RICOH

「自分たちの工場のセキュリティは自分たちで守る」現場とグループ統括、専門家が一体となって進めた工場セキュリティジャーニー

デジタルサービス企業への変革に取り組むリコーでは、情報セキュリティ、プロダクトセキュリティは推進してきたものの、「工場セキュリティ」をどう実現するかが課題となっていた。同社はまず現状把握からスタートし、現場の意見を大切にしながらリファレンス工場での対策を推進。そのモデルを国内外の各工場に展開しようとしている。

株式会社リコー

本社所在地　東京都大田区中馬込1-3-6
設　　立　1936年2月
連結従業員数　81,017名
連結対象子会社・関連会社　240社
（2023年3月31日現在）

株式会社リコー
セキュリティ
統括センター
セキュリティ・安全保障
エキスパート
若杉 直樹氏

リコーインダストリー
株式会社
執行役員
東北事業所所長
プリンタ生産事業部
事業部長
庄司 勝氏

ITやプロダクト面での対策を推進してきた一方、欠けていたファクトリーセキュリティ体制

「“はたらく”に歓びを」というビジョンを掲げるリコーは、今まさに、OAメーカーからデジタルサービスの会社への変革に取り組んでいる最中だ。デジタル複合機などエッジデバイス領域での強みを生かしつつ、クラウドなどを活用した新たなサービスの実現に取り組んでいる。

導入・構築のポイント

(1) アセスメントを通じて現状を把握することから始め、専門家の意見を得ながら段階的に対策を実施

(2) 現場の課題解決にフォーカスし、人とプロセス、フォーティネットの技術を生かし成熟度を向上

(3) リファレンス工場の成功モデルを、国内外の各工場に展開する形で無理なく対策を推進

ただ、外の世界とつながるということは、セキュリティがいっそう不可欠になることも意味する。

以前から同社は、CEO直下にセキュリティ統括センターを組織化し、5つのビジネスユニットと連携しながらグループ全体で情報セキュリティ推進体制を整えてきた。そしてグローバル各国のさまざまなセキュリティ法制度や規制を踏まえながら戦略に取り入れ、世界的なガイドラインとなっているNIST SP800-171への準拠も目指している。

この体制の中で、CSIRTを中核とした「コーポレートセキュリティ」とPSIRTを中核とした「プロダクトセキュリティ」、2つの推進体制を整備して対策に取り組んできた。しかし「1つ足りないところがありました。それは、ファクトリーセキュリティの推進体制であるFSIRT（Factory SIRT）です」（株式会社リコー セキュリティ統括センター セキュリティ・安全保障エキスパート 若杉直樹氏）

サイバー攻撃者はしばしば「弱いところ」「止まっては困るところ」を突いてくるが、その意味で、生産データや工場の稼働は格好のターゲットになりつつある。現に、ランサムウェアをはじめとするサイバー攻撃によって、情報システムが影響を受けるだけでなく生産ラインが停止するといった深刻な被害が国内でも複数発生していることを踏まえ、リコーでも次の一手の必要性を感じていた。NIST SP800-171対応、そして変化する世界情勢の中での安全保障やリスク管理といった観点からも、工場のセキュリティ対策の緊急度は高まっていた。

「リファレンス工場」の役割を果たす最初のモデルとなったリコーインダストリー東北事業所

現場にフォーカスしながら リファレンス工場で対策を実践し、段階的に展開する方針を策定

当時、リコーの各工場におけるセキュリティ対策の状況は、「統一的なセキュリティの対応を進める以前に、各工場のセキュリティの状態がどうなっているのか可視化できていない状態でした」と若杉氏は振り返る。

リコーはグループ全体で数十もの工場を展開しているが、CSIRTを中心としたコーポレートセキュリティ対策の一環として、工場の入口のネットワークまでは対策を実施していた。しかしそこから先のOT環境となるとスコープ外で、PC管理についてもパッチ適用などの運用は行っていたものの、具体的に工場の中でどのように使われ、どういったアプリケーションが動作しているかまでは把握できていなかったという。そこでまず、「工場セキュリティの対応状況を把握する必要がある」と判断した。

工場でのセキュリティ対策を進めていく上で留意したことが2つある。1つは、数十に上る工場すべてで一気に対策を進めるのではなく、まず「リファレンス工場」を選定して実践し、成熟度を上げた上で、他の各工場に展開していく段階的なアプローチを採用することだ。

最初のリファレンス工場に選ばれたのが、複合機やプリンタの「組み立て」、トナーの製造という「プラント」、そしてリコー全体のコストや品質を左右する「キーパーツ」という3つの事業を手がけるリコーインダストリー東北事業所だった。

