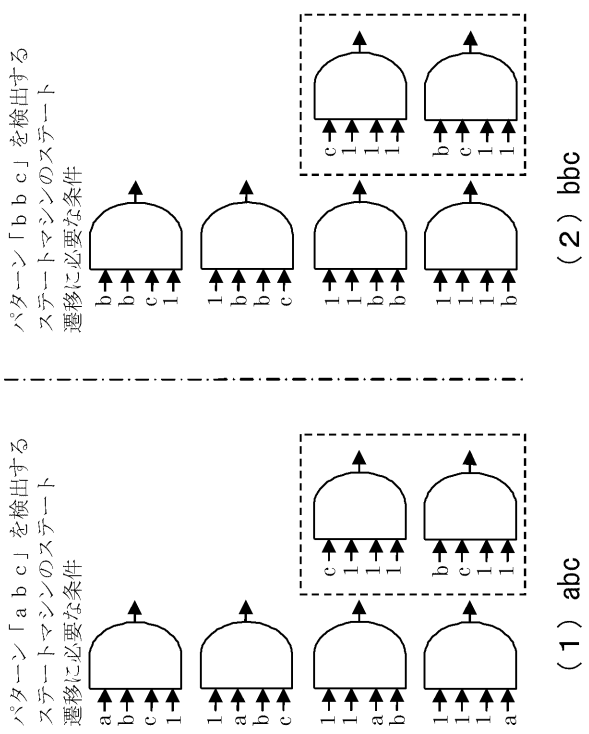
【図３】


(1)
4×256 個の比較器
32
data
[7:0]
[15:8]
[23:16]
[31:24]
(2)
4 入力 AND 群
(ステートの
遷移条件生成)
条件 1
条件 2
条件 3
条件 n
(3)
マッチングパターン全てを合んだ
ステートマシン
A
B
C
(4)
4 入力 OR 群
(パターン検出
信号生成)
パターン 1
検出
パターン 2
検出
パターン 3
検出
パターン n
検出

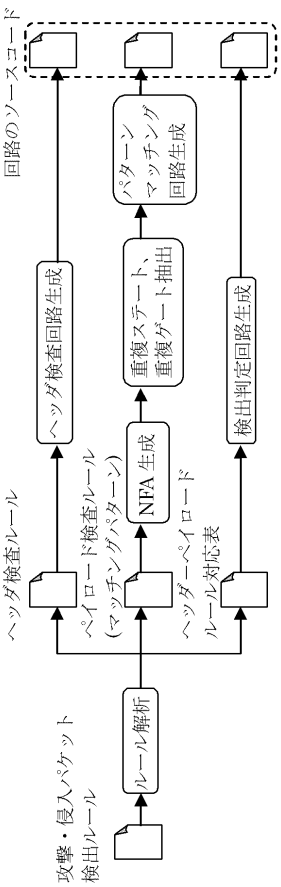
【図４】


（１）従来
（２）本発明

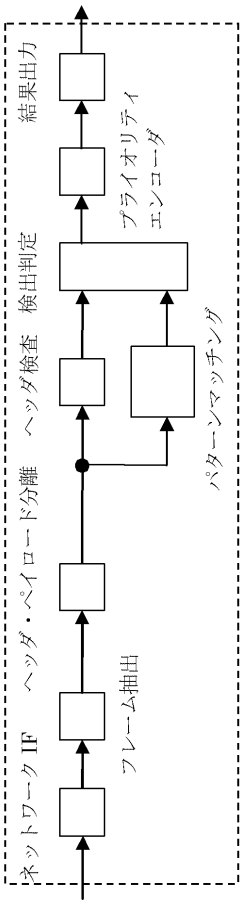
【図５】


パターン「ａｂｃ」を検出する
ステートマシンのステート
遷移に必要な条件
（１）abc
パターン「ｂｂｃ」を検出する
ステートマシンのステート
遷移に必要な条件
（２）bbc

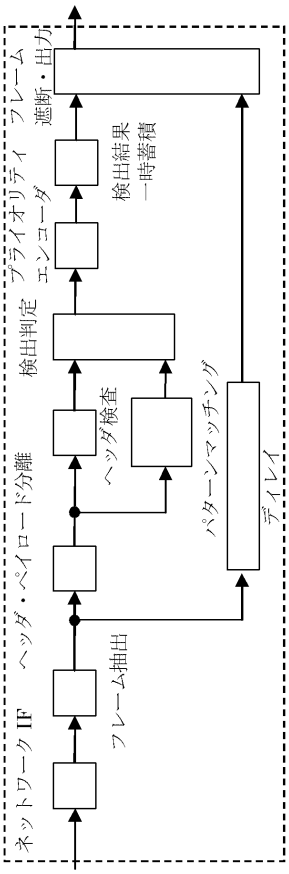
【図６】


攻撃・侵入パケット
検出ルール
ルール解析
ヘッダ検査ルール
ペイロード検査ルール
(マッチングパターン)
ヘッダーペイロード
ルール対応表
NFA 生成
ヘッダ検査回路生成
重複ステート、
重複ゲート抽出
パターン
マッチング
回路生成
検出判定回路生成
回路のソースコード

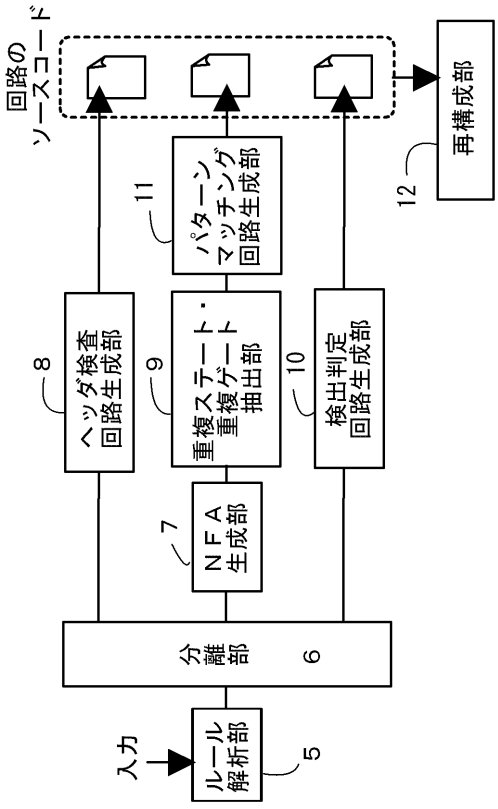
【図７】


ネットワークIF
ヘッダ・ペイロード分離
ヘッダ検査
検出判定
結果出力
フレーム抽出
パターンマッチング
プライオリティ
エンコーダ

【図８】


ネットワークIF
ヘッダ・ペイロード分離
検出判定
プライオリティ
エンコーダ
フレーム
遮断・出力
検出結果
一時蓄積
ヘッダ検査
パターンマッチング
フレーム抽出
ディレイ

【図９】


回路の
ソースコード
再構成部
12
パターン
マッチング
回路生成部
11
ヘッダ検査
回路生成部
8
重複ステート・
重複ゲート
抽出部
9
検出判定
回路生成部
10
NFA
生成部
7
分離部
6
入力
ルール
解析部
5

フロントページの続き

(72)発明者　前田　敦司
茨城県つくば市天王台一丁目１番１　国立大学法人筑波大学内
(72)発明者　片下　敏宏
茨城県つくば市天王台一丁目１番１　国立大学法人筑波大学内
(72)発明者　戸田　賢二
茨城県つくば市東１－１－１　独立行政法人産業技術総合研究所つくばセンター内

審査官　矢頭　尚之

(56)参考文献　特表２００５－５２７０４２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／６６