1G ネットワーク対応の H/W IDP の検討

稲田　徹†　　竹内　清史†　　鈴木　清彦†　　小貫　淳史†　後沢 忍†
三菱電機(株)情報技術総合研究所†

１．はじめに

近年、ネットワークは、社会インフラとして機能し始め、それに伴い、ネットワークを舞台としたテロや犯罪行為が急増している。これらの行為の対策として、不正侵入の検知と同時に不正侵入パケットそのものを遮断する IDP(侵入検知/遮断装置)を導入するケースが増えている。IDP は、その特性上、ネットワークの中間に位置するため、通常のネットワークトラフィックに影響を与えない、非常に高速な検知が必要とされる。我々は、現在、普及し始めた 1G イーサネットに対応するため、パケットの受信から、コンテンツの検索までを全て H/W で行う IDP を開発した。本稿では、IDP の H/W 実装時の課題とその解決方式を紹介する。

２．IDP の動作

2.1　通常のパケットに対する動作

IPD の通常パケット(非分割パケット)に対する概略動作を図１に示す。

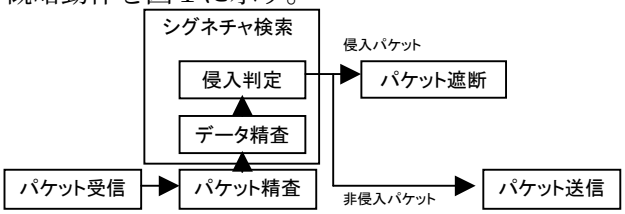

図１　IDP の動作(非分割パケット)

パケットを受信した IDP は、まず、パケットの精査(ヘッダ精査、他)を実施しした後、シグネチャと呼ばれる侵入パターンを示すファイルとパケットのデータ部の精査(主に文字列検索)を実施する。データ精査の結果、侵入パケットであると判断されたパケットは、速やかに廃棄(遮断)され、それ以外のパケットは、送信(中継）される。

2.2　分割パケットに対する動作

IDP のデータが分割されたパケット(IP フラグメントパケット、TCP パケット)に対する動作を図２に示す。

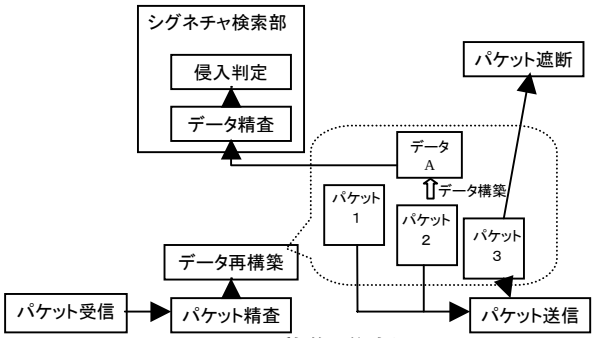

図２　IDP の動作(分割パケット)

パケットを受信した IDP は、分割されたパケット、この場合、パケット１、２、３からデータＡを再構築し、シグネチャ検索部へ渡し、侵入の判定を行う。このとき、データＡを再構築したパケットについては、一部、図の場合は、パケット３、を残してシグネチャ検索部へのデータＡの通知と同時にネットワークへ送信(中継)する。その後、データＡが侵入データであると判定された場合は、装置に保持したパケット３を廃棄(遮断)することにより、侵入の防御を行う。このような処理を行うことで、装置内のリソースの有効活用を行う。

３．1G ネットワーク対応の高速化

一般的に中継機器の高速化手法としては、ネットワークプロセッサに代表されるような並列処理とパイプライン処理が効果が高い手法として採用されている。しかし、1G ネットワークの場合、最大で毎秒 100 万パケット以上の処理能力が要求されるため、ネットワークプロセッサよりもさらにきめの細かいパイプライン処理を実現可能な、H/W(今回の試作は、FPGA と CAM の組み合わせ。将来的には、ASIC 化を想定。)実装を我々は採用した。

我々の試作した装置では、２章で記述した IDP の動作を

① パケット受信／パケット精査
② データ再構築
③ シグネチャ検索

の３つの部分に分け、それぞれをパイプライン

A Study of High Speed H/W Based IDP
Toru INADA, Kiyofumi TAKEUCHI,Kiyohiko SUZUKI, Atsushi ONUKI,Shinobu USHIROZAWA
Information Technology R&D Center, Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura, 247-8501 Japan