東北事業所では組み立て事業において、デジタルマニュファクチュアリング、いわゆる「工場のスマート化」に取り組んでおり、その意味でセキュリティの重要性を感じていた。またトナー事業は、リコーにとって事業継続を左右する生命線であり、万一サイバー攻撃によって停止した場合、リスクが非常に大きい。この2つを兼ね備えている事業所という観点で選定された。

話を聞いた東北事業所側も歓迎した。「元々東北事業所ではISMSに沿ったセキュリティ対策を進め、OSやアプリケーションのアップデートを実施していく土壌がありました。また、いろいろな企業でサイバー攻撃による被害が発生していることも耳にしていたため、工場のセキュリティ対策をその上に追加し、ドライブをかける必要があると感じていました」（リコーインダストリー株式会社 執行役員 東北事業所所長 プリンタ生産事業部事業部長 庄司勝氏）

もう1つ留意したポイントは、現場目線で取り組み、現場の課題解決にフォーカスしながら進めることだ。実は、リコーが工場セキュリティを推進する統合組織作りに取り組んだのはこれが初めてではなかった。だが、過去のチャレンジはなかなかうまくいかなかったという。「統括組織はルールなどの形で押さえつけがちですが、それでは現場は『我々

の言うことは聞いてくれない』となり、乖離が生まれてしまいます。それをなくそうとしました」（若杉氏）。過去の反省を踏まえ、現場に極力負荷をかけず、かつ技術だけではなく人とプロセスも含めた形で取り組む方針を立てた。

とはいえ、情報セキュリティに関しては経験があるものの、工場セキュリティについてはまったくの白紙からのスタートだ。そこでリコーが独力で進めるのではなく、専門的な知見を持つ第三者にアドバイザーのような形で参画してもらい、客観的なアセスメントを踏まえながらギャップを埋めていくことで、強化を進める方針とした。そのパートナーとして選んだのがフォーティネットだった。

「まずベンダーさん数社に声をかけて各ベンダーが作成したアセスメントシートをいただき、東北事業者での現状を記入し、その結果についてフィードバックしてもらいました」（若杉氏）。

その内容を中心に、技術的なスキルや対応の際のコミュニケーション能力を、統括組織だけでなく東北事業所の現場のメンバーとともに検討し、パートナー候補を二社に絞った。そしてその二社に、実際に東北事業所に足を運び、詳細な課題についてのアセスメントを実施してもらった。試しにフォーティネットの機器を工場の現場に設置し、トラフィックを分析したところ、深刻な事態につながる恐れのあるマルウェアなどは見つからなかったが、「暗号化通信の比率が多いため、どういったデータが含まれているか把握できるようにすべき」といった有益なアドバイスを得ることができた。

現場目線とコミュニケーションを重視しながらファクトリーセキュリティを推進した若杉氏

「フォーティネットを選んだ一番の理由は、コンサルティング能力に優れていたことです。また我々は東北事業所をリファレンス工場とし、国内だけでなくグローバルの工場にも展開しようと考えていました。フォーティネットもグローバルな企業であり、機器の調達や設置、その後の保守といった面でも安心と判断して選定しました」（若杉氏）

「自分たちの工場のセキュリティは自分たちで守る」という意識の浸透を図りつつリードした庄司氏

「自分たちの工場は自分たちで守る」を前提に、人とプロセス、技術にまたがり対策を実践

こうしてリコーでは、フォーティネットと共同で2022年4月からファクトリーセキュリティの向上に向けたプロジェクトを開始した。

フォーティネットが経済産業省のガイドラインをベースに作成したチェックシートでは、組織的対策、運用的対策、技術的対策、サプライチェーン管理といった分野ごとに33項目の質問を行い、企業の取り

組みをAからDの四段階で評価する仕組みとなっている。東北事業所で行った最初のアセスメントではほとんどがC評価となり、ところどころにBもあるがDの箇所もある、といった結果だった。

この結果を踏まえ、「課題はいろいろあるものの、喫緊の課題を解決するために、最初の2022年度は成熟度をCからBに上げることを目標にしました」（若杉氏）。いきなりAを目指すのではなく、全体を底上げして及第点を目指すこととした。

将来的にFSIRTの形に育てていくことを視野に入れ、全体推進はセキュリティ統括センターがリードし、他の工場にも参加してもらった。その下に「ガバナンス」「ルール策定・教育」「技術検討」という3つのワーキンググループを組織し、現場の課題解決に取り組み始めた。

全体を統括側で引っ張りつつも、ワーキンググループのリーダーには工場から人を出した。その理由を庄司氏は、「自分たちの工場のセキュリティは、自分事として自分たちで守るということが前提にあるからです」と語る。わからないところは外部の専門家にアドバイスを求めつつも、あくまで主体は自分たちであるという軸をしっかり持った上で取り組んだ。

