ＷＡＦ読本補足資料

Web Application Firewall(WAF)の導入に向けた検討項目

～WAF の製品・サービスの種類と選択基準について～

2019 年 3 月

独立行政法人情報処理推進機構
セキュリティセンター

目次

はじめに

ウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保護するセキュリティ対策の一つとして、Web Application Firewall（WAF）の導入が挙げられます。独立行政法人情報処理推進機構（IPA）では、WAF の理解を手助けする情報として、「WAF 読本」の公開を行ってきました。

「WAF 読本」を参照された方が実際に WAF の導入を検討される際、選択可能な導入方法が 3 つ存在します。この 3 つの製品やサービスから、組織に応じた WAF を選択する際にどのような観点で検討すべきかを解説した補助資料として本書を作成しました。

本書が WAF の導入を検討する際の一助となれば幸いです。

本書の位置づけ

本書は、「WAF 読本」を参照された方で、WAF の導入を検討されている組織やすでに導入済みの組織での運用を見直す場合を対象とした資料です。

WAF を導入することで、ウェブサイトが被害を受ける可能性を低減することができますが、攻撃の検知・遮断や、ウェブサイトの利用者に悪影響を及ぼさないようにするには、適切な設定や定期的なメンテナンスが必要となります。

本書では実際に WAF を導入するにあたり、正しく WAF を運用し続けるためにどのような観点で製品やサービスを検討すべきかについて解説しています。

本書では、第 1 章で 3 種類の製品・サービスとそれぞれの特徴について解説し、第 2 章では具体的な選択の観点として 3 つの観点を解説しています。

ウェブサイトの脆弱性と WAF の有効性

ウェブサイトにおける情報漏洩等の被害報告に終わりはなく、連日のように被害が報告されています。これらの被害では、ウェブサイトで使用しているソフトウェアの脆弱性を狙われたことで被害が生じたとの報告があります。また、利用者が多いソフトウェアに深刻な脆弱性が報告された場合、脆弱性を悪用した攻撃が発生するまでの期間が極めて短いことが確認されています。

2017 年に報告された Apache Struts2 の脆弱性(S2-045)では、日本時間の 3 月 6 日に脆弱性が報告されてから、PoC(Proof of Concept)が確認されるまで 12 時間程度であったとされており、国内で実際に被害が発生したのは、3 月 8 日の 17 時頃であったことが報告されています。

(日時は日本時間)

日付	時間	事象
2017年3月6日	19時ごろ	Apacheより、S2-045に関する情報が公開される。
2017年3月7日	午前	中国のウェブサイトでPoCが公開される。
2017年3月7日	13時ごろ	中国国内で攻撃を検知。
2017年3月7日	17時ごろ	日本国内で攻撃を検知。
2017年3月7日	21時ごろ	Apacheより、修正バージョンが公開される。
3月7日中にWAFベンダからシグネチャがリリースされた		
2017年3月8日	5時ごろ	保険特約料支払いサイトへの攻撃が発生。
2017年3月8日	11時ごろ	JPCERT/CCより早期警戒情報を公開。
2017年3月8日	14時ごろ	IPAより注意喚起情報を公開。
2017年3月8日	17時ごろ	都税支払いサイトへの攻撃が発生。
2017年3月8日	21時ごろ	Apacheより修正バージョンのアナウンスメール送信。
2017年3月9日	午前	JPCERT/CCが注意喚起を公表。
2017年3月9日	18:00	GMO-PGがS2-045を把握。対象サイトの調査を開始。
2017年3月9日	20:00	GMO-PGにて対象となるシステムの洗い出しが完了。
2017年3月10日	0:30	GMO-PGにて保険特約料支払いサイトと都税支払いサイトへの不正アクセス発生を確認。

