Web Security White paper

経営層の約80%が陥る
Webセキュリティの誤認と軽視

～ Webセキュリティを成功させる3つのチェックポイントとは？～

株式会社サイバーセキュリティクラウド
Webセキュリティ事業部

サイバーセキュリティは大きく分けて２つ
対策すべきは「Webセキュリティ」

サイバーセキュリティは大きく２つに分けることができます。ひとつはマルウェアに対してPCや社内ネットワークを守るための**社内セキュリティ**。
もうひとつはソフトウェアの脆弱性やWebアプリケーション層への攻撃から外部公開サーバー守る**Webセキュリティ**です。

過去に発生したセキュリティインシデントを紐解いてみると、セキュリティ被害の多くはWeb経由であり、依然として増加傾向にあります。
その原因の一つには、「既にWebセキュリティ対策は万全である」といった誤認や、「漏洩して困るような情報は扱っていない」といった軽視に代表されるような対策の不十分さが挙げられます。

2016年個人情報漏洩インシデント事故 Top10

例えば、2016年に発生した個人情報漏洩に関するインシデントを見てみると、漏洩人数の多い上位10件のうち、7件は不正アクセスが原因でした。

No	漏洩人数	業種	原因
1	793万人	生活関連サービス業,娯楽業	ワーム・ウィルス
2	98万人	情報通信業	不正アクセス
3	81万人	電気・ガス・熱供給・水道業	紛失・置き忘れ
4	64万人	情報通信業	不正アクセス
5	58万9463人	情報通信業	不正アクセス
6	42万8138人	情報通信業	不正アクセス
7	42万1313人	卸売業、小売業	不正アクセス
8	35万人	生活関連サービス業,娯楽業	不正アクセス
9	21万9025人	卸売業、小売業	不正アクセス
１０	21万人	電気・ガス・熱供給・水道業	管理ミス

※出典：NPO日本ネットワークセキュリティ協会による調査報告書

情報セキュリティ10大脅威のうち半数以上がWebサービスへの脅威

また、IPA（独立行政法人情報処理機構）が公開している「情報セキュリティ10大脅威」によると、2017年の“組織”における情報セキュリティ10大脅威のうち、7件はWebサービスへの脅威であることがわかります。

しかしながら、こうした脅威は決して目新しいものではありません。
実は2013年以降、Webサービスへの脅威は継続的に上位にランクインしており、こうした脅威に対する企業の対策が十分でないことがわかります。

順位	脅威の内容
１位	標的型攻撃による情報流出
２位	ランサムウェアによる被害
３位	ウェブサービスからの個人情報の窃取
４位	サービス妨害攻撃によるサービスの停止
５位	内部不正による情報漏えいとそれに伴う業務停止
６位	ウェブサイトの改ざん
７位	ウェブサービスへの不正ログイン
８位	IoT機器の脆弱性の顕在化
９位	攻撃のビジネス化（アンダーグラウンドサービス）
１０位	インターネットバンキングやクレジットカード情報の不正利用

※出典： IPA（独立行政法人情報処理機構） 2017 情報セキュリティ10大脅威

経営者が認識すべき３原則

Webセキュリティ被害の増加にともない、2015年には経済産業省とIPAが『サイバーセキュリティ経営ガイドライン』を策定し、経営者に対してセキュリティ対策を推進するよう求めました。
ガイドラインの概要部分では「経営責任や法的責任が問われる可能性がある」といった強い文言が記載されており、経営者へ警鐘を鳴らしています。

経営者が認識する必要がある「３原則」※
サイバー攻撃が避けられないリスクとなっている現状において、経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である。
自社のみならず、サプライチェーンのビジネスパートナーやシステム管理等の委託先を含めたセキュリティ対策を徹底することが必要である。
平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにするなどのコミュニケーションを積極的に行うことが必要である。

