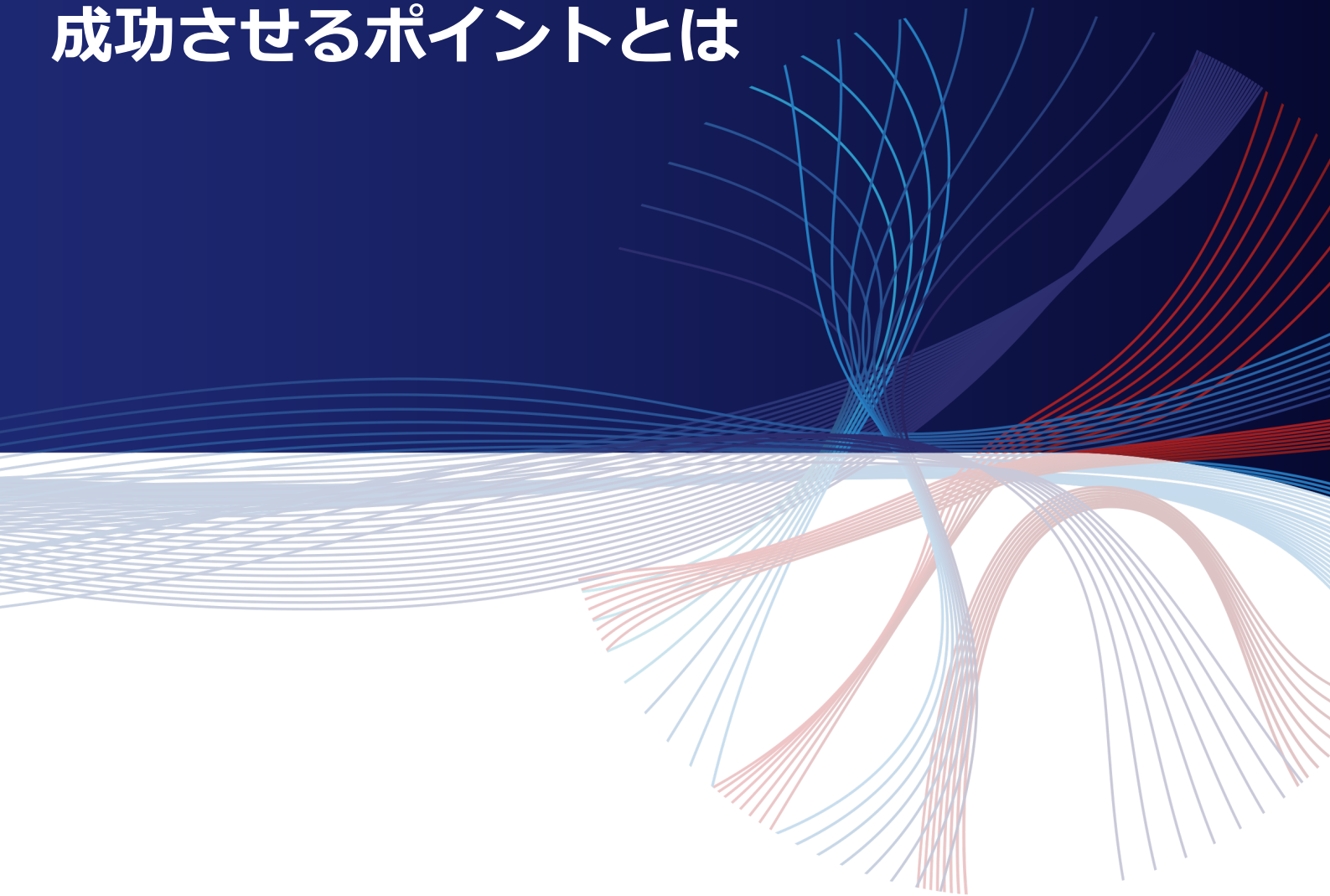
SCADAfence

Technical Whitepaper

制御システム=OT向け セキュリティフレームワークの実装を 成功させるポイントとは



SCADAfence (Japan)
〒103-0023 東京都中央区日本橋3-3-3

Info-jp@scadafence.com
www.scadafence.com/ja

SCADAfence

NISTやIEC62443などはセキュリティフレームワークとして、自社のOT環境の品質向上に向けた取り組み姿勢を外部へ可視化することにつながる。そして、市場やビジネス関係者に対する信頼も増して、自社の価値を向上できる。

