導入事例

ヤマハ発動機株式会社様

ヤマハ発動機株式会社
IT本部　サイバーセキュリティ推進部
グローバル戦略グループ
グループリーダー
蔦木 加代子氏

※インタビューを実施した2025年11月17日時点の組織名、役職名です。

ヤマハ発動機は「感動創造企業」を掲げ、オートバイや自転車に始まり、ボートなどのマリン製品、さらには産業機器などのB2Bビジネスや金融サービスなど幅広い事業を通して新たな感動を提供している。海外売上比率が約94%を占める同社にとって、100社以上にも上る海外子会社のセキュリティ対策は避けては通れない課題だ。そこで同社は三井物産セキュアディレクション（MBSD）のさまざまなセキュリティサービスやコンサルティングを活用しながら、グローバル全体でセキュリティを底上げしていく体制作りを進めている。

本社	静岡県磐田市新貝2500
創立	1955年（昭和30年）7月1日
資本金	861億円（2025年12月末現在）
Webサイト	https://global.yamaha-motor.com/jp/

導入サービス

☑ **AD Security Baseline Check**
WindowsのActive Directory環境で
侵害リスクとなる問題を手軽に検出できる
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

サイバーセキュリティをグローバル全体で強化

MBSDの戦略策定から運用までの伴走によるセキュリティ対策推進支援と AD Security Baseline Checkサービスによる海外拠点におけるリスクの可視化事例

背景と課題

ヤマハ発動機では現在、データ分析の民主化を目標に掲げてデジタルトランスフォーメーション（DX）に取り組んでいる。この取り組みに欠かせないのがサイバーセキュリティだ。

同社は10年以上前から、グローバルでOffice 365の展開や認証基盤の刷新を行い、働き方を支える基盤・インフラの標準化を通してグローバルITガバナンスを推進してきた。そうした環境や枠組みを生かしながらグローバルでのセキュリティ対策強化を進めている。

また経営層も、サイバーセキュリティを品質などと並ぶ重要リスクの一つとして捉えている。ガバナンス力を高めるため、以前の組織を格上げして新たに「サイバーセキュリティ推進部」を設け、ITリスク管理やCSIRT、そしてグローバルセキュリティ戦略を統括的に推進する体制を整えた。

導入のきっかけ

WannaCry感染を機にグローバルの実態を見直し、MBSDとともに体制強化を推進

ただ、ここに至るまでにはさまざまな積み重ねがあった。

ヤマハ発動機が本格的にグローバルのサイバーセキュリティ強化に取り組む契機となったのは、2017年、世界中で猛威を振るったランサムウェア「WannaCry」の被害に海外子会社が遭ったことだった。

国内ではマイクロソフトからのパッチを速やかに適用することで被害軽減を図れたが、問題は海外の各社の対策状況だった。

「対策はできているかどうか尋ねても回答は曖昧で、パッチ適用を依頼しても確実に実施されたか確認が取れませんでした。結局、全社の状況を確認し終えるまでに6ヶ月もかかってしまったのです。この状況ではまずい、グローバルのセキュリティ体制を強化していく必要があると痛感しました。」（IT本部　サイバーセキュリティ推進部　グローバル戦略グループ　グループリーダー　蔦木加代子氏）

もちろん、対策が手付かずだったわけではない。それ以前からITリスクマネジメントガイドラインを定め、セルフアセスメントを実施していたが、実情と乖離しているのではないかという懸念が浮上した。そこで改めて実態調査を実施し、見えてきた実態を踏まえ、NISTのサイバーセキュリティフレームワークを参照しながら、ヤマハ発動機としてのグローバル共通フレームワークを作成して本社主導で実施することとした。

「当初は三年計画でロードマップを作成し、優先順位を付けながら実施するつもりでしたが、当時の本部長からは『一年で進めてほしい』と指示を受けました。当時のリソースではとても構築から運用まで持っていくのは難しいことから、専門的な知見を持つ外部の力を借りることにしました」（蔦木氏）