動作させるとともに、個々の処理部分の内部でもさらに細かいパイプライン動作を実現することにより、1G ネットワークに対応する高速処理を実現している。

４．H/W 構成

試作した IDP 装置の H/W 構成を図３に示す。

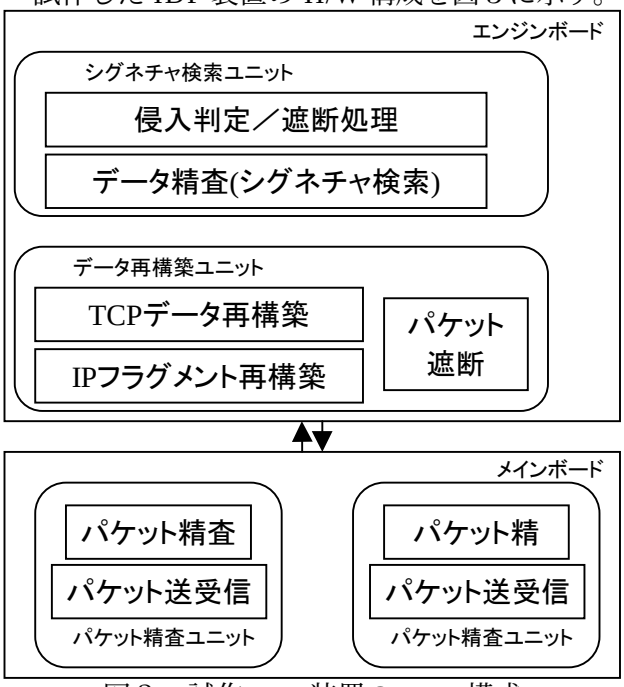

図３　試作 IDP 装置の H/W 構成

試作した IDP 装置は、大きくメインボードとエンジンボードに分割されている。メインボードは、受信ポートに対応したパケット精査ユニットから構成され、エンジンボードは、データ再構築ユニットとシグネチャ検索ユニットから構成される。この他に装置全体を管理する CPU ボードが存在するが、スペースの都合で割愛している。

メインボードのパケット精査ユニットは、主に受信パケットのパケットヘッダの精査を実施する。パケットヘッダの精査は、IDP の他にも VPN などでも必須機能であるため、拡張性も考慮し、メインボード機能とした。

エンジンボードのデータ再構築ユニットでは、IP フラグメントパケットのリアセンブル処理、TCP データの再構築処理、およびパケットの遮断処理を実施する。シグネチャ検索ユニットでは、シグネチャの検索および侵入判定処理を行い、侵入を検知した場合は、データ再構築ユニットに遮断通知を発行し、侵入データを廃棄する。

なお、それぞれのユニットは、FPGA および CAM から構成されている。

５．課題

IDP を H/W 実装するための検討の結果、図３の３つのユニットのうち、データ再構築ユニットの TCP データ再構築部分とシグネチャ検索ユニットのデータ精査部分において、以下に示す２つの課題が明確になった。

① TCP 再構築用バッファリソースの低減
② シグネチャ検索処理部分の高速化

我々は、これらの課題を以下に示す方式を採用することで解決した。

5.1 バッファリソースの低減

TCP 再構築処理では、多くのセッションを同時に扱うため、TCP 組み立て用に膨大なバッファリソースをが必要となる。今回の試作では、有限のバッファリソースを効率よく使用するため、TCP データ再構築処理において使用メモリ容量を削減する方式を採用した。

我々の採用した方式は、精査データをさらに分割してシグネチャ検索ユニットへ通知することによりバッファリソースの低減を実現する方式で、その有効性を今回の試作で確認した。

5.2 シグネチャ検索処理の高速化

シグネチャ検索において、大きなウェートを占める処理として、文字データの整形処理があげられる。文字データの整形処理とは、不要なバックスペースなどを削除する処理で、通常の文字列処理と同様にバイト単位で処理を行うと、1G の速度に対応することが困難である。今回の試作では、文字データの整形処理を４バイト(ワード)単位で行う方式を採用し、1G の速度に対応することに成功した。

６．まとめ

1G ネットワーク対応の H/W IDP の実現方式および課題とその解決策についての整理を実施し、試作装置を作成した。

なお、今回の試作は、性能を最優先するために、非常に高価な部品を使用しており、今後、原価の低減や、F/W との連携・処理分担によるより実用度の高い装置として、今回の成果を流用していくことが今後の課題である。

[参考文献]

[1] Snort: The Open Source Network Intrusion Detection System, http://www.snort.org .
[2] Norimitsu NAGASHIMA : “A study of packet reassembly method in IntrusionDetection and Prevention System”,APSITT 2003, pp.133-138, Nor.2003.
[3] 鈴木 諭司・西山 怜 他 : “CAM を用いた不正検知型侵入検知システム実装手法の提案,” 情報処理学会第 65 回全国大会, Vol.3, pp.555-556, Mar.2003.