一方で、セキュリティフレームワークは全ての組織において万能なアプローチではないと言及していることからも、組織によって異なるリスクがあり、このリスクをマネジメントするために必要な対策を判断し、優先順位を決め、限られたコストの中で費用対効果を最大化することが適切である。

本資料では、OT環境の特性に応じてセキュリティフレームワークを導入し、成功させるポイントについて述べる。

OT向けセキュリティフレームワークを取り巻く状況

OT機器へのセキュリティ対策を考えなければいけなくなったタイミングで、これまで経験が無い管理者がゼロから独自に考えて高コストなわりには脆弱なセキュリティ対策を実施してしまう、といった非効率な活動に陥らないためにも、セキュリティフレームワークの適用は1つの指針として考えられる。本章では、OT環境とセキュリティフレームワークとの関連性や、その特性とメリットについて述べる。

なぜ、セキュリティフレームワークを導入するのか

OT機器セキュリティの必要性が高まる中で、セキュリティポリシーの策定をはじめ運用体制の整備などが求められている。大規模な環境に限らずサプライチェーンを構成する中業規模の環境であっても、サイバー攻撃への明確な対応が求められている。

この際、各社で適切な対策やポリシーを一から作成するのは高度な専門知識を持つ人材の確保などを考えると非常に困難である。そこで有効な手段として挙げられるのが、サイバーセキュリティフレームワークだ。

セキュリティフレームワークの種類

OT機器向けのサイバーセキュリティフレームワークとして、採用が広がっているのは、米国国立標準研究所が発行するNISTや、国際電気標準会議が規格したIEC62443がある。また、米国連邦エネルギー規制委員会から権限委譲された民間団体であるNERCが策定した大規模発電および送電施設を対象向けのNERC CIP、英国国立サイバーセキュリティセンターが策定したサイバー評価フレームワークであるNCSC CAFなどの利用も広まっている。

セキュリティフレームワークに遵守することのメリット

米国では連邦政府が防衛産業以外の全ての調達先に、NISTをガイドラインとして準拠することを要求している。日本では、現時点では防衛省の調達のみで、この基準が採用される段階であるが、米国ほど多くの企業に影響を及ぼす段階ではない。しかし、日本国内の企業もNISTへの対応を求められることが予想される。

また、経済産業省の産業サイバーセキュリティ研究会では、制度・技術・標準化を検討。標準モデルとして、サイバー・フィジカル・セキュリティ対策フレームワークを策定しているが、そのなかで、防衛産業だけでなく、ビル、電力、自動車産業、スマートホームなどの分野にも適用していくことを言及している。

今後は、業界やビジネスパートナーが求めるセキュリティフレームワークに遵守していないと、営業活動や調達の段階で劣位になる可能性も出てくる。

もしセキュリティリスクが内在したまま経営をすることは不利になるが、一方ではセキュリティフレームワークに遵守している度合いが高いと、営業活動で有利に立てて自社の競争力を高めることへつなげられる。

SCADAfence (Japan)
〒103-0023 東京都中央区日本橋3-3-3
Info-jp@scadafence.com
www.scadafence.com/ja

SCADAfence

セキュリティフレームワークをOT環境へ適用する際の課題

セキュリティフレームワークを導入する必要性やメリットを理解できても、OT機器へ適用していくためには、コスト面、技術面、運用面などでの様々な阻害要因が考えられる。本章では、主に製造業界における工場、サプライチェーンを構成する大規模から中小規模の環境の現場におけるセキュリティフレームワークを導入する際の課題を挙げる。

OT資産の棚卸しはデリケートである

これからセキュリティ施策を進める場合、そもそも、自社の工場や生産ラインシステムにおいて、現在、どのようなOT機器が、何台くらい設置されていて、それぞれがどのような役割で連携しているのかを把握できていないケースが一般的である。

というのも、IT機器と比べた場合、OT機器はベンダー独自に開発されていることもり、通信プロトコルも独自で標準化されておらず、カタログレベルの資産情報であっても収集するのが難しいケースが多いからだ。特に、複数ベンダーのOT機器を導入している環境で、それぞれのベンダー独自のプロトコルに対応しながら、これらの機器群を横断して一括で資産情報を整理していくのは困難である。

