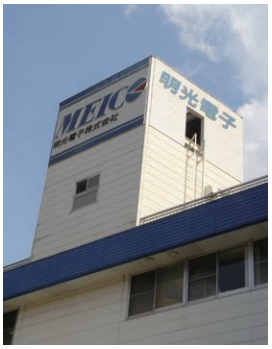
明光電子株式会社

顧客、仕入先との信頼関係を築く
情報セキュリティーを
IBM Managed Security Servicesを
中心とする対策で強化し
“明光電子”ブランドをさらに向上

お客様情報



明光電子株式会社 福岡本社

明光電子株式会社

●横浜本社所在地
〒222-0033 神奈川県横浜市港北区新横浜3-18-9　新横浜ICビル
http://www.meicodenshi.com/

1979年（昭和54年）福岡市において、ICおよび電子部品の専門商社としてスタート。当初は80%が輸入ICの取り扱いだったが、多品種小ロットに注力して商品分野を拡大。各業界のトップクラスのメーカーと直接取引を行い、なおかつその80%が競合しないことを強みとする。あえて敵味方をはっきりさせることにより、新製品の企画に役立つ情報提供からサンプル開発、技術サポートまで、幅広い業務プロセスにまたがる高品質のサービスを提供。国内・海外の1,000社以上の仕入先のうち、TDK、TDKラムダ、ローム、オムロン、シイエムケイ・プロダクツ、三社電機製作所、新電元工業、ニチコンなど、300社以上の一流メーカーと直接取引をしている。

“専門商社”と“便利屋”の二面性を持つユニークな半導体・電子部品商社として知られる明光電子株式会社（以下、明光電子）は、「多品種小ロット」に注力した独自の差別化戦略で成長し、他社の追随を許さないビジネスモデルを築いてきました。その大前提となるのが、“安全・安心”をベースに顧客や仕入先との信頼関係を構築する情報セキュリティーです。2014年にIBM® Security Network Intrusion Prevention System（以下、Network IPS）およびIBM Managed Security Services（以下、MSS）を導入。さらに2016年にFireEyeおよびMSS、IBM Eメール・セキュリティー管理サービス（以下、ESMS）を追加してセキュリティー・レベルの向上を図り、常に先手を打つ“攻め”のセキュリティー対策で、企業ブランド力をさらに高めています。

情報セキュリティーは事業継続や取引拡大を支える経営課題そのもの

半導体・電子部品は、世界で最も熾烈な競争が繰り広げられている産業の代表格です。その中で「戦わずして勝つ」というブルー・オーシャン戦略（競争相手がいない未開拓市場である「ブルー・オーシャン」を切り開く経営戦略）を地で行く独自の経営スタイルを貫き、成長を続けてきたのが、電子統合商社の明光電子です。

同社の主な事業は、顧客である電機・電子メーカーが必要とするさまざまな半導体や電子部品を国内外の仕入先から調達し、提供することです。ただ、実際の業務はそれだけにとどまりません。「私たちは“専門商社”と“便利屋”の顔を併せ持った会社なのです」と話すのは、代表取締役の十川　正明氏です。商談には必ず製品の企画段階から参画し、情報提供や技術サポート、製造、検査、さらには在庫管理にいたるまで、幅広い役割を担っています。

明光電子の強さのもうひとつの理由が、「多品種小ロット」への注力です。

「パレートの法則」によれば、市場全体の売上の80%を、上位20%の顧客が占めます。半導体・電子部品ビジネスも例外ではなく、手早く売上を伸ばしたいのであれば、この上位20%の顧客に的を絞ってビジネスを展開するのが得策と思えます。しかし、多くの競合他社がしのぎを削る中で、同じような方法で戦っていたのでは勝てる見込みがありません。結局は、ほとんど利益を生み出さない不毛な価格勝負に挑んでいくしか道がなくなってしまいます。

そこで明光電子は、大手商社が振り向かない「多品種小ロット」にあえて勝負をかけてきました。個々の案件の売上は小さくても、幅広く販売することに徹した結果、明光電子が直接取引を行う仕入先は各業界のトップ企業300社以上、

事例概要

課題

- 顧客の製品開発のあらゆるプロセスに関わる事業活動に不可欠な“安全・安心”に裏付けられた顧客、仕入先との信頼関係を構築するための情報セキュリティー強化

ソリューション

- IBM Security Network Intrusion Prevention System
- IBM Managed Security Services
- FireEyeソリューション
- IBM Eメール・セキュリティー管理サービス

効果

- 情報セキュリティー対策について、各業界の最先端を走る顧客から高く評価されており、「明光電子」企業ブランドが向上
- 顧客、仕入先からのすべてのセキュリティー監査をクリア
- 社内でのネットワーク監視の手間が省力化