図 S2-045 における発生事象の時系列

このように、脆弱性が短期間のうちに悪用されてしまえば、ウェブサイトの運営者がアップデートによる脆弱性の解消を行う間もなく攻撃にさらされてしまいます。しかし、上記の脆弱性の際、複数の WAF ベンダからは 3 月 7 日中に攻撃を遮断することができるシグネチャをリリースしていたことが確認されています。

ウェブサーバで使用されているソフトウェアを更新が公開された当日中に行うことや、ソフトウェアの脆弱性の修正を短期間で実施することは困難であり、急速に拡大する脆弱性の悪用に対応することができません。しかし、WAF を導入し、その運用が適切であればこのような場合において、被害を水際で食い止められる可能性があります。

WAF が検知できる攻撃

WAF はウェブサイトを狙った攻撃から、ウェブサイトを保護するために有効ですが、すべての攻撃から保護できるものではありません。

一般的な WAF では、攻撃の監視対象としているプロトコルは HTTP と HTTPS のみであり、それ以外のプロトコルに対しては監視対象としていません。このため、SSH を使用したサーバに対する不正アクセスや FTP を使用したファイルアップロードの不正な試み等を検知することはできません。

また、WAF が検知可能な攻撃は WAF に設定されたシグネチャによって定義されています。そのため、攻撃に対応したシグネチャがベンダから提供されるか、運用者が独自にシグネチャを開発するまで、新たな攻撃を検知することができません。

1. WAF の製品・サービスについて

本章では、どのような製品やサービスが存在するか紹介し、各々の特徴について解説いたします。

WAF には、ネットワーク機器として独立した製品である「アプライアンス型」とサーバにソフトウェアを導入する「ソフトウェア型」、ウェブサイト運営者のウェブサーバやネットワーク環境を変更することなく WAF を導入できる「クラウドサービス型(以降はサービス型と記載)」の 3 種類に大別されます。

小規模な組織や WAF の運用に必要な人員を用意できない場合に「サービス型」の WAF を導入する企業が見られます。また、1990 年以降では、中小企業でレンタルサーバを使用して、企業のウェブサイトを構築することが多くなっていますが、が WAF を標準提供しているレンタルサーバ事業者も増えており、物理的なネットワークの変更やソフトウェアの追加が出来ない組織にとって、WAF を利用する有効な選択肢となっております。

3 つの製品やサービスが存在しますが、各組織のネットワーク環境や運営方針に合わせた WAF を選択できなければ WAF を適切に運用できず、検知漏れ等の問題やウェブサイト運用への障害が生じます。

以下の表にてそれぞれの製品・サービスの特徴を解説します。

表 1-1 製品・サービスの種類

製品・サービス	特徴
アプライアンス型	各組織のネットワーク内に専用の機器として WAF を設置し、ウェブサーバへの通信を WAF に通過させることで検査する 仮想基盤向けの仮想アプライアンスとして提供される場合もある
ソフトウェア型	各組織が運営するウェブサイトのウェブサーバに、ソフトウェアとして WAF をインストールし、ウェブサーバへの通信内容を検査する
サービス型	組織外に存在する WAF サービス提供者のサービスサーバを経由することで検査を行い、組織内のウェブサーバへ通信を中継する 組織内のウェブサーバにエージェントとなるソフトウェアをインストールし、組織外の WAF ベンダのサービスサーバと連携して検査する方式も存在する