また、OT機器には、それを管理する制御端末も存在し、そこで最新の資産情報を収集することも可能である。この際、生産ラインシステムの中で稼働中のOT機器へアクセスするような方法だと、誤った操作により、動作中のOT機器が止めてしまったり、高い負荷によって動作を遅延させてしまったりするリスクもありえる。IT機器であれば、セキュリティフレーワークに向けた運用管理の一環として能動的に管理対象へアクセスして情報収集できるかもしれないが、OT機器では生産ラインシステムへの影響をより一層配慮する必要がある。

さらには、スマートファクトリをはじめOT機器がネットワークへ接続するケースが増えていく中で、ネットワーク構成も複雑性がより増している。従来は、工場、生産ラインシステム、作業エリアなどによって、アクセスが制限された閉じられた環境下で利用していたOT機器が外部ネットワークと接続した場合、IPアドレスの重複、ファイアウォールによるアクセス制御や異なる複数のネットワークセグメントの存在などが発生する。これらのネットワーク環境にもとで、資産情報を一括で収集していくためには、どのようにネットワーク経由での情報を収集するのか、収集した後にどのように整理して可視化するのか、といった点で工夫が必要となる。

OT向けセキュリティ対策は優先度が低くなりがち

OT機器が外部のIT業務ネットワークやクラウドとの新しい接続が急速に進められている中で、セキュリティへの影響は明らかである。しかし、OT機器を管理する立場の視点では、サイバーセキュリティが最優先事項として扱われているとは言い難い。

その理由は、新たな業務としてセキュリティ運用へ投入する人員リソースが不足していること、効果的なセキュリティソリューションを配備する専門的な知識が不足していること、実際に発生していない脅威や脆弱性の有力な証拠を示すことが難しいことなど、様々な要因が挙げられる。

もしくは、セキュリティ施策の重要性は理解していても、自社で稼働しているOT機器やネットワーク構成に最適な導入策や運用手順を確立できないケースもある。

特に、一般的なIT機器向けのセキュリティ施策の考え方をそのままOT機器へ適用しようとすると、運用に関わる要件や優先順位が異なるため大きな阻害要因となりえる。

例えば、仮に脆弱性が判明してパッチを適用する必要があった際、IT機器は定期的あるいは計画的なメンテナンスの際に実施するケースが多い。しかし、OT機器は、ベンダー固有の限られた機器でパッチ適用の事前のテストが十分にできない、あるいは稼働中の生産ラインシステムに影響範囲を調査していると迅速な適用が難しいといった理由からパッチ適用のハードルが高い。

そして、OT機器には高い可用性が最優先事項として求められ24時間365日の安定稼働が多いが、IT機器では許容範囲の再起動も許容されないケースが多い。

セキュリティ対策のゴール設定が曖昧になりやすい

セキュリティフレームワークの1つであるNISTは、セキュリティを担保するための考え方に関する記述はあるが、実装していくためのひな形などは提供されていない。そのため、セキュリティ担当者が自社の現状を踏まえて改善していくためには、運用方法の変更、体制強化、セキュリティソリューションの導入などアレンジ力も試されるが身に付けるには時間を要する。

SCADAfence (Japan)
〒103-0023 東京都中央区日本橋3-3-3
Info-jp@scadafence.com
www.scadafence.com/ja

SCADAfence

このように、セキュリティフレームワークでは具体的なセキュリティ対策については定義しておらず、セキュリティに関する指針や管理手法を示すのがメインで、具体的なセキュリティ対策についてはリファレンスとして紹介されている。そして、自分たちの組織に合わせた指針、管理手法やリファレンスを選択する事が重要になる。

この過程では、自社の資産情報や運用から評価を行い、現在の実態を踏まえながら企業・組織の目指すレベルを決めていくが、適切なゴール設定がポイントとなる。必ずしも、上位のレベルを目指すことは必要なく、自社全体、あるいは工場単位、サプライチェーン全体を見据えたあるべき姿・望む姿を想定した上で多角的な検討を行い、関係者間での合意形成を進める必要がある。

ゴール設定は、業種や業態、資産数などの規模感、そしてビジネス要求によって様々である。

例えば、サプライチェーンで代表されるように、現在は単体経営を進めている企業でも、新規事業や事業拡大に挑戦する際に、他社・他組織との事業提携や業務委託の拡大に踏みきる際には、セキュリティフレームワークにおけるサプライチェーンリスクマネジメントの項目に特に注力して対応する必要がある。