その一社がMBSDだった。以前から新たなセキュリティ施策に関する提案を受けており、時代を先取りしていたその内容に、前任者ともども好印象を抱いていた。さらに、経営層向けのアプローチでも助力を受けることができた。

「役員など経営層向けに、専門家の視点からセキュリティセミナーを実施することで、サイバーセキュリティについて理解を深め、重要リスクに含めてもらうよう後押ししてもらいました」（蔦木氏）

成果

1年半でプロジェクトを完了、成熟度を踏まえつつさらなる対策強化を支援

外部の力も生かしながら、セキュリティ戦略の策定、各社への導入、さらにガバナンスを効かせる体制を作り上げていく一連の取り組みを、ヤマハ発動機では約1年半で終えることができた。MBSDは、ゼロトラストセキュリティに基づくエンドポイントセキュリティ製品やネットワークセキュリティ製品の導入支援に加え、ID監視に関連するセキュリティ運用面でも協力を行った。

MBSDはそれ以来、約10年間に渡る取り組みに常に伴走してきた。「サイバーセキュリティ対策は、社内のことをよく知っていなければ進められません。MBSDからは、人との関係性はもちろん、我々のネットワークやインフラ構成を知った上で、さまざまな提案やアドバイスをいただいています」（蔦木氏）

その後、軽微なインシデントが発生したこともあったが、その都度迅速に対応し、深刻な事態に至る前に食い止めている。「もしインシデントが起きたとしても、すぐに対応できる体制作りができたと思っています」と蔦木氏は述べている。

あるケースでは、MBSDのアナリストが現地に赴き、復旧支援から一次対応までを支援した。加えて、インシデントで見えてきた実態を踏まえて海外の複数拠点に対するアセスメントと、Active Directoryに対する簡易ペネトレーションテストとも言える「AD Security Baseline Check」を実施したことにより、机上調査だけでは把握しきれなかった実態を把握し、継続的なセキュリティ改善につなげることもできた。このように、各拠点の成熟度に応じて必要な施策や体制を都度提案できていることも評価している。

「AD Security Baseline Check」は文字通りAD環境にフォーカスして、短期間で効率的にセキュリティ状態を診断するサービスだ。専用ツールを用いて診断を実施し、その結果をMBSDが解析することで、パスワード関連の設定不備やADサーバの構成ミス、不適切なポリシー設定といった代表的な問題を診断できる。

今後の展望

内製と外部に任せる領域を整理し、さらなる対策強化を継続

いくらフレームワークを定め、標準的な対策を推奨しても、実際に実施するかどうかは現地の体制に左右される部分もある。そこでヤマハ発動機では、世界各地に分散している基盤の一部をクラウドに集約し、本社による一定レベルの運用の元に移行させ、リスクの高いポイントを根本的に減らしていくことも計画している。

MBSDとともにグローバルセキュリティ体制を作り上げ、運用していく中で、ナレッジの移転が進んできた。「一緒に仕事をする中で私自身も、またメンバーも、新たなトレンドや留意点、枠組みなどさまざまなことを学び、成長している感覚があります」と蔦木氏は語る。

同社はさらに、内製で実施していくことと、MBSDのような外部の専門家に依頼することの整理を進めている。セキュリティ実施体制のチェックなど比較的学びやすい業務については、MBSDとともに現地に行き、手法やプロセスを学んで「手の内化」し、内部に展開していく方針で、キャリアプランの策定や人材育成にも反映していく。一方、より高度な専門性が求められる領域や24時間365日体制での監視・対応が求められる部分については外部に委ねたり、自動化を進めることで、リソースを効率的に活用していく。

セキュリティ対策はストレスのかかる業務になりがちだが、サイバーセキュリティ推進部では人・プロセス・テクノロジーの三位一体で持続的に成長できるサイバーセキュリティ組織を目指す。「まだ道のりは途中です。終わりのないこの道のりを、MBSDに伴走していただければと思っています」（蔦木氏）

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

 このリーフレットの記載内容はインタビュー実施時点（2025年11月17日）のものです。

CS41-1001-2604