各製品・サービスのメリットとデメリット

各製品やサービスにおけるメリットとデメリットをまとめると下記のようになります。

表 1-2 各製品・サービスごとのメリットとデメリット

	各製品・サービスのメリット	各製品・サービスのデメリット
アプライアンス型	■運用負荷 ・独立した機器を使用するためウェブサーバに負担をかけることはない ■設定の自由度 ・ウェブサイトへのアクセス数に応じて導入機器の性能を選択できる ・ウェブサイトやネットワーク環境に合わせ、検知条件や検査対象の通信を設定できる	■コスト ・アプライアンス製品は一般的に調達費用が高価 ■運用負荷 ・ネットワーク環境の構成変更が必要 ・導入時の機器設定や導入後の運用を各組織にて実施する必要がある ・運用開始後もアップデートや検知設定の見直しが必要 ・検知した通信が攻撃を目的としていたか、WAF 運用者による確認が必要な場合がある
ソフトウェア型	■コスト ・専用機器が必要ないためアプライアンス型と比較して調達費用が安価 ■運用開始までのハードル ・ネットワーク環境の構成変更が不要 ■設定の自由度 ・検査対象が限定されており、他のサーバや業務端末の通信に影響しない ・ウェブサイトやネットワーク環境に合わせ、検知条件や検査対象の通信を設定できる	■運用負荷 ・運用開始後もアップデートや検知設定の見直しが必要 ・検知した通信が攻撃を目的としていたか、WAF 運用者による確認が必要な場合がある ・ウェブサーバに同居する形ため、サーバの処理性能に悪影響を与える可能性がある
サービス型	■コスト ・製品の調達が不要なため、一般的には他の製品種類に比べ安価。また、ウェブサイトで発生する通信量やサービス内容によって利用料を変更できる ■運用開始までのハードル ・アプライアンス型やソフトウェア型よりも導入までの期間が短い ・組織のネットワーク環境によらずに導入が可能 ■設定の自由度 ・ウェブサイト運営者が WAF のシグネチャやソフトウェアのアップデート等のメンテナンスを行う必要がない	■コスト ・ウェブサーバや監視対象の URL の数、通信量が多い場合、他の製品種類に比べ、コストが高くなる場合がある。 ■運用負荷 ・WAF の調整可能な項目は、WAF サービスの提供者が提供するサービスに依存するため、ウェブサイト運営者の意向に沿った設定が出来ない場合がある ・WAF サービス提供者のネットワーク障害等の影響を受ける場合がある

2. 製品・サービスの選択基準

本章では、1 章で解説した 3 つの製品やサービスについて、選択基準となる観点を 3 つ例示します。本章の内容を元に、各組織の実情にあった製品やサービスを選択するようにしてください。

2.1. 3 つの選択基準

WAF の導入を検討するうえで検討が必要な選択の基準として、以下の 3 点が挙げられます。

① 運用開始までの期間と導入に必要な費用
② WAF の設定自由度
③ 導入後の運用業務

①については、導入決定後から導入が完了するまでの期間と導入に際し必要となる費用を意味しています。

ウェブサイトへの被害が発生する前に事前対応として導入する場合は、導入完了までの時間を比較的に長くとることもできます。しかし、実際に被害が発生したため、それ以上の被害を防止する事後対応として導入する場合は、可能な限り短期間に導入したい場合が多いと考えられます。

費用については、可能な限り少ないことが望ましいですが、製品・サービスの種類や検査対象の通信量、必要とする機能等により初期費用が変動するため、製品を選択する段階で確認が必要となります。

[2.2.1. 運用開始までの期間と導入に必要な費用に対する検討]

②については、導入した WAF をどこまで自由に設定できるかという観点を指します。例えば、WAF がどのサーバへの通信を監視対象にするか、どのシグネチャを有効あるいは無効にするか等の設定ができるかという観点です。シグネチャの選択については、保護したいウェブサイトが独自のサービスを提供している等で、誤検知が頻発する場合は検知対象の調整が必要になります。

[2.2.2. ＷＡＦの設定自由度に対する検討]

③については、WAF の導入後に WAF の管理者にどれだけの業務負担が生じるかという観点です。先にも述べた通り、WAF の種類によっては導入後にシグネチャのアップデートや有効なシグネチャの調整等が必要になります。

[2.2.3. 導入後の運用業務に対する検討]

なお、WAF の運用に関しては専門の企業に運用をアウトソースすることも可能です。何らかの事情から「アプライアンス型」や「ソフトウェア型」を選択せざるを得ず、WAF を運用する担当者を組織内で用意できない場合は、アウトソーシングを検討するとよいでしょう。