※サイバーセキュリティ経営ガイドライン Ver2.0 より一部抜粋

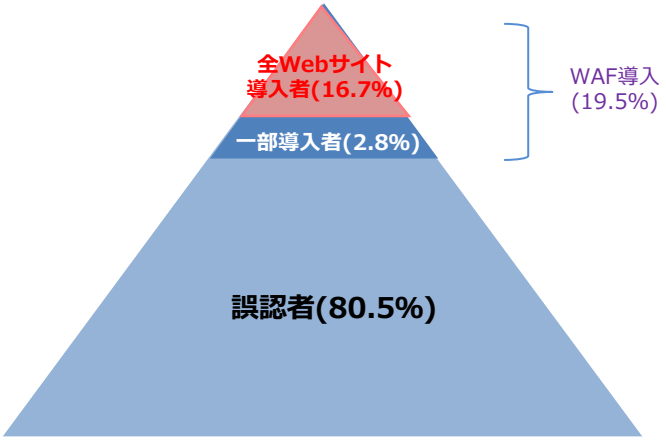
サイバー攻撃による被害は、サービス停止、売上機会の損失、ブランドイメージの棄損に留まらず、予期せぬ二次災害を起こす可能性もあります。
日本ではWebサイトのサイバー攻撃の対策漏れが重過失と認定された判決があり、米国ではサイバー攻撃から株価下落という事態を招き、経営陣を相手にした株主代表訴訟が起こされた例もあります。

こうした様々な理由から、サイバーセキュリティ対策は急務の経営課題といえます。

Webセキュリティのチェックポイント ①
「Webサイトのセキュリティは実施済だ」

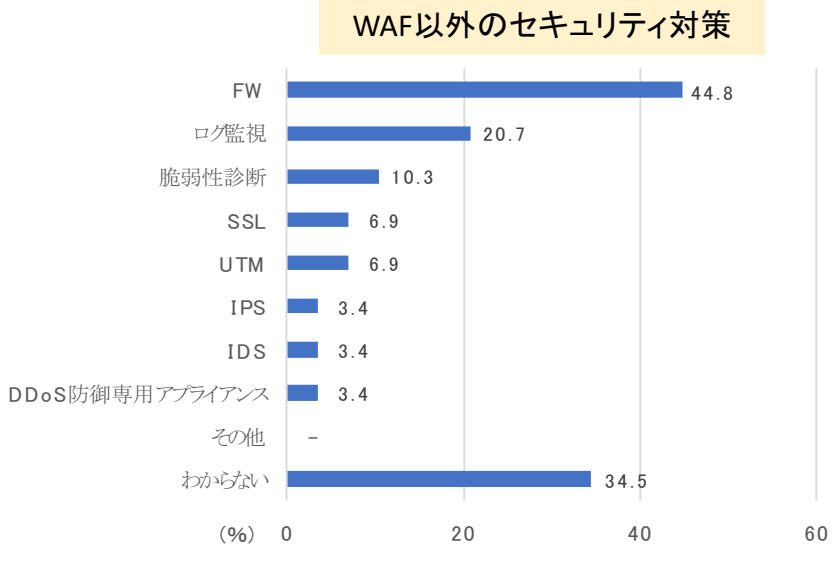
政府主導でサイバーセキュリティ対策が推し進められており、企業も既にそのリスクを十分に理解して対策しているのでは？と思うかもしれません。

しかし、市場でのアンケート調査を行ったところ、興味深い結果となりました。
Webセキュリティ対策を実施していると答えた経営層のうち、約8割※は不正アクセスの侵入口となるWebアプリケーション層への対策が実施できていない状況だったのです。
さらに、対策を実施している残りの2割に関しても、一部のWebサイトにしかセキュリティ対策を実施できていないという結果となりました。



※出典：株式会社マーケティング・アンド・アソシエイツ「セキュリティソフト浸透度調査」

セキュリティ対策を実施していると答えたものの、 Webアプリケーション層へのWAF（Web Application Firewall）対策まで認識が及んでいない経営層（誤認者 80.5%）の回答の詳細を見てみると、経営層の多くが認識しているWebセキュリティ対策はFW（ファイアウォール）やログの監視であることがわかりました。



