三栄ハイテックス株式会社

自社と顧客にとっての生命線を守るため、運用負荷の少ないFortiEDRを導入 ベストプラクティスサービスを活用して 最適な設定を見出し、EDRの自社運用を開始

三栄ハイテックスはデジタル時代を支える半導体/LSIの設計会社だ。半導体設計・製造に関する情報は、同社はもちろん顧客にとっても「生命線」となる。この情報を漏洩から確実に守るために他社のEDR製品を導入したものの、運用に課題を抱えていた同社は「FortiEDR」への移行を決断。フォーティネットの導入支援を得て自社運用を開始している。

三栄ハイテックス株式会社

本　　社　静岡県浜松市東区子安町311-3
創　　業　1977年11月
設　　立　1983年12月
事業内容　LSI設計/半導体設計、AI開発など
従業員数　357名（2022年4月）

三栄ハイテックス
経営企画部部長
安達 晴康氏

三栄ハイテックス
経営企画部
情報システム室
池谷 直氏

設計情報を守るため、自社はもちろん、顧客からも厳しく求められるセキュリティ対策

あらゆる産業を支える半導体。国内では大手半導体企業のM&Aによる再編が進む一方、台湾・中国をはじめアジア市場が躍進し、目まぐるしく変革し続けている。その中で独立系の半導体設計会社として国内有数の規模を誇る三栄ハイテックスは、技術者集団として、半導体を通して国内のさまざまなメーカーのモノ作りを支えてきた。近年はAIなどソフトウェア領域にも力を入れ、一貫したサポートを展開しつつ、中国やベトナム、台湾などアジア地域での事業を拡大している。

その同社にとって、顧客企業それぞれのノウハウや先端技術が詰め込まれた半導体の設計情報は何よりも守るべき機密情報だ。経済安全保障の観点からも重視されている半導体の情報が漏洩するようなことがあれば、あっという間に技術の差を埋められ、市場での優位性に影響が生じる恐れがある。こうした背景から三栄ハイテックスでは、「昔から、セキュリティには非常に厳しく取り組んできました」と、三栄ハイテックス 経営企画部部長の安達晴康氏は述べる。

しかも最近では、経済安全保障が重視され、サプライチェーン全体にまたがるセキュリティ対策も求められるようになっている。「メディアでたびたび情報漏洩事件が報道されることもあり、取引のあるお客様からセキュリティ対策状況を問われたり、チェックリストの提出を求められる場面も増えています」（安達氏）

導入・構築のポイント

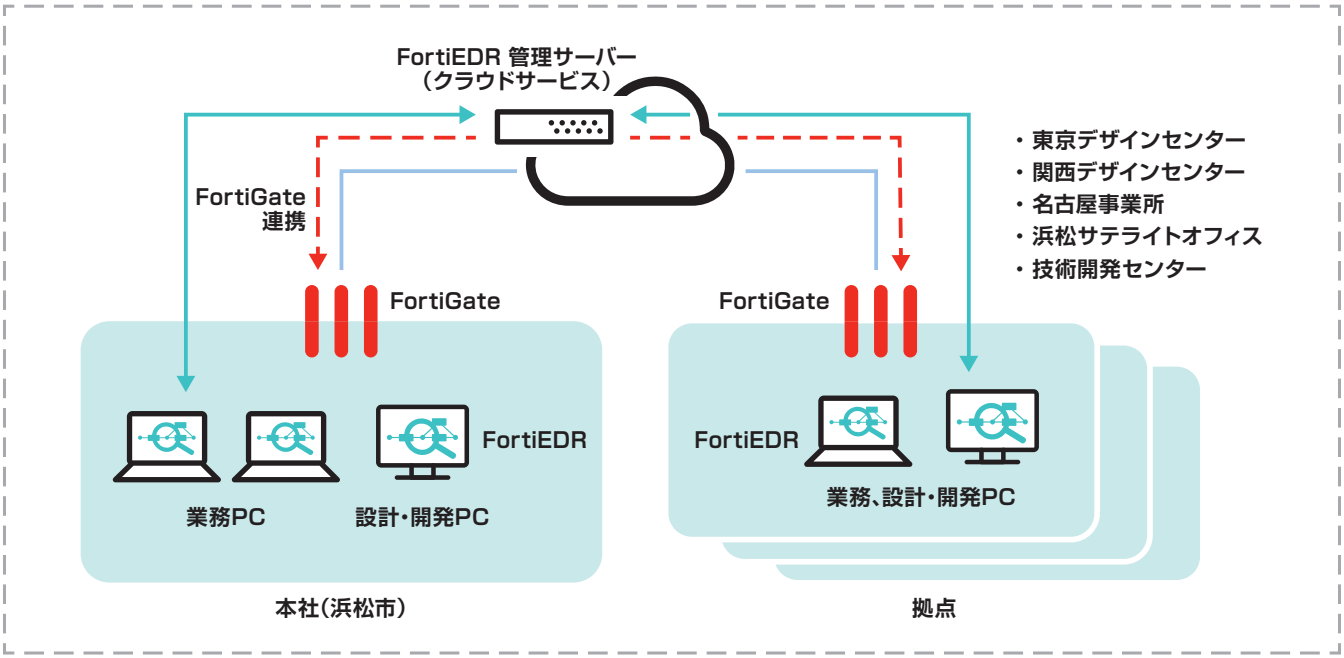
（1）より踏み込んだ対策ができて、運用の容易な第2世代EDR製品であるFortiEDRを導入