[2.3.WAF 運用のアウトソーシング]

以上の 3 つの基準について検討し、各組織において基準が満たされる製品やサービスを選択することが必要です。

2.2. 各選択基準に対する検討

次に 3 つの選択基準の内容を具体的に解説します。

2.2.1. 運用開始までの期間と導入に必要な費用に対する検討

WAF の運用開始までに発生する費用や検討項目として、以下のような項目が考えられます。

1. WAF の初期費用
2. WAF の導入に向けた環境整備
3. WAF の運用開始までの期間
4. WAF の運用コスト

1 は WAF の導入に際し発生する費用です。各製品やサービスによって発生する費用が異なります。

「サービス型」の場合、購入費用に該当する物として初期契約の料金が発生します。この金額は契約内容によって異なる場合もあるため、一概に費用の高低を論じることができません。他の 2 つについては、一般的には物理的な機器の調達が必要となる「アプライアンス型」が高くなる傾向があります。続いて、ソフトウェアの調達が必要な「ソフトウェア型」となると考えられます。

2 は WAF の導入に向け行う作業です。WAF を導入するに際し、組織内の物理的なネットワーク構成の変更や、論理的なルーティング設定の見直しを行う必要があります。

WAF の導入環境の調整については、組織の物理的なネットワーク構成の変更が必要な「アプライアンス型」の負担が最も大きいといえます。ただし、ウェブサーバのネットワーク切断を伴いますが、インライン設置のように導入が容易な方法もあります。次に、ウェブサーバにソフトウェアをインストールし、正常な動作環境を整える必要がある「ソフトウェア型」の負担が高いといえます。最後に、ウェブサーバへの通信をプロキシ経由にするようにネットワークの設定を変更する「サービス型」が最も負担が少ないと考えられます。

３については、上述の２とも関連する項目となります。

一般的な見解として、機器の購入や輸送・設置に加え、物理的なネットワーク構成の変更が必要となる「アプライアンス型」が最も期間を必要とし、続いてソフトウェアの調達とインストールが必要となる「ソフトウェア型」、サービスの契約とネットワーク機器の設定変更のみとなる「サービス型」が最も短い期間になると考えられています。

