2.2. 状況認識のためのセキュリティアプライアンス

組織におけるセキュリティインシデントの発生状況を認識することは、組織の情報セキュリティ対策を計画するにあたって大変重要なことです。現実世界で事故や犯罪の起こりやすい地域に監視カメラや検問を設置するように、ネットワーク上にもそのような機能がなければ、状況を認識することができず、「犯人」を捕らえたり、リスク分析に基づく次の一手を打ったりすることができません。そのような機能の技術的な解として、さまざまなセキュリティアプライアンスが開発されています。これらの機器は、通常セキュリティの強化によるインシデントの予防という側面が注目されますが、発生時の緊急対応や調査のための証拠の収集、また逆に外部で発生したインシデントに対する身の潔白を示すために重要な役割を果たすこともあります。

今回はセキュリティインシデントの状況認識のためのセキュリティアプライアンスとして、ファイアウォール（FW)、侵入検知システム（IDS)、侵入防止システム（IPS)、統合セキュリティアプライアンスとしての UTM、および Web アプリケーションファイアウォール（WAF）について取り上げました。また、セキュリティアプライアンスによって対策される具体的な事例として P2P ファイル共有の問題について取り上げています。

FW はネットワーク型 FW とホスト型 FW に大別されます。ネットワーク型 FW は、パケット単位、セッション・アプリケーション単位でネットワークトラフィックを制御するもので、設置場所の観点から主として、組織とインターネットの接続点に置かれます。一方ホスト型 FW は、主として PC などのエンドポイントへ、アンチウィルスソフトウェアと共に導入され、PC をインターネットワームなどの攻撃から保護しています。

IDS も FW と同様に、ネットワーク型 IDS（NIDS）およびホスト型 IDS（HIDS）にわけられ、また検知方式によって Abuse（誤用）検知型（Signature 型）と Anomaly（異常）検知型に大別されます。例えば、Abuse 型の NIDS はネットワーク上に流れる通信パケットを捕獲し、プリプロセッサ部で前処理を行い、検知部へ入力として渡します。そして検知部では、Signature データベースと呼ばれる攻撃のパターンを集めたデータベースを利用し、攻撃パターンに一致したものを検知結果として出力します。この出力されたメッセージはアラート部でログとして記録され、更にメールなどで管理者へ通知されます。しかし NIDS によって検知された攻撃は、成功したか失敗したかはわからないという欠点があります。当然その攻撃先で、その攻撃に対する防御策が採られていれば攻撃は成功しないことになります。よって NIDS は攻撃の予兆を捕らえるためのツールと言えます。代表的な NIDS としてオープンソースの Snort が知られています。

一方 HIDS は、主としてサーバホストに導入され、プロセスの異常な動作やファイルの改ざんなどを検知することができます。また受信したパケットについて NIDS と同様に処理してネットワークから導入ホストへの攻撃そのものを検知することができます。代表的な HIDS として tripwire が知られています。HIDS は、NIDS と異なり、検知結果に基づいた次のアクションとの連携が同一ホスト内であるため容易にできるという利点があります。しかし導入するホスト自身のリソースに余裕がなければ HIDS を導入するのは難しい場合もあります。この場合、NIDS をスイッチとサーバの間に入れて監視し、攻撃の予兆を検知する方式を採用せざるを得ないことになります。

IPS は IDS 部分と動的 FW 部分から成り、IDS 部分で検知した結果を基に攻撃元 IP アドレスからの通信を動的ブロックするアプライアンスです。IDS はネットワークやホストを監視するだけで、基本的に保護や防御はしませんから、2003 年に米国で発表されたレポート[1] の影響もあって、検知して攻撃を遮断できる次のセキュリティアプライアンスとしての IPS が注目を浴びました。IPS もネットワーク型 IPS（NIPS）とホスト型 IPS（HIPS）があります。NIPS はネットワーク上

[1] http://www.sans.org/reading_room/whitepapers/detection/1028.php

の通信を監視、攻撃と見なした通信をブロックします。NIDS と NIPS が大きく異なるのは、NIPS の IDS 部分の性能が NIDS 以上に求められることです。ネットワーク帯域にも耐え得る必要があり、監視する通信を選び、確実に検知できるものに限ってブロックする必要があります。誤検知があると遮断するべきでない通信まで遮断してしまうことになるからです。

このように様々な種類のセキュリティアプライアンスが出てきたため、これらを個別に導入する場合の導入や管理コストが問題になってきました。このため、これらの機能を単一の筐体にまとめた、統合セキュリティアプライアンスが開発されました。現在このような機能や機器は UTM（Unified Threat Management: 統合脅威管理）と呼ばれています。単一の機器で多数の機能を有し、また操作が統一されているため、導入や管理コストが低いという利点があります。その一方で、全体としての処理性能や各機能の設定自由度が低かったり、耐故障性に問題があったりする場合もあります。大規模な組織には性能が見合わない場合もあるため、導入時には注意が必要です。