（2）使い勝手の良さに加え、経営層に対する定期報告に活用できるレポート機能を評価

（3）ベストプラクティスサービス（BPS）で自社にとって最適な設定を見出し、自社運用を開始

運用負荷の少ない「FortiEDR」を選定、使い勝手の良さもポイントに

三栄ハイテックスでは以前から、フォーティネットの「FortiGate」でネットワーク出入り口の守りを固めるとともに、従業員が利用するPCにアンチウイルス製品を導入するなど



の対策を講じてきた。「アンチウイルスは成熟した分野となり、Windows Defenderでも十分有効だと考えるようになりました。さらに、一歩進んだ対策としてEDRを検討することにしました」（安達氏）

こうした背景からある海外メーカーのEDR製品を導入したが､徐々に「過検知」が目立つようになり、運用負荷が拡大してきたという。また、国際情勢の変化からそのメーカーの体制にも不安を抱くようになり、切り替えを検討することになった。

いくつかのEDR製品の情報を収集し、比較検討した中で採用を決定したのが「FortiEDR」だった。以前からFortiGateを利用し、フォーティネット製品に対する信頼感があったことに加え、コストパフォーマンスに優れていること、WindowsだけでなくmacやLinuxなど幅広いOSにも対応していることがポイントとなった。

さらに、レポート機能や使い勝手の良さにも魅力を感じたという。「いくら機能が豊富でも使い勝手が悪ければ意味がありません。我々は情報システム部門として、経営層に『今、セキュリティはこういう状況にあります』と定期的に報告する義務がありますが、その報告書作成が容易にできそうだと感じました」（安達氏）。

こうして三栄ハイテックスでは2022年2月にFortiEDRのPoCを開始し、3月に正式導入を決定した。その後、2022年4月に導入に向けた準備を開始した。

運用中のFortiGate
FortiEDRとの連携を予定

フォーティネットの支援を得ながら適切な設定を見出し、自社運用に向けノウハウを蓄積

一般にEDR製品は、エンドポイントにソフトウェアをインストールすれば終わりとはいかない。外部パートナーが提供する、MDR（Managed Detection and Response）と呼ばれる運用監視サービスと組み合わせて導入するケースが一般的だ。しかし三栄ハイテックスでは自社でのEDR運用にこだわっていた。コスト面もさることながら、「お客様の重要な情報を扱う以上、外部に依頼せず自社運用すべきと考えているからです」（安達氏）

