TOYOTA SYSTEMS

工場設備、R&D設備における情報共有とセキュリティ確保、相反する要求をFortiGateで両立 OSのアップデートが困難な試験設備の防御にも活用

自動車業界が大変革期に直面する中、工場におけるモノづくりのあり方もまた変わろうとしている。トヨタ自動車およびグループ企業をITソリューションで支えるトヨタシステムズでは、モノづくり現場から得られるデータの共有・活用とセキュリティを両立するため、防御の基本であるセグメンテーションをFortiGateで実現した。

株式会社トヨタシステムズ

【名古屋本社】
名古屋市中村区名駅1-1-1 JPタワー名古屋32F
【東京本社】
東京都港区港南1-8-23 Shinagawa HEART14F
設　　立 2019年1月1日
資 本 金 54.5億円
従業員数 3,088人（2021年4月1日時点 派遣社員含む）
売　　上 1,255億円（2019年度実績）
関係会社 トヨタ自動車株式会社
　　トヨタファイナンス株式会社
出資比率 トヨタ自動車株式会社 100%出資

株式会社トヨタシステムズ
インフラ事業本部
副本部長
寺澤 知昭氏

株式会社トヨタシステムズ
セキュリティサービス部
ソリューション1G GM
田中 徹氏

株式会社トヨタシステムズ
セキュリティサービス部
ソリューション1G 主査
菅井 秀行氏

株式会社トヨタシステムズ
セキュリティサービス部
ソリューション1G 主任
角谷 一成氏

導入・構築のポイント

(1) 工場ネットワークと情報システムネットワークの間でアクセス制御と不正通信の監視を行い、セキュアな形で情報共有を進めて業務を効率化

(2) OSのアップデートが困難な試験設備に付随するPCをアクセス制御とIPSで保護

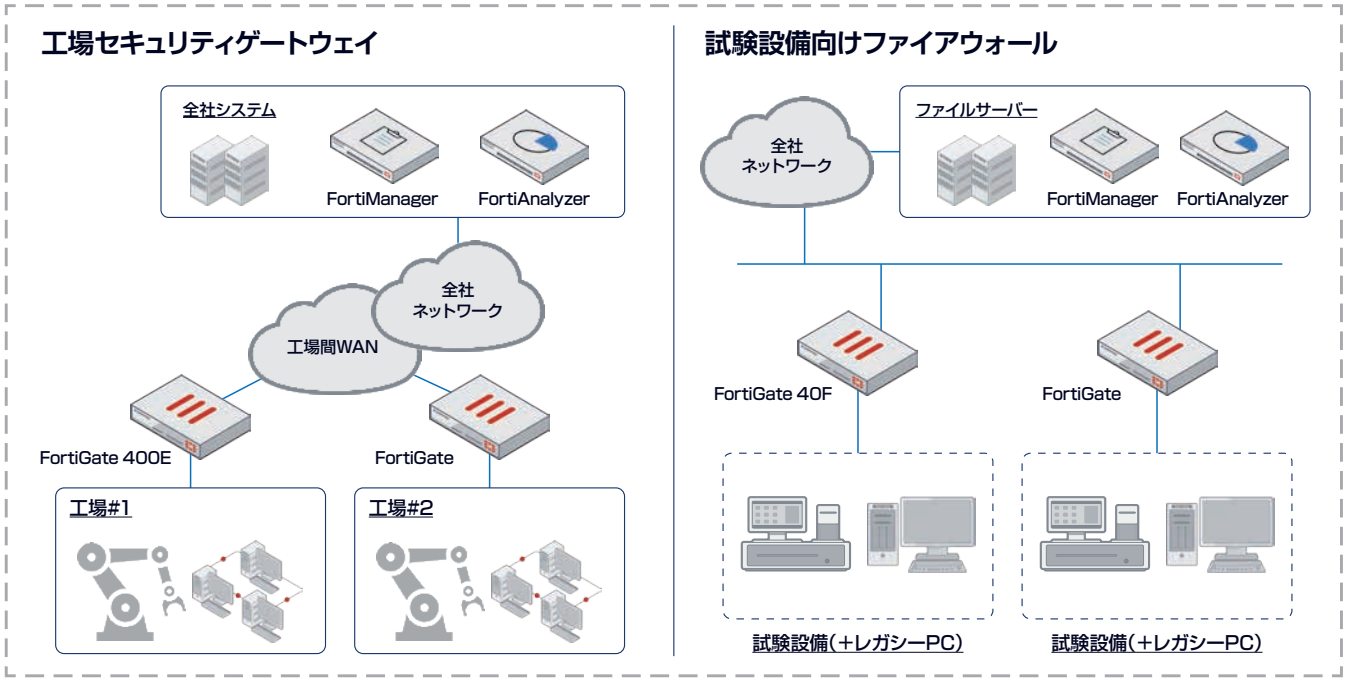
(3) コストパフォーマンスに優れた機器を監視サービスと組み合わせ、負荷の少ない運用体制を実現