WAF はその名の通り、Web アプリケーションに対する攻撃を防ぎます。近年 Web を媒体としたサービスが非常に普及しており、またこれを対象とした攻撃も激しさを増しています。この際に問題になるのが、脆弱性が発見されたにもかかわらず、開発者の不在や改修コストなど様々な理由により修正が不可能な「レガシー」なアプリケーションです。WAF は、これを解決するための「外堀」として機能します。WAF は一般にウェブサービスを提供するサーバの手前に設置することにより、クライアントからの要求やサーバからの応答内容を検査し、必要なら危険な要求や応答内容を安全なものに変換することで、レガシーなアプリケーションを修正することなく防御を強化することができます。今回の報告ではネットワーク型についてだけ紹介していますが、サーバに追加で導入する形のソフトウェアもあります。

続いて、セキュリティアプライアンスによって対策される具体的な事例として P2P ファイル共有について取り上げています。「P2P」とは「Peer to Peer」のことで、元々は計算機ネットワークの形態の一つを指す言葉です。参加ホストに明確なサーバ・クライアントの区別が無く、両方の機能を兼ね備えた「Peer」同士によって構築されます。また、この言葉は P2P モデルを応用したソフトウェアそのものを指すこともあります。応用例としてはファイル共有がもっとも有名ですが、それ以外にも音声通信やコンテンツ配信などで利用されています。

P2P 自体は単なる通信技術の一つですが、応用としてのファイル交換ネットワークが世界的に問題視されている現状があります。主な問題点は、違法に複製されたソフトウェアや動画の共有と、ウイルスなどに起因する情報漏洩です。また、利用者による P2P ソフトウェアの多用のためネットワーク帯域が圧迫され、通常利用に差し支えるという問題が起こる場合もあります。このため、P2P ファイル共有ソフトウェアを組織として制限・遮断したいという要求があります。しかし、P2P ではポート番号を必ずしも固定する必要がないため、単純な静的ポート遮断では対応できず、ネットワーク側で対策するにはより高機能のセキュリティアプライアンスの導入が必要となります。また、技術の悪用が問題であるため、規則や広報など人的な手段による規制も重要です。言語の問題のみならず、国によって著作権に対する意識が異なるなどの問題もあり、留学生や外国人研究者への対応には注意が必要です。

セキュリティアプライアンスの導入には、管理的な側面から、コストの問題や運用ポリシーの問題があります。導入時におけるコスト、および導入した後の維持管理のコストが挙げられるでしょう。また運用ポリシーを決めておかないと組織の構成員から「盗聴」や「検閲」ではないかと誤解を受けることがあります。またアプライアンスより生成されるログには個人情報を多く含んでいる可能性があるため、その取り扱いやアクセス権の管理などの問題が生じてきます。またセキュリティアプライアンスは廉価なものではありませんし、設置または配置される場所によって得手不得手があるため、導入場所を間違えると大きな損失を抱えることになります。通常 NIDS/NIPS や UTM などのネットワーク型セキュリティアプライアンスは、対外ルータの近傍へ設置されますし、検疫システムは L2 スイッチや統合認証システムとの連携が重要になりますので、

PC などのエンドポイント近傍に設置されます。またインライン型の IDS/IPS などは、ルータやスイッチとサーバの間に設置されます。更に導入時のコストを下げるための方策として、導入時期を慎重に選ぶ必要があると思われます。すなわち、セキュリティアプライアンスを導入しやすいネットワークがあり、それは主要なネットワークトラフィックを容易に監視が可能であることや IDS 用のミラーポートやネットワークタップ装置が置きやすいとか、また UTM などのインライン型 IDS/IPS がそのトラフィックの速度帯域に耐えられることなどが要求されます。したがってネットワークの設計段階で、上記の導入しやすいネットワークの条件を考慮すれば良いということになります。すると組織内のネットワーク施設の更新時期が適当であり、更新計画にセキュリティアプライアンスの導入を前提にして、ネットワーク設計を行う必要があるということになります。

またセキュリティアプライアンスは一般に大量のログを生成します。そしてそのログには大量の個人情報が含まれる可能性が高いことから、その管理については慎重に行われる必要があります。つまり管理ポリシーが必要になります。ログの管理ポリシーとしては、安全な保存場所の確保、アクセス権限（閲覧）規定、統計解析作業のためのリソース確保等を考慮する必要があります。

以上、「状況認識のためのセキュリティアプライアンス」と題して、ファイアウォール（FW）、侵入検知・防止システム（IDS/IPS）、Web アプリケーションファイアーウォール（WAF）、P2P アプリケーションの制御、セキュリティアプライアンス導入時のコストやネットワーク設計について検討しました。また付録として、これらセキュリティアプライアンスの導入・運用現況について 10 機関についてアンケート調査を行った結果を添付しておりますのでご覧ください。