ただ、従業員数350名強の同社には、

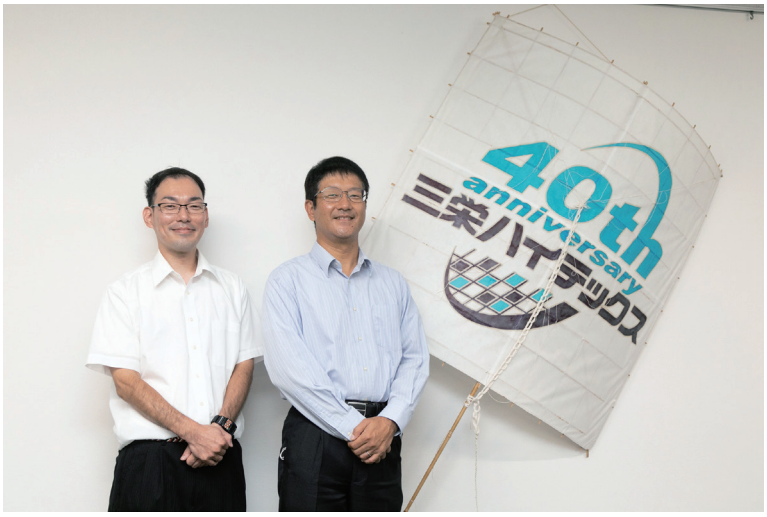
何人ものセキュリティ担当者がいるわけではない。どのようにスムーズに導入し、運用体制を確立していったのだろうか。

まず、不審な動きを見つけたらログに記録するだけで動作停止までは行わない「シミュレーションモード」で、FortiEDRの運用を開始した。しばらく様子を見ながら設定のチューニングを進め、2022年8月から本格的に運用を開始したという。

それを支えたのがフォーティネットの「ベストプラクティスサービス（BPS）」だ。FortiEDRでは、製品導入時から数ヶ月間かけて、製品の使い方や設定のアドバイスをするBPSを標準で提供している。BPSを活用することで、ホワイトリストを含む各種の設定を導入企業の環境に合わせて円滑に進めることができ、自社でのEDR運用に向けたノウハウを蓄積できる。

「どのような範囲でホワイトリストに登録すべきかは、やはり自分たちで判断しなければいけません。必要最低限、不審な動きを監視できるような設定に落ち着くまで、1カ月程度かけました」（三栄ハイテックス 経営企画部 情報システム室、池谷直氏）というが、以前利用していたEDR製品に比べ、ホワイトリストの登録作業をはじめとする運用は楽になった。不審な動きを検出する範囲やその後のアクションなどの細かなカスタマイズについても、BPSを通してフォーティネットのエンジニアからアドバイスを得て設定を進めていった。

この結果、従業員からは特にクレームもなく運用できている。一方で、悪意ある攻撃をこれだけ検出できた、という実感はあまりない。というのも、すでにFortiGateなどを組み合わせて多層防御を施しており、Emotetのような攻撃については境界でブロックできているからだ。



本社がある浜松市では、毎年5月の浜松まつりで「凧揚げ合戦」が開催される。
40周年を迎えた2017年にミニチュアを作成（実際に揚げる凧は3〜8畳の大きさ）。

ただ「たとえば端末でファイルをコピーすると、その時点でメモリ間の移動などを検出していることがわかります。FortiEDRはWindows Defenderよりも先にこうした挙動を見つけています」（安達氏）という。引き続き運用の枠組みを整備しながら、効果を確かめていきたいとしている。

想定外のメリットもあった。三栄ハイテックスでは別途資産管理ソフトウェアを導入し、PCに導入されているソフトウェアを管理してきたが、FortiEDRではさらに、外部と通信を行っているアプリケーションを検出できるようになり、社内の状況をよりきめ細かく把握できるようになった。「FortiEDRでは通信を元に、どんなソフトウェアが利用されているか、バージョン情報も含めて細かく把握できます。パッチを当てていないバージョンが動いていれば使用禁止にするといった設定もでき、非常に便利だと感じています」（安達氏）

FortiGateとの連携によって、悪意ある通信を速やかにブロックする仕組みも模索

三栄ハイテックスは今後、FortiEDRの運用を確立させていくとともに、FortiGateとの連携を行う計画だ。「ウイルスのようにすぐわかる脅威ではなく、より巧妙なマルウェアが侵入して怪しい振る舞いをしていることをFortiEDRで検知したら、そのマルウェアと悪意ある外部サーバーとの通信をFortiGateで止めるといった連携を期待しています」（安達氏）

社内のIT環境も、トレンドに合わせて改善していく方針だ。中には、どうしてもオンプレミスで動作させる必要がある開発ツールもあるが、できるものは徐々にクラウド環境へと移行していく。「トラフィックの出入りもクラウドで検知し、セキュリティもクラウドで管理するようなソリューションが徐々に登場しています。我々もそういった方向を見据えつつ、よりよいソリューションを組み合わせながら、安心・安全な環境を実現していきたいと思います」（安達氏）

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

CS-i-Sanei-Hytechs-2211-JP-R1