100年に一度の変革期、さらなる効率化と情報共有が課題に

デジタル時代の到来とともに製造業は大きな変革期に突入している。中でも100年に一度の大変革期に直面しているのが自動車業界で、各社が生き残りをかけて「CASE（Connected、Autonomous、Shared&Services、Electric）」への対応を図ろうとしている。

トヨタシステムズでは長年、自動車メーカーやサプライヤーの情報システムを支えるとともに、現場の業務とのバランスを取りながらセキュリティ対策の企画・提案も行ってきた。ただ、この過渡期にあって、モノづくりのあり方もまた変化してきている。トヨタ自動車やトヨタグループ向けにITソリューションを提供しているトヨタシステムズのインフラ事業本部副本部長、寺澤 知昭氏は、「物理的なものに頼ったオペレーションから脱却し、効率化と情報の利活用を推進していかなければいけない」と危機感を顕わにした。「モビリティカンパニー」を支えるアプリケーションや基盤をクラウドで構築して業務の効率向上を図るとともに、クルマや顧客にまつわるさまざまな情報を共有し、活用していく必要があるという。

従来は工場の生産制御システムは、「ミッションクリティカルな部分にはできるだけ手を触れない」という考え方で分けておけばよかった。だが、デジタル技術を活用して効率性を上げることを考えると、必然的に何らかの形で工場のシステムと情報システムとをつなぎ、情報を共有していかなければならない。その中でどのように必要十分なセキュリティを確



保するか——トヨタシステムズでは先進的なIT技術を活用するだけでなく、工場セキュリティのあるべき姿を模索し始めている。

セキュリティを保ちながらカイゼン活動関連の情報共有を実現

その一環として同社は、フォーティネットの「FortiGate」を活用し、工場設備セキュリティゲートウェイの実現に取り組んだ。

「工場の中で展開されるさまざまなカイゼン活動を加速するため、カイゼン活動に関するさまざまな情報を共通プラットフォームに載せ、複数の工場にまたがって活用できるようにしたいと考えました。ただ、こうしてつながりが強くなると、工場ネットワークと情報システムネットワークで双方のリスクが拡散しやすくなるため、ネットワーク側でのしっかりとした対策が必要だと考えました」(トヨタシステムズ　セキュリティサービス部 ソリューション1G 主査 菅井 秀行氏)

情報システムネットワークと工場ネットワークの設備の中には密結合になっていた部分もあった。そこを分けて問題が発生しても拡散しない仕組みにするとともに、両者の間に「境界ネットワーク」を設け、FortiGate 400Eを導入。アクセス制御や不正通信の検知・遮断を実施することにした。

同時に、外部のセキュリティ企業も活用して監視体制を構築。システム構成や脅威の状況と照らし合わせながらシグネチャ更新を判断するほか、FortiGateから何らかのアラートが上がった場合にはセキュリティアナリストが精査を行う。もし深刻な問題となりそうな場合には、問題の発生箇所に応じてしかるべき窓口に連絡し、速やかに対応する仕組みを整えた。

実は一部の工場では、既に別の製品が工場設備セキュリティゲートウェイとして導入され始めていた。しかし導入を進める中で、性能・機能が同等以上でコストパフォーマンスに優れるFortiGateを採用することになった。

決め手の1つは、試験導入における結果だ。「独自のASICを搭載しており、工場システムにおいてもいろいろなシグネチャを使って検知できるのではないかと期待していましたが、PoCで実際に、既存の機種と同等の検知ができるだけでなく、過検知が少ない点を評価しました」(菅井氏)。アラートに追われて運用負荷が上がる事態は避けたいだけに、監視サービスも含めたコストパフォーマンスが高い点も評価した。

同社がフォーティネット製品を扱うのは初めてのことだった。だが「保守のルートをしっかり作り、何かあったときには緊急対応してもらえる体制を整えてもらいました」(菅井氏)と、対応を評価している。またトヨタシステムズ セキュリティサービス部 ソリューション1G GMの田中氏は、「実際にASICを開発しているエンジニアに話を聞く機会もありまし