４については、運用開始後に発生する項目ですが、運用開始前に検討しておくべきランニングコストに該当する項目になります。

「サービス型」については、サービスの毎月の利用料が該当します。契約内容により料金は変動しますが、一般的に通信量が多いほど利用料も増加する傾向があります。

「アプライアンス型」や「ソフトウェア型」の場合、シグネチャやソフトウェアアップデート、運用サポートを受けるためのライセンス契約が発生します。

以上の観点から、WAF の導入における負担を端的に表すと下記の図のようになります。

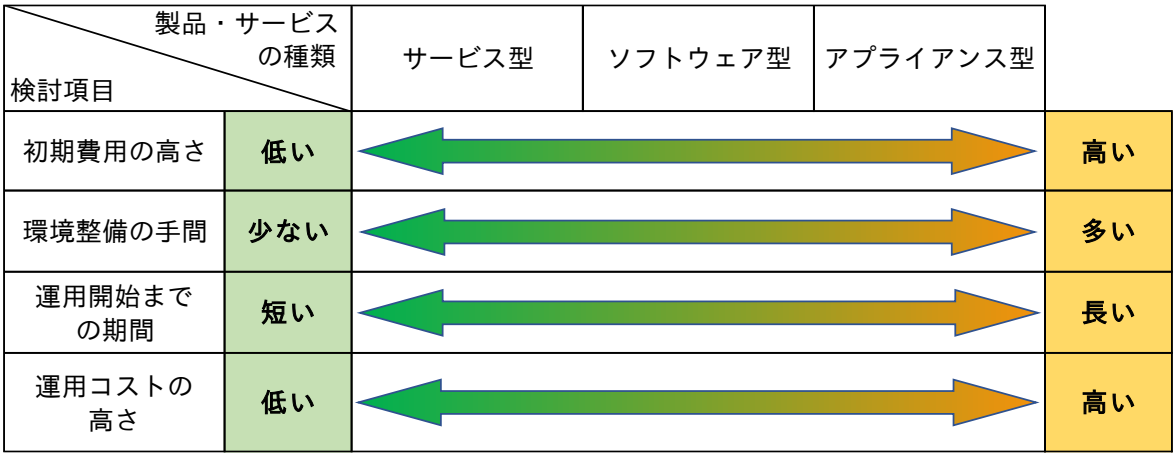

図 2-1 運用開始までの期間と導入に必要な費用の比較

上記の比較は、一般的に考えられるコストの比較であり、購入する製品の性能や利用するサービス内容、組織のネットワーク環境によって異なります。

2.2.2. WAFの設定自由度に対する検討

本節では、導入した WAF に実施できる設定の自由度から見た選択基準について解説します。WAF の設定自由度に関係する項目として、以下の項目が考えられます。

1. WAF の設置場所
2. WAF の検査・遮断対象の通信

１については、WAF をネットワーク上のどこに設置できるかという点になります。WAF の種類によって導入可能な場所が異なり、導入前に必要な準備も異なります。

「サービス型」の場合、WAF 自体が組織のネットワーク外に存在するため、ネットワークの論理的な観点で考えた場合、設置可能箇所はインターネットと組織のネットワークの境界のみとなります。そのため、組織のネットワークの物理的な変更が必要なことは少なく、論理的な設定の変更だけが必要な場合がほとんどです。

一方で「ソフトウェア型」の場合は、ソフトウェアをインストールしたサーバで検知を行うため、設置できるのは組織内のネットワークとなります。そのため、基本的にはインストールされたサーバへの通信のみが検査対象となります。「アプライアンス型」の場合も同様に、物理的に

WAF を設置することから、ネットワーク上のどこに WAF を導入するか、ウェブサーバが複数存在する場合はどのサーバへの通信を検査対象とするかによって、設置場所を検討する必要があります。「アプライアンス型」の場合、「ソフトウェア型」とは異なり、通信経路の途中に設置し攻撃の遮断を行うインライン設置や、ネットワーク機器で通信をミラーさせ通信内容の検査のみを行う設置方法等、複数の方法を選択できる場合があります。

２については、検査対象とする通信や遮断対象とする通信の自由度に関する項目です。WAF では、通信内容や通信パターン等によって攻撃とみなす通信が定められています。どの通信を検知・遮断するかについては、WAF の開発ベンダより基本となるシグネチャが提供され、新たな攻撃が発見されるたびに更新されます。

しかし、ウェブサイトで提供しているサービスによっては、正常な通信が誤って検知されることや、基本的なシグネチャだけでは検知できない攻撃が発生することがあります。このような場合、正常な通信を検知・遮断しないようにしたり、独自のシグネチャを作成し攻撃を検知できるようにしたりするといった対応が必要になります。

このように独自の検知条件を設定できるのは、製品を組織内に独自に導入できる「アプライアンス型」や「ソフトウェア型」となります。「サービス型」の場合、検知パターンは WAF サービスの提供者によって設定されており、調整可能な範囲は提供されるサービスに依存します。