取り扱う半導体・電子部品は産業用を中心に31万点以上に拡大。「こうして他社の追随を許さないビジネスモデルを築くことができました」と十川氏は話します。

もっとも、明光電子が追求するこのビジネスモデルには、大前提となる条件があります。それは“安全・安心”に裏付けられた顧客との信頼関係の構築です。

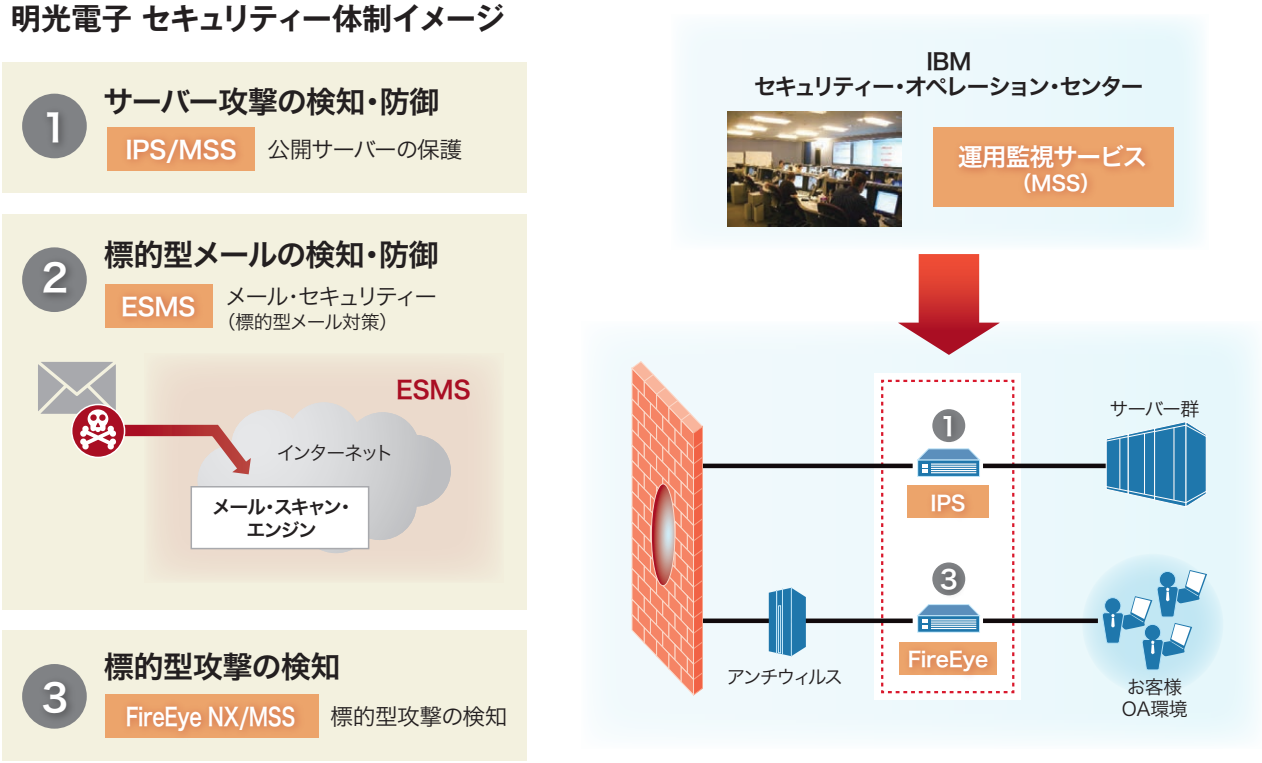
「お客様の製品開発にあらゆるプロセスで関わっていく以上、多くの機密情報や知的財産情報をやり取りすることになります。これらの情報が決して外部に漏れるようなことがあってはなりません。私たちにとって情報セキュリティーは、事業継続や取引拡大を支える経営課題そのものなのです」と十川氏は強調します。

情報セキュリティーの維持管理は外部の専門家に任せたい

ただ、情報セキュリティー対策のための潤沢な体制を社内に構築するのは容易なことではありません。むしろ、ITシステムを社内で運用することに疑問を持っており、「できることなら情報セキュリティー対策も含めて丸ごとクラウドに移管したいと考えてきました」と十川氏は話します。

同社の取締役であり、情報企画部の部長を務める川路 渉氏も、「情報セキュリティー対策で最も負荷が大きいのは、ネットワーク監視です。日々膨大な量のアクセス・ログが出力され、一覧するだけでも1～2時間を費やします。それでいながら、『絶対に侵入されていない』という確証を持つこともできません。そんな非効率な作業に追われている貴重なリソースを新たなIT戦略の立案など、もっと前向きな仕事に割り振りたいものです。情報企画部のメンバーを煩雑な手間と不安から解放するため、私も情報セキュリティーの維持管理は外部の専門家に任せたいと望んでいました」と話します。

明光電子 セキュリティー体制イメージ



出典：明光電子株式会社

“私たちにとって情報セキュリティーは、事業継続や取引拡大を支える経営課題そのものなのです”