Webセキュリティのチェックポイント ②
「委託先が対策してくれているはず」

Webシステム構築を外注した際に「ITベンダー側で適切なセキュリティ対策を施してくれているだろう」と思ってしまったことはないでしょうか？実はそう考えている企業は多く存在します。しかし、ITベンダーは要件定義されていないことは基本的に実施しません。

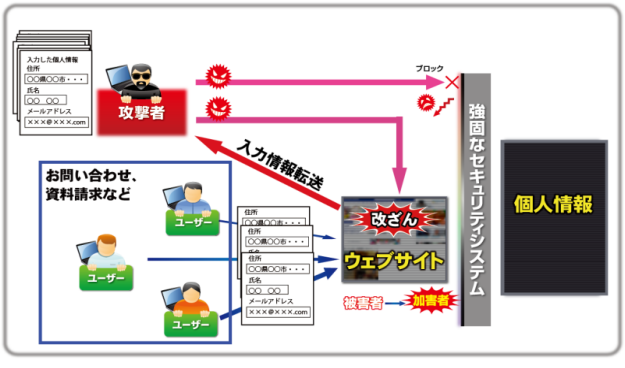
このようにお互いの認識齟齬から適切なWebセキュリティ対策が施されず、サイバー攻撃の脅威にさらされているWebサービスが数多くあります。

《関連する事件例》
化粧品などを販売する通販サイトで発覚した個人情報の漏洩について調査報告書が発表された。報告書では、サイト内で使用していた「SSI」に脆弱性があり、通販サイトの運営システムに関連して同社が複数の事実誤認をしていたことが記載されている。

クレジットカード情報：約5万件
個人情報　　：約42万件

Webセキュリティのチェックポイント ③
「個人情報は別の環境で管理しているから大丈夫」

情報システムの責任者やシステム管理会社から「個人情報は持っていないから大丈夫」「個人情報は別システムで管理しているから大丈夫」と回答されたことはありませんか？
こうした「大丈夫」という認識は、実は誤りであるケースが多くあります。



《関連する事件例》
個人情報はWebサイトとは別のデータベースで管理し、さらにセキュリティシステムを導入していた。しかし、クレジットカード情報を入力する入力フォームが改ざんされ、ユーザーが入力した情報が外部のデータベースに送信されてしまう状態だった。

メールアドレス、氏名、住所など：約75万件
メールアドレスのみ　　：約43万件

攻撃者が重視するのは「効率化」

Webサービスへのサイバー攻撃が増加するなかで、その傾向にも変化があります。昨今のサイバー攻撃の主流は「効率化」です。
標的型攻撃のように、ターゲット企業が施すキュリティ対策を一つ一つ突破するのはなく、スキャン活動を行ったり、数回攻撃して突破できない場合は次の企業へターゲットを移すなど、Webセキュリティ対策が十分でない企業を狙います。
攻撃者も時間とコストをかけて攻撃しているため、同じコストで同様の成果が出るのであれば当然セキュリティの施されていない企業を狙うのです。

こうした攻撃者の傾向から、現在ではサイバーセキュリティ対策をしていると公言することでサイバー攻撃の被害に遭うリスクを減らす事ができると考えられています。

経営陣主導でWebセキュリティを見直す

本資料では、Webセキュリティの被害状況や対策を施す際に陥りやすいポイントをご紹介しました。
サイバー攻撃はWebサービスやWebサイトを展開する企業であれば全ての企業が対象であり、サービス停止、売上機会の損失、ブランドイメージの棄損、株価下落といった様々な損害を及ぼします。
セキュリティの専任がおらず対策状況が曖昧になっているケースもありますので、企業経営のリスク排除として、経営陣主導で自社のWebセキュリティを見直すことが大切です。