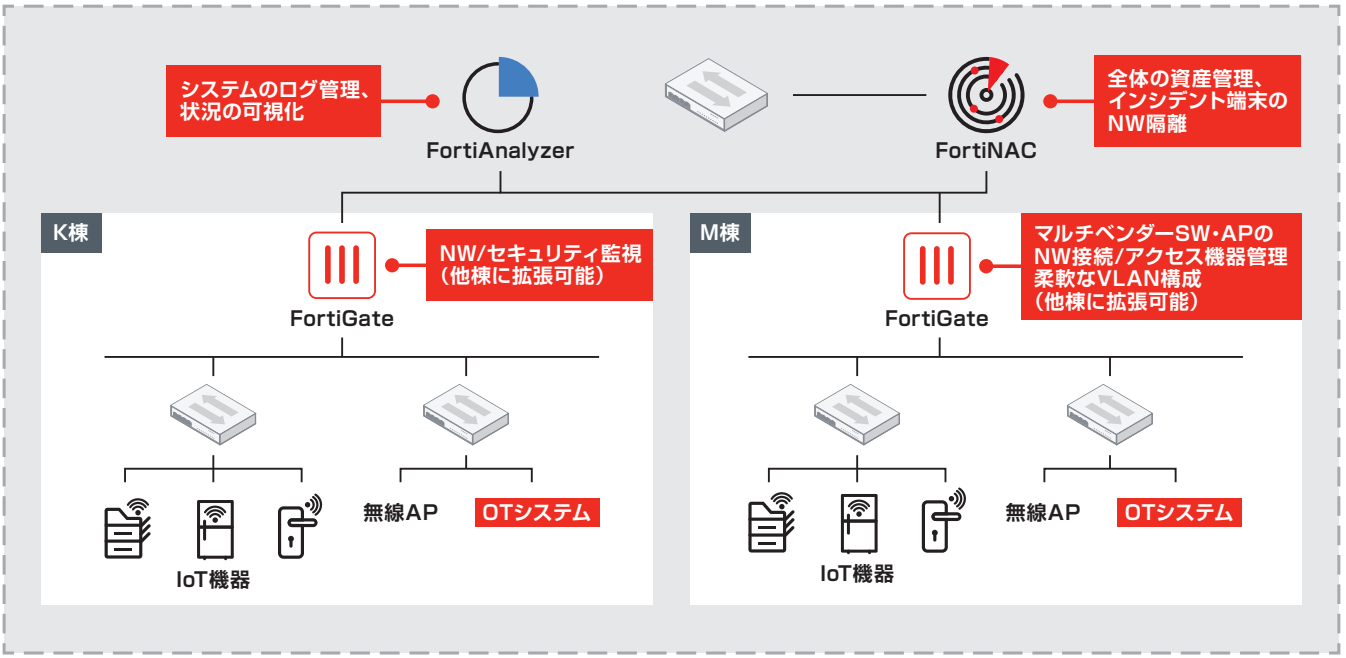
ガバナンスワーキンググループでは、現場の意見も踏まえながらファクトリーセキュリティを推進する組織体制やコミュニケーションパスの再構築などを検討した。またルール策定・教育ワーキンググループは、文字通りセキュリティに関する教育体系やルールの策定に取り組み、文書化していった。

その際に留意したのは、やはり現場主義だ。「リコーインダストリーの社員や外部の協力会社から来ているメンバーはいろいろな教育プログラムを受けています。そこにさらにセキュリティに関する教育を入れ込むとなると、現場は疲弊してしまうでしょう。全体の教育プログラムの中にうまくセキュリティ教育をアドオンすることで、効率的かつ腹落ちしやすい形で理解が進むと考えました」（庄司氏）

具体的には安全教育、いわゆる「5S活動」の中に、セキュリティに関する教育やルールを追加していった。つまりセキュリティも5Sの中に含めることで、現場の負荷にならない形で、無理なく進めている。さらに、工場内の食堂に置かれている情報提供用のモニターに10秒程度の簡単なセキュリティミニ教育コンテンツを流したり、小規模な勉強会を開催するといった形で、プロセスと人の部分を強化していった。

技術検討ワーキンググループでは、ネットワークや端末、ファシリティ、ログ管理などの仕組みについて検討したが、具体的なHowとしてのソリューションから入るのではなく、成熟度をCからBに高めるための要件をまとめてから対策を具体化した。

アセスメントの結果では、同じ東北事業所でも、トナー工場側ではネッ



トワークセグメンテーションが比較的実現できていた一方で、組み立て工場ではOTシステムがネットワークセグメントとして独立しておらず、IT環境と混在していた。この状況を整理するため、ITとOTのセグメンテーションと境界防御を実現する要件を立て、その手段としてFortiGateを導入した。さらにFortiNACを導入してOT全体での資産管理と可視化を行い、万一何かが起きた際にはその端末を隔離できる仕組みを整えた。そして一連のログを統合的に管理するFortiAnalyzerも活用し、全体の流れをしっかり可視化する形としている。