以上の観点から、WAF 設定の自由度を端的に表すと下記の図のようになります。

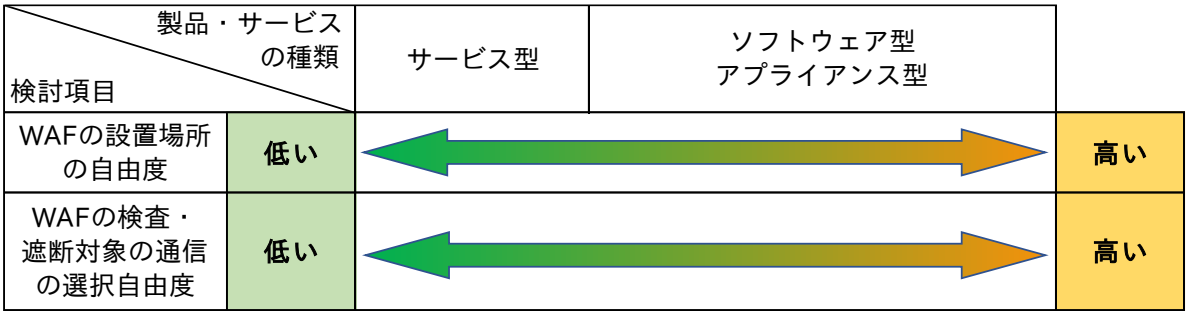

図 2-2 WAF の設定自由度の比較

2.2.3. 導入後の運用業務に対する検討

本節では、WAF 導入後において各組織に発生する運用負荷からみた選択基準について解説します。WAF 導入後に発生する負担として、以下のような項目が考えられます。

1. WAF の初期設定・動作検証
2. WAF の日常的な正常性確認
3. WAF の故障時対応
4. WAF の設定内容の見直し・修正
5. WAF の検知ログ確認

1 は WAF の導入後に実施する作業です。WAF の導入後、運営しているウェブサイトの参照や自組織のネットワーク通信に異常が生じていないか、想定した通りに攻撃を検知・遮断できているか等について確認する必要があります。

2 と 3 は、WAF の運用開始後に実施する作業です。導入した WAF が日々正常に動作しているか、正常に検知が行われているか等を確認・監視する必要があります。導入した「アプライアンス型」の WAF に物理的な障害が発生すれば 3 の故障対応を行う必要があります。また、「ソフトウェア型」の WAF が異常な動作を行っていれば、ベンダに問い合わせを行う等の対応の必要となります。一方で、「サービス型」の WAF の場合においてはこれらの対応は発生しません。「サービス型」ではサービスとして WAF を利用しているため、ハードウェアやソフトウェアの正常性監視や修理対応については、WAF サービスの提供者が行う作業となります。そのため、WAF サービスの提供者側でネットワーク障害等が生じた場合、サービス利用者側では対応ができない状況で障害の影響を受ける可能性があります。

4 は、WAF の運用中に定期的もしくはウェブの閲覧に問題が生じたときに行う作業です。「アプライアンス型」や「ソフトウェア型」では、各製品仕様の範囲内で各組織の責任のもと、検知対象等の設定を自由に行うことが出来ます。「サービス型」については、各サービスで定められた範囲で設定の変更が可能であり、WAF の設定の大部分はサービスの提供者が実施します。

5 は、誤検知や検知漏れが生じていないかの確認作業です。正規の利用者による通信が誤って検知される場合や、攻撃の見落としが発生した場合に行う必要がある作業となります。これについても「アプライアンス型」や「ソフトウェア型」では各製品仕様の範囲内で各組織の責任のもと実施可能ですが、「サービス型」については大部分をサービスの提供者が実施します。