たが、製品のコアとなる技術を自前でしっかり作っているところに良さを感じました」とモノづくり企業への共感を感じ、今後もさまざまなニーズに応えていってほしいと期待を寄せた。

2020年9月時点で工場全体のうち3分の1でFortiGateが稼働し、「FortiManager」「FortiAnalyzer」を組み合わせた監視体制も動き出した。評価を踏まえて、全工場の工場設備セキュリティゲートウェイをFortiGateに入れ替えることも検討していく。

今この仕組みで監視しているデータ量はそれほど多くないが、「今後は、不具合があったときに振り返りができるよう、画像や動画を継続的に蓄積して分析したいといった要望も出てくるかもしれません」（菅井氏）。ゆくゆくは、生産そのものにかかわる制御系の通信をしっかり監視し、AIなどを活用して不正な通信を検知・遮断するような仕組みも検討していく。

どうしてもOSをアップデートできないR&D設備をFortiGateで保護

トヨタシステムズがフォーティネットとともに取り組む工場セキュリティ強化施策はもう1つある。クルマの性能評価試験、エンジン開発試験、ハイブリッドシステム、燃料電池の研究開発設備に付随する端末の保護だ。

クルマの安全を保つ上で、小さな部品レベルから組み上げた車体レベルに至るまで、各種の試験は不可欠だ。こうした試験設備の多くに専用ソフトウェアを導入したPCが付随しているが、そのセキュリティ対策が課題となっていた。

「R&D部門全体で約1万700台の設備制御用PCがあります。Windows 10にアップデートできるものはしていますが、OSをアップデートしたりパッチを当てたりすると試験設備ごと止まってしまったり、メーカーのサポートが受けられなくなるものもあり、全体の約6%がWindows 10にアップデートできない古いOSのままでした。R&D設備は一般に稼働年数が長いのですが、その中でOSがなかなか最新のものに追従できない状態でした」（トヨタシステムズ セキュリティサービス部 ソリューション1G 主任 角谷 一成氏）

一部ネットワークから遮断した状態で利用している設備もあるが、試験内容によっては計測結果を情報システム側のファイルサーバに書き込まなければならず、情報システムに接続せざるを得ないものもある。かといって、古いOSのまま動いている設備を情報システムネットワークにそのまま接続させるのは、マルウェア感染・拡散のリスクを考慮すると避けたかった。

そこでトヨタシステムズでは、各実験室の手前に小型のファイアウォールを導入し、ネットワークとの通信を制御することにした。「アクセスコントロールリストによって通信を制御するとともに、IPSによって、脆弱性を突くような不正な通信があったら自動的に遮断するようにしました。同時にIDSの機能によってログを収集し、SOC側で集中的に管理・監視できる体制を整えました」（角谷氏）

そこで採用したのが「FortiGate 40F」だ。採用を決めた理由の1つは、ASICによって高い性能を発揮しつつ、コストパフォーマンスに優れていることだ。保護対象として考えている機器は約450台に上ることから、費用対効果は重要な要素だった。また、通信元のIPアドレスが変わらず透過的に保護でき、既存のネットワーク設定に影響を与えないことも決め手の1つとなった。

R&D設備を保護するFortiGate 40Fは2020年9月から徐々に稼働を開始しているが、「導入後、試験業務に支障を来すようなことなく運用できており、満足しています」と角谷氏はいう。

今後は、運用監視の負荷を減らすため、FortiManagerを活用しての一括管理を進めていく。また不正通信を検知するシグネチャについては工場設備セキュリティゲートウェイと共通化し、誤遮断の可能性を減らしつつ運用コストのさらなる低減に取り組んでいく方針だ。

同じ課題に直面するグループ企業の支援も視野に

トヨタシステムズも含めたトヨタグループ全体がITはもちろん、OTのセキュリティにも取り組みを強化しているが、「オールトヨタで集まる場でも、設備制御用端末のセキュリティ強化に向けてどんな施策が必要かをワーキンググループを設けて議論しています」（田中氏）という。今回の取り組みについてもそのワーキンググループで紹介し、同じ課題に直面しているグループ企業を支援し、ともにレベルを高めていきたいと考えている。

絶え間ないカイゼン活動を通して品質の高いモノづくりに取り組んできたトヨタグループ。デジタル技術を駆使して「コトづくり」へ取り組み始めた今もその精神は変わらず、絶え間なく改善しながらグループ全体のセキュリティの強化に努めていく。

フォーティネットジャパン株式会社

〒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