ここまでの取り組みを進めるには、少なくない時間とリソースを要したのも事実だ。ただ、「自分たちの工場のセキュリティは自分たちで守るんだという意識に加え、東北事業所をリファレンス工場として、他の事業所や海外の工場に水平展開するという大きなシナリオを念頭に置き、『自分たちがやって終わりじゃないんだ』ということを皆に意識してもらいました。我々が中途半端なところで妥協してしまったら本当に他の拠点の参考になるのか、自信を持って対策の必要性を他の拠点に対して説得できるのかという観点をメンバーには強く求めました」（庄司氏）

グループ全体を推進する統括側の体制と、工場トップのリーダーシップ、そして現場のやる気。これらがかみ合って東北事業所での対策は進展し、「チェックシートの評価をBに上げる」という最初の目標を達成することができた。上から、あるいは下からの一方向ではなく、双方向でのコミュニケーションが功を奏したと言えるだろう。

「今回の取り組みを推進する中で、東北事業所だけでなく他の事業所からも、いろいろな困りごとや現場の課題を聞かせてもらいました。それらを解決していくうちに、各工場とのコミュニケーションが強化され、結束力が生まれたことがファクトリーセキュリティ推進グループの起点となったととらえています」（若杉氏）

フォーティネットの専門家としてのアドバイスもさまざまな場面で役に立った。コロナ禍の時期ではあったが、定期的に現地に足を運び、現場を見ながら、フェイスツーフェイスで率直に議論を交わしていったという。「現場をよく見た上でともに知恵を出していきたいと思ってスタートしましたが、一年以上こうした形でプロジェクトを進めていただき、うまく化学反応を引き起こしながら解決策を導き、一定のレベルまで達したことに大変感謝しています」（庄司氏）

当初の目標を達成して他工場への展開を開始、事業継続を守る取り組みを今後も推進

フォーティネットのアセスメントでB評価を達成し、全体の底上げに成功した東北事業所。この経験を踏まえ、

同じ事業所内のキーパーツ事業や他の建屋などに水平展開を考えているという。また当初の計画通り、国内外の他工場でも、東北事業所で構築したリファレンスモデルの展開を始めている。すでに3つの工場でフォーティネットによるアセスメントを開始した段階だ。

この作業に統括部門も関わることによって、「自分たちの力である程度アセスメントが行えるよう、フォーティネットのコンサルタントからいろいろ教えてもらいながらスキルを磨いています。また、いったんBという評価を達成しましたが、PDCAサイクルを回して継続的に向上させていく取り組みも必要となるため、工場内にもセルフアセスメントができる人材を育てていこうと考えています」（若杉氏）

リコーグループ全体としては、A評価を追求する前に、まず以前から目標として掲げていたNIST SP800-171準拠を目指し、さらなる成熟度の向上に取り組む計画だ。「今回のアセスメントのベースとなっている経産省のチェックリストとNIST SP800-171、あるいはIEC62443の項目をマッピングし、効率的に国際標準を取得していきたいと考えています」（若杉氏）

東北事業所で培った「People」、「Process」に関するアセットを横展開する一方で、テクノロジに関しては工場の構成や規模によって最適解が異なってくる。そういった面で、引き続きフォーティネットの知見に期待しているという。また、海外工場へのグローバル展開時の調達能力にも期待しているという。

庄司氏は、今回の取り組みを通して、工場のセキュリティ対策とBCPに多くの共通点を感じているとした。東北事業所は2011年の東日本大震災で大きな被害を受けてしまった。もちろん震災前から、耐震補強工事などハード面での備えに加え、事業継続計画を立て、どのように復旧していくかというソフト面での対策も推進していたが、いざ被災してみると意外な盲点が明らかになったという。

「建屋の被害はなかったのですが、復旧プランはすべてパソコンの中に保存していました。震災後一週間停電が続いたため、パソコン内に保存していた計画を読み出すことすらできず、使えませんでした」（庄司氏）。この経験を踏まえ、今では「人命に関わるもの」「安否に関わるもの」はすべて紙にプリントアウトし、アナログで保存するよう徹底している。

震災のような災害は来ない方がいいに決まっているが、残念ながら避けることはできない。同様にサイバー攻撃も、予防し、起きないに越したことはないが被害をゼロにすることは難しい。「サイバー攻撃に遭わないようにする活動も必要ですが、万一被害に遭った際、どうスピーディに復旧させ、お客様に迷惑をかけないよう事業を継続していくかを考える取り組みも必要だと感じています」（庄司氏）。こうした尊い経験も踏まえ、現場の理解を高めながら引き続き工場のセキュリティ対策を推進していく。

FORTINET
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