以上のことから、WAF 導入後の運用負担を端的に表すと下記の図のようになります。

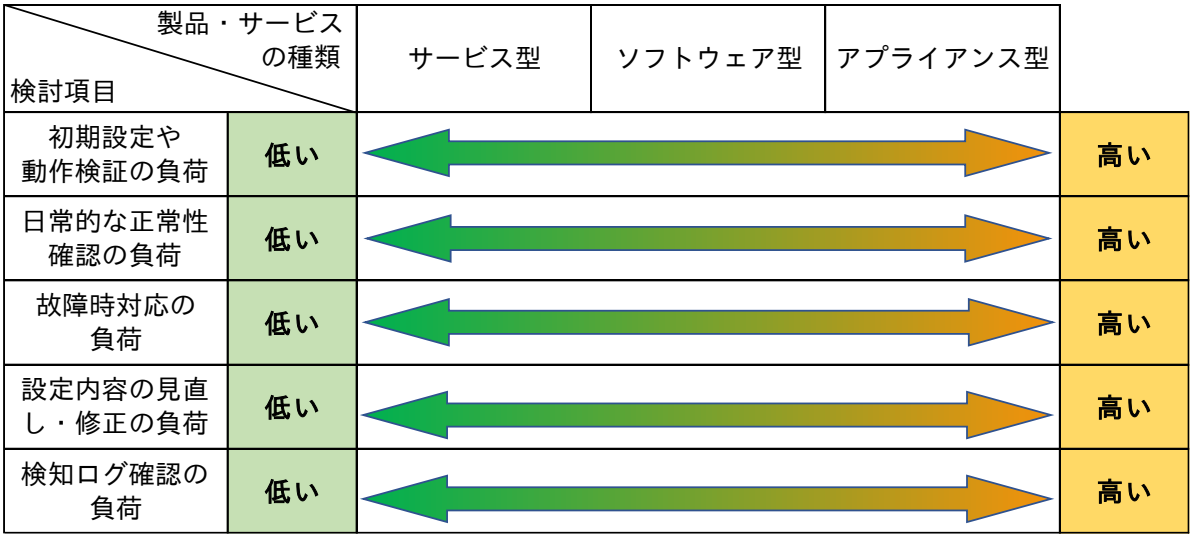

図 2-3　導入後の運用業務負荷の比較

WAF を適切に運用するためには、ネットワークやセキュリティについての知識が必要となり、ウェブサイトの性質によっては 24 時間の監視体制が必要な場合もあります。各組織内でこれら

の体制を構築することは極めて負担が大きく、組織によっては対応が困難な場合が見受けられます。

このような場合は、「サービス型」を選択し負担を減らすことや、WAF の運用をアウトソーシングする等の検討が必要です。

2.3. WAF 運用のアウトソーシング

ウェブサイトで特殊なサービスを提供している場合や、クラウドサービスを利用することが組織のポリシー上許可されない等の理由がある場合、「アプライアンス型」や「ソフトウェア型」の WAF を選択する必要がありますが、組織内で「アプライアンス型」や「ソフトウェア型」の WAF を運用・管理できる職員を用意できないことも考えられます。

このような場合は WAF の運用のアウトソーシングを検討するとよいでしょう。

WAF の正常性監視や攻撃検知時のエスカレーションといった運用の業務委託を請け負う専門の企業が存在しており、WAF に精通した職員が用意できない組織でも「アプライアンス型」や「ソフトウェア型」の WAF を運用することが可能です。

運用の委託を請け負う企業によって、管理可能な WAF が異なる場合がありますので、導入時点で運用を委託することが確定している場合は、委託先の企業がどの WAF の管理が可能かあらかじめ確認しておく必要があります。

3. 製品・サービスの選択例

本章では 2 章で解説した観点をもとに、各組織に適した WAF の製品やサービスの選択における検討項目について、基本的な項目を以下の表にまとめました。

表 3-1 各検討項目からの判断基準例

確認項目			選択項目		
			選択肢：A	選択肢：B	選択肢：C
1 運用開始までに関する選択基準					
	1	急いで導入する必要がある	至急	早急	急がない
	2	組織内で設定等を検討できる	出来ない	出来る	
	3	組織内でネットワーク構成の見直し・変更ができる	出来ない	少し	出来る
2 設定自由度に関する選択基準					
	1	検知対象を細かく設定する必要があるか	ない	ある	
	2	ウェブサイトで独特のサービスを使用しているか	ない	ある	
	3	ウェブサイトの停止が致命的な問題になるか	ならない	ならない	なる
3 運用面に関する選択基準					
	1	組織内で随時設定の見直しができるか	出来ない	出来る	
	2	検知結果の確認・調査ができるか	出来ない	出来る	
	3	ネットワークに障害が生じた際、問題の切り分けができる	出来ない	出来る	