代表取締役
十川 正明氏

“ネットワークのアクセス・ログを確認していた手間も、IBMによる運用監視サービスのおかげで現在は完全に省力化されています”

取締役
情報企画部　部長
川路 渉氏

“情報セキュリティー対策の重要性や基本的な仕組みをしっかり学びつつ、アプリケーション開発に専念させてもらっています”

情報企画部
加瀬 響氏

こうした状況下にあった2014年、明光電子はITシステムを不正アクセスから防御するNetwork IPSおよびセキュリティー運用監視サービスのMSSを導入しました。

選定の決め手となったポイントは、「IBMの“本気度”を感じたことです」と十川氏は話します。「IBMは私たちを東京セキュリティー・オペレーション・センターに案内し、セキュリティーの専門技術者たちが、実際に24時間365日体制で監視・運用・管理を行っている現場を見せてくれました。率直なところ、カタログ・スペックを見比べるだけなら他社のセキュリティー製品や運用監視サービスも大差ありません。しかし、そのほとんどはブラックボックスです。ここまで実態を明らかにしてくれたのはIBMだけでした」

そして、それから2年を経た2016年5月、明光電子はマルウェア感染を防御するFireEyeおよびその運用・監視を担うMSS、Eメール・セキュリティー管理サービスのESMSという新たなセキュリティー・ソリューションを追加導入しました。

「標的型攻撃に象徴されるように、ますます悪質化・巧妙化していくサイバー攻撃の動向を考慮し、私たちは先手を打つための対策を求めていました。そうした中でIBMから新たな提案をいただいたのです。ネットワーク構成を変更することなく、既設のアプライアンスと同じ経路にFireEyeのサンドボックスを追加するだけで、すべての準備が完了し、Network IPSと同様に、MSSの監視対象にすることができるのも大きなメリットでした」と川路氏は話します。

情報セキュリティーのレベルの高さが業界最先端を走る顧客から感心される

今回のFireEyeおよびMSS、ESMSの追加により、明光電子のセキュリティー・レベルはさらに向上したわけですが、社内の負荷はまったく増えていません。「以前には毎日1～2時間の工数を割いてネットワークのアクセス・ログを確認していた手間も、IBMによる運用監視サービスのおかげで現在は完全に省力化されています」と川路氏は話します。

この効果は、若手メンバーの育成にも大きく表れています。入社2年目で情報企画部に配属となった加瀬 響氏は、「情報セキュリティー対策の重要性や基本的な仕組みをしっかり学びつつ、アプリケーション開発に専念させてもらっています」と話します。

そして、一連のセキュリティー対策への取り組みによる最大の成果と言えるのが、明光電子のブランド力の向上です。

「お客様や仕入先から弊社の情報セキュリティーに対して、問い合わせを受けることがよくあります。そうした場面で、『とっくに対応できていますよ』と胸を張って答えられます。情報セキュリティーがビジネスの足を引っ張らないどころか、各業界の最先端を走るお客様から感心していただけるのです。これは非常に大きな強みになっていると感じています」と十川氏は話します。

実際、明光電子は多くの仕入先、顧客企業、さらにその関連会社から、毎年1回は必ずセキュリティー監査を受けているのですが、そのすべてを難なくクリアできています。

「私たちとしては、事実をありのままに記述して粛々と報告するだけです。常に堂々と構えて高い評価をいただけることは、一人ひとりの営業担当者の活動のしやすさにもつながっています」と川路氏は話します。

左から川路氏、十川氏、加瀬氏

新たなサイバー攻撃が問題視され始めた時点で すでに対策を終えている状態を維持し続ける

セキュリティーを取り巻く環境は今後もどんどん変化していきます。数年前にはまったく騒がれていなかった標的型攻撃が現在では深刻な社会問題となっているように、今後も未知のサイバー攻撃が登場し、脅威となる可能性も大いにあります。

「新たなサイバー攻撃が問題として世の中で認識され始めた時点で、私たちはすでにその対策が終わっているという状態を、今後も維持し続けていきたいと考えています」と十川氏は話します。

とはいえ、セキュリティーの動向を読み解くための情報はあまりにも膨大です。明光電子がそれらの情報を独自に集め、世界中で起こっている事象を分析し、対策テクノロジーのトレンドを見極めていこうとしても困難です。「だからこそそこに、世界最大級の民間セキュリティー研究開発組織であるIBM X-Forceを擁して、幅広い知見やノウハウを持つIBMとのパートナーシップに向けた期待があるのです」と川路氏は話します。

ライバルを寄せ付けないブルー・オーシャン戦略をさらに強化すべく、引き続き明光電子はIBMとの二人三脚で、“攻め”の情報セキュリティーを実践していく構えです。

日本アイ・ビー・エム株式会社

〒103-8510　東京都中央区日本橋箱崎町19番21号