VPN(Virtual Private Network)システム構成技術の検討･装置アーキテクチャ

4G－1　後沢　忍　時庭　康久　稲田　徹
三菱電機（株）情報技術総合研究所

1．はじめに

ネットワークのセキュリティ確保は複数の機器（技術）を組み合わせて実現するのが最近の主流になってきている。具体的には、アクセス制御を行うファイアウォール、侵入検知を行う IDS(Intrusion Detection System)、情報の秘匿や改ざん防止を行うVPN(Virtual Private Network)によって実現されている。各機器の性質上、それぞれが持っている情報を共有することによって効果的なセキュリティ確保が可能である。例えば、IDS の検知情報に基づいて VPN のポリシーを変更する等が考えられる。一方これらの機器は専業のベンダが独立に発展させてきた経緯があり、3者の連携という観点では立ち遅れているのが現状である。本稿では、VPN 装置に着目し IDS 等との連携を密にするための装置アーキテクチャについて述べる。

2．ネットワークセキュリティシステムの現状分析

複数機器によるネットワークセキュリティの実現例を図1に示す。図では外部ネットワークを脅威の対象とみなし、内部ネットワークを防御するために両者の接続点に複数のセキュリティ機器を配置している。そして、これらの機器は、防御を担当する管理者によって運用されている。

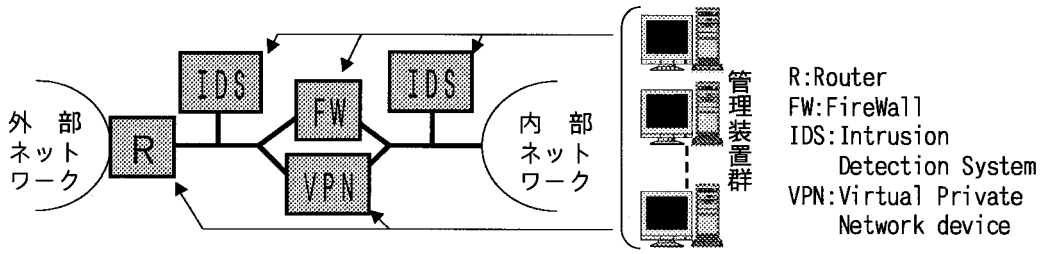

図1．ネットワークセキュリティの実施例

外部との接続はルータとその内側にファイアウォールという構成が一般的である。VPN 装置の位置はセキュリティポリシーによって、ファイアウォールの外側若しくは内側に直列に設置するケースもあるが、本構成例ではファイアウォールと並列に置いている。この場合、VPN(IPSEC)フレームはファイアウォールで一律廃棄するようなポリシーに設定しておく。ファイアウォールは VPN フレームを除く全てのフレームのアクセス制御を担当し、VPN 装置は VPN 対象フレームの暗復号，相手認証，改ざんチェックなどを担当する。IDS もポリシーによって配置が変わるが、本例では VPN 装置の両側に置いている。内側の IDS は VPN を経由した攻撃への防御を意図したものである。そしてこれらの機器群は、一般的にそれぞれ専用の管理装置によってリモート管理／運用がなされている。

A Study of VPN (Virtual Private Network) Device Architecture

Shinobu USHIROZAWA , Yasuhisa TOKINIWA and Toru INADA
Information Technology R&D Center, Mitsubishi Electric Corporation , 5-1-1 Ofuna, Kamakura, 247-8501 JAPAN　(E-mail) ussy@isl.melco.co.jp

３．装置アーキテクチャの提案

図１の各機器の運用を考えた場合、各機器固有の設定情報（ファイアウォールのアクセスリスト、VPN装置のSPD(Security Policy Database)、IDSのシグネチャ）は対象フレームのアドレスやポート番号等が基本となっており重複しているものが多い。各機器に設定するネットワークトポロジ情報や収集するログ情報もほとんどが同じである。従って、各機器の設定／運用情報を共通化するメリットは大きい。また最近では、IDSの検知情報を基にルータのフィルタ設定をネットワーク経由で変更するシステムもあるが、攻撃対象のネットワークを介して制御情報をやり取りすることになるため、信頼性に問題がある。上記を鑑み、複数の機器を１つの装置内でバス結合するアーキテクチャを提案する（図２）。

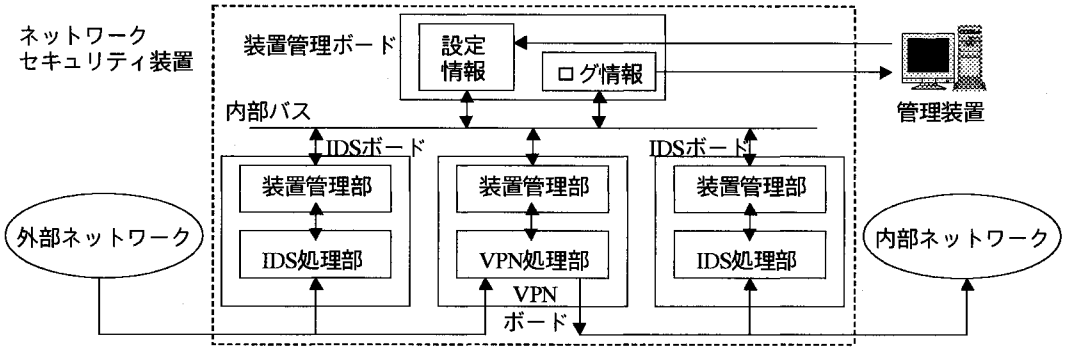

図２．装置アーキテクチャ

図２はVPNとIDS機能を１つのネットワークセキュリティ装置で実現する場合のアーキテクチャの例であり、VPNボード，内外用IDSボード，装置管理ボードが内部バスによって接続されている。各ボード間の制御情報等のやり取りは内部バスを経由して行われる。外部ネットワークからのフレームはVPNボードと外側IDSボードで受信され、それぞれの処理が行われる。VPN処理部ではIPSECの復号処理を行い、平文フレームを内部ネットワークに送信する。このフレームは内側のIDSボードでも受信される。内外IDSボードでは攻撃検知処理を行い、攻撃を検知した場合にはVPNボードと装置管理ボードに対して内部バスを介して通知を行う。攻撃検知通知を受けたVPNボードは、SPDの変更等を行い該当するトラヒックを遮断する。装置管理ボードはリモートにある管理装置の指示を受けて、各ボード上の装置管理部と内部バスを介して設定情報やログ情報のやり取りを行う。

４．まとめと今後の課題

VPNとIDS等の連携と効率的な運用管理を実現するための装置アーキテクチャを示した。現在、本アーキテクチャに基づく装置を試作して評価を行っている。内部バスとしてPCIバスを採用しており、IDSボードだけではなく、市販の汎用ボードの拡張も可能な構成となっている。今後は、PKIボード等との連携も含め、セキュリティ装置としての機能拡張を行っていく予定である。

参考文献

[1]後沢他“ＶＰＮ構築技術の検討・技術動向の分析”，情処６１回全国大会，2000
[2]永嶋他“ＶＰＮ構築技術の検討・暗号処理の高速化”，情処６１回全国大会，2000