導入事例

株式会社ゴルフダイジェスト・オンライン様

2000年の創業当初からデジタル技術を活用してきたゴルフダイジェスト・オンライン（GDO）にとって、セキュリティは常に身近な課題だった。MBSDのWebアプリケーション脆弱性診断に加え、コンサルティングを活用することで、自社だけでは得られない客観的な視点や知見を参考にしながら、全社的なセキュリティ戦略を推進している。

本社	東京都品川区東五反田2-10-2 東五反田スクエア8階	資本金	1,458百万円
		従業員数	1,514名（2024年12月末現在）
設立	2000年5月1日	Webサイト	http://www.golfdigest.co.jp/

導入サービス

☑ **Webアプリケーション診断**
保有するWebアプリケーションシステムに対して、疑似攻撃を行い、Webアプリケーションシステムに存在する情報漏えいや改ざんといった様々なリスクを調査するサービス

☑ **コンサルティングサービス**
20年の豊富な経験と実績があり、お客様のコストに見合ったソリューションや体制を立案

開発や事業のペースに合わせて伴走
専門家ならではのアドバイスを通して、企業全体のセキュリティ向上を支援

GDOの事業特性と課題

創業時からデジタルを前提にしてきたGDO、セキュリティもインフラの一部に

「ゴルフで世界をつなぐ」というミッションを掲げるゴルフダイジェスト・オンライン（GDO）は、2000年の創業当初からデジタル技術を活用し、ゴルフ場の予約サービスやゴルフ用品のEコマース、オンラインマガジンの提供など、ゴルフを軸に幅広いサービスを提供してきた。近年ではAI技術の進歩を踏まえ、社内の業務改善はもちろん、ユーザー一人一人の属性や志向に合わせたゴルフ場のレコメンドサービスといった形で顧客向けサービスにも活用し始めている。

長年オンラインでサービスを提供してきたGDOにとって、外部からのサイバー攻撃のリスクは常に身近なものだった。同社のセキュリティへの姿勢について、テクノロジー本部本部長の山外芳伸氏は「後付けではなく、インフラの一部としてセキュリティに取り組んでいます」と述べる。

具体的にはWebアプリケーションの定期的な診断やWebアプリケーションファイアウォール（WAF）の導入をはじめ、さまざまな側面から対策を実施してきた。昨今の攻撃の増加と巧妙化を受け、2023年7月にセキュリティ対策を推進するためにセキュリティマネジメント室を新設。セキュリティとインフラは切り離せないため、2025年7月にセキュリティとインフラを統合してサイバーセキュリティ・インフラ統括室として戦略的な対策を加速させている。

テクノロジー本部 サイバーセキュリティ・インフラ統括室室長の清水正朗氏は「かつてのように、各自のパソコンにアンチウイルスソフトを入れておけば済むような状況ではありません。社員のセキュリティ意識向上をはじめ、広い範囲をカバーしていく必要があると判断し、IT以外の部門とも連携しながらあるべき姿を目指すために立ち上げました」と、その意図を説明した。

脆弱性診断サービス導入のきっかけ

進捗に合わせ、柔軟な体制でWebアプリケーションの脆弱性診断を実施

そんなGDOがMBSDの支援を受け始めたのは2009年に遡る。

アプリケーション開発の段階から「やるべき対策をしっかり実施しよう」という意識が、現場のエンジニアからマネージャーレベルにまで浸透しており、その一環として脆弱性診断を実施することにした。

「自分たちでは安全にWebアプリケーションを作ったつもりでも、果たして大丈夫かどうか確信が持てない状況でした。そこでMBSDに脆弱性診断を依頼し、以後もシステムの大規模な入れ替えに合わせて診断をお願いしてきました」（清水氏）

評価しているポイントの一つは、見つかった問題点をまとめたレポートのわかりやすさだ。開発に携わるエンジニアにもわかりやすい内容が、推奨される対策とともに提供される。「項目ごとに『これは一体どんな意味でしょう』と確認し直す必要がないため、リリースまでのスピードアップにも寄与しています」（清水氏）

また、必ずしも計画通りに進むとは限らない開発の進捗状況やプロジェクトの予算に合わせ、機能を限定して診断を実施したり、優先順位を推奨するなどの柔軟な対応が得られるのも、他にない特徴だと感じている。「アプリケーションができあがってからでないと診断はできないと言われるのが一般的ですが、MBSDには『おそらくこの時期にこういったアプリができる予定なので、このくらいのタイミングでお願いしたい』といった相談に応じて、できる範囲で対応していただいています」（清水氏）

Webアプリケーションを取り巻くリスクが高まるにつれ、遵守すべきガイドラインや対策のレベルも向上している。直近では、クレジットカード決済において3Dセキュアの導入が求められているが、GDOはそうした水準を満たすべく、リリース前には診断を実施するルールを定め、サービスのセキュリティ向上に努めている。

その効果を清水氏は「診断に加え、WAFの性能向上も相まって、アプリケーションレイヤーに関してはほぼ問題なく、安眠できる状態を維持できています」と語った。

今後は、エンジニアのスキルアップを図りながら、開発段階からセキュリティを意識して極力指摘事項を減らし、もし問題点が見つかったとしても手戻り少なく対応できるような体制作りも視野に入れていく。その中では生成AIの積極的な活用も視野に入れている。