Aの項目が多い：サービス型
Bの項目が多い：ソフトウェア型
Cの項目が多い：アプライアンス型

上記の項目では、大項目ごとに各組織が検討すべき項目をまとめています。

例えば、1-1 の項目では、導入の緊急性について確認しています。攻撃がすでに確認されており、今後の被害の発生の防止を急務とする場合は、選択肢の「至急」を選択することになり、「A」の項目の選択肢としてカウントします。

全ての項目について確認し、最終的に「A」の項目が最も多い場合は、サービス型の WAF の導入が組織として適していると判断できます。「B」の項目が多い場合はソフトウェア型が適しているという判断になります。

「B」のソフトウェア型と「C」のアプライアンス型の選択肢が共通する項目が多くあります。これは、ソフトウェア型とアプライアンス型の運用において、ウェブサイトを運営する組織に求

められる対応の多くが共通しているためです。もし、「B」と「C」の選択数が同じになってしまった場合は、導入に必要な費用等の表以外の項目から判断する必要があります。

4. WAF について誤解されていること

WAF はウェブサイトを標的とした攻撃に対して、被害の緩和に有効な対策方法です。しかし、インターネット上からのすべての攻撃を、常時防御できる万能な解決策ではありません。WAF の導入に際し、どのような攻撃に対して有効で、適切な攻撃の検知を行うためにはどのような運用が必要か、あらかじめ理解していただく必要があります。

WAF を導入する際に「WAF を導入すれば、すべての攻撃を防御できる」と誤解されている方がいます。本書の冒頭でも解説しましたが、この認識は誤りです。

WAF での検知は、シグネチャとして攻撃通信が定義されたものを検知する仕組みです。そのため、ウェブサイトで使用しているソフトウェアに脆弱性が発見されても、それに対応する新規のシグネチャが WAF に導入されるまで、検知できない場合があります。

過去に発見された脆弱性と類似していたり、カスタムアプリケーションの脆弱性であれば、既存のシグネチャで検知できる場合もありますが、新しく発見された特有の脆弱性の場合はベンダによるシグネチャの提供を待つ必要があります。

また、ベンダが公開するシグネチャを利用するためには、WAF のサポートが継続されていることが必要です。

新しい脆弱性やそれを悪用した攻撃が確認されてから、ベンダが攻撃に対応したシグネチャを作成するまでには時間がかかります。対象となる攻撃に対応したシグネチャの作成にどの程度の時間が必要かについては、各ベンダにて異なります。とあるベンダによれば、脆弱性の脅威度や脆弱性を悪用した攻撃の発生頻度を鑑みてシグネチャの作成優先度を決定しているとのことです。

しかしながら、本書冒頭で紹介した S2-045 での事例の場合のように、ベンダからシグネチャが早急に提供され、被害の防止につながる場合もあります。

IPA では、WAF による対策を脆弱性による被害の緩和策として位置付けており、ウェブサイトに脆弱性が発見された場合は、ソフトウェアの修正等の根本的解決や WAF の導入等の保険的対策の両面から検討し、対策を実施していただくことを推奨しております。

おわりに

本書では、WAF の製品やサービスごとに特徴や検討すべき項目を解説しました。

WAF を効果的に運用するためには、単に高性能な製品を購入するのではなく、それぞれの製品のメリットやデメリットを把握し、組織の状況に合わせた WAF 製品を導入し、適切な設定で運用していただくことが必要です。

本書が、組織ごとに適切な WAF の製品やサービスを評価していただく一助となれば幸いです。

Web Application Firewall(WAF)の導入に向けた検討項目 第 1 版

[発　　行] 2019 年　3 月 28 日 第 1 版

[著作・制作] 独立行政法人情報処理推進機構 セキュリティセンター

[協力　会社] 株式会社ジェイピー・セキュア

[執　筆　者] 熊谷 悠平

[協　力　者] 渡辺 貴仁　板橋 博之　田村 智和　鹿野 一人　小林 桂　堀江 亘　木村 泰介