コンサルティングサービス導入後の利用拡大と体制整備

専門的かつ客観的な視点に基づくアドバイスを得ながらセキュリティ戦略を推進

こうして「アプリケーションを守る」という命題では成果を上げてきたGDOだったが、セキュリティ上留意すべきポイントは他にも多岐にわたる。

「アプリケーションのセキュリティだけで十分かというと、決してそうではありません。PCのセキュリティもあれば、社内オフィスのセキュリティもあります。どこかに死角はないか、またどこから手を付ければいいかを明確するに当たって社外の力を借りるのが最善だろうと判断しました」（山外氏）

個人情報を扱う予約サービスやクレジットカード決済を行うEC事業を展開するGDOにとってセキュリティは重要な課題だが、決して本業ではない。セキュリティを専門とする人材が社内に多数在籍するわけでもない中で、あるべき姿に向かってどのようにレベルアップしていくかという全体戦略を描くのは難しいと感じていた。

「私は元々エンジニアだったこともあり、アプリケーションの診断を実施すべき、EDRを導入すべきといった個別の対策については進言できます。しかしGDO全体としてどこに手を加えるべきか、何を優先すべきかという話になると自信を持って断言できませんでした」（清水氏）

そこで、Webアプリケーション診断や緊急時の対応支援を通して信頼関係を築いていたMBSDに依頼し、セキュリティ戦略全体に関するコンサルティングを受けることにした。

「NISTのサイバーセキュリティフレームワーク 2.0に基づいて実施すべき事柄を洗い出し、今、何がどの程度できているかを把握しました。そして、最終的に目指しているレベルに向け、今すぐ手を付けるべき対策、次に実施すべき対策といった順番を整理した上で、全体の底上げを進めています」（山外氏）

MBSDのアドバイスを通して、社内の議論だけでは得られなかった視点や、客観的な視点で優先すべき事柄について示唆を得ることができ、戦略は大きく前進している。「第三者視点からのアドバイスを得ることで、経営層への説得力が大きく増しました。また、何を実現するかについて合意した後の『どう実現するか』という手段についても、我々にはないアイデアを出していただけています。おそらく、我々だけではここまでのことはできなかったでしょう」（山外氏）

そんなアドバイスを踏まえて進めている取り組みの一つが、全社的なデータの棚卸しだ。「各社員が平時から業務の中でデータを適切に扱えているかどうか、機密扱いの情報を認識してそれにふさわしい形で保管できているかを可視化しようとしています」（山外氏）。これまで実施してきた情報漏洩の防止策や保護策と並行して、データをより適切に扱うための体制や規約の整備も含め、MBSDの支援を得ながら包括的な取り組みを進めている。

もう一つは、百台以上に上るサーバの脆弱性対応の最適化だ。「現状では、パッチがリリースされたのですべて適用してくださいと依頼していますが、それでは現場の労力が大きすぎます。脆弱性の情報を踏まえ、緊急度が高いものは一気に適用する一方で、他の策などでリスクを緩和できるものは定期メンテナンス時にまとめて実施するといった具合にメリハリを付けて対応できるよう、判断基準や運用体制も含め、整備をともに進めています」（山外氏）

実作業を効率化するために、MBSDがプロの視点から提案してきたツールも導入していく。ただ「その際も、あまり『この製品を導入した方がいいですよ』と押し売りをしてこないところが信用できると思っています」と山外氏は述べ、幅広い情報収集力に基づき、構築だけでなく、その後の運用を見据えた提案を評価しているとした。

今後の展望と期待するパートナーシップ

GDOの歩みに合わせて伴走しながらの支援に今後も期待

GDOでは引き続き、MBSDと定例ミーティングを重ねながら、全体のセキュリティレベルの底上げに取り組んでいく。

「データ管理を進め、組織体制ではCSIRTを整備するといった優先度の高い施策を中心に、2026年末までの計画を立てています。MBSDの伴走を得ながら、『全体としてこれだけセキュリティが担保できている』という状態に持っていきたいと考えています」（山外氏）

特に前向きに考えているのは、経営層向け、社員向けのセキュリティインシデント対応訓練だ。「今の状態でも、何かが起こったときには対応できるとは思っています。しかし、より深刻な事態が起きたときには、もっと素早く決断を下す必要に迫られるかもしれません。そうした事態に備え、想定通りに行動できるかどうかは常にチェックしておかなければいけないと思っています」（清水氏）。この観点で、インシデント対応やフォレンジック調査などでさまざまなケースを支援してきたMBSDの経験を生かし、より真に迫ったシナリオ作成やロールプレイに期待しているという。

これまでの長期にわたる支援に対し、清水氏は「何かを依頼すると、『いや、そこは不要なんだけどなぁ』という部分まで含んだ重厚長大な提案が出てくるパートナーもありますが、MBSDにはピンポイントでニーズに応える柔軟な対応をしていただけています」と評価している。

「診断やコンサルティングにおいて、常に確かな成果を出していただけるのはもちろんのこと、こちらの事情で思うように進まない時や少し立ち止まるような時でも、変わらず寄り添いながら『それなら、こういう方法もありますよ』といった形で柔軟にご提案くださることに、非常に感謝しています」（山外氏）と、これからも伴走者としてのMBSDに期待しているという。

開発元

三井物産セキュアディレクション株式会社

〒103-0013
東京都中央区日本橋人形町1-14-8
JP水天宮前ビル 6階
TEL: 03-5649-1961
Mail: sales-info@mbsd.jp

製品に関する最新情報はこちらから → www.mbsd.jp

お問い合わせ

CS11-1001-2508