また、新たな業界に参入するためにセキュリティフレームワークを取り入れ自社の品質の高さをアピールするには、その業界の慣習に沿って実装する必要がある。あるいは、現在は非上場である企業が、数年後に上場を目指すようなケースでは、上場企業に値する管理体制をセキュリティの観点を含めて、迅速な整備が求められるだろう。

これらの、制約や前提条件が異なる環境のもとで、セキュリティフレームワークを軸にゴールを設定し、スムーズに実装していくのは困難である。

セキュリティフレームワークをOT環境の特性に応じて導入するポイント

セキュリティフレームワークの導入と有効活用に向けては様々な課題があるが、本章では実装に向けた解決策を提示する。ここでは、弊社がこれまでにお客様と一緒に試行錯誤しながら進めた案件や検証の中で培った経験と、今後のOT機器に対するセキュリティ運用のあるべき姿をベースにしている。

適材適所で濃淡を付けてOTの資産情報を収集する

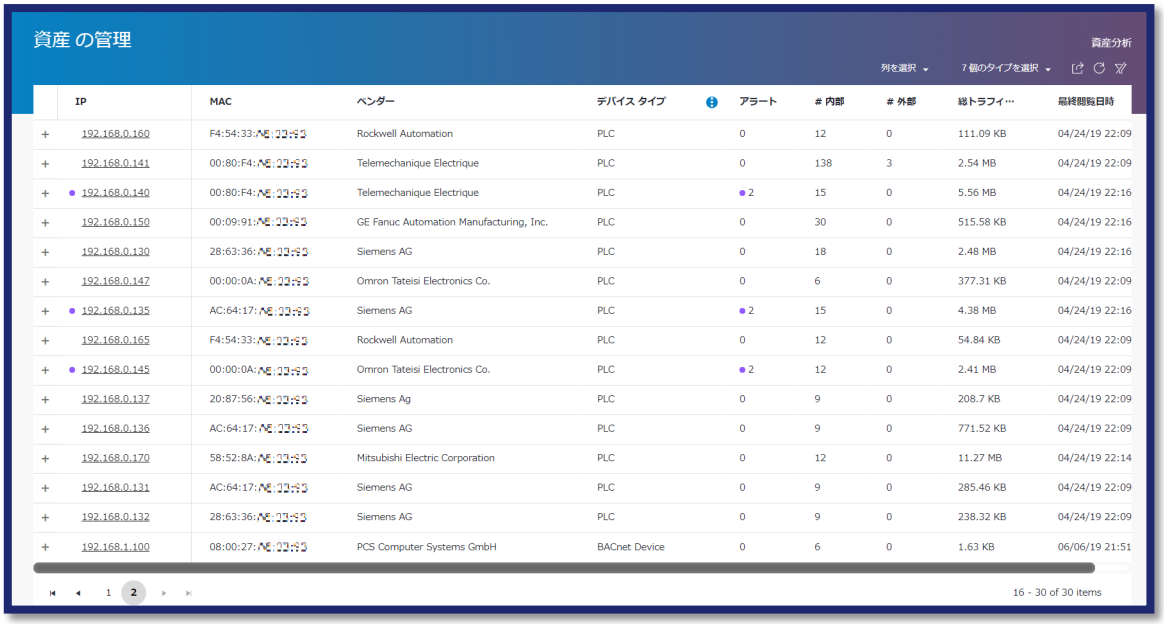
NISTには資産管理の分類があり、例えば「自組織内の物理デバイスとシステムが目録として作成されている。（NIST ID.AM-1）」、「自組織内のソフトウエアプラットフォームとアプリケーションが目録として作成されている。（NIST ID.AM-2）」や「組織内の通信とデータフロー図が作成されている（NIST ID.AM-3）」などのサブカテゴリーで構成されている。

これらを可視化するためには、自社の工場やネットワークに存在するOT機器に関連した資産情報を収集する必要がある。この場合、安全で、網羅性が高く、且つ効率的に実現するためのポイントがある。

１つめは、既存で稼働している工場の生産ラインシステムに影響を与えることなく、安全面に考慮して情報を収集することである。情報収集の観点では、管理ツールから見て能動的に管理対象へアクセスして収集する“アクティブ型”と、管理対象から発行する情報をもとに受動的に収集する“パッシブ型”の2種類に分類できる。IT機器の運用ではアクティブ型が一般的であるが、OT機器では、安全面を考慮してパッシブ型を軸に採用を検討する。パッシブ型の代表的な手法としては、パケットキャプチャが挙げられる。ただし、この場合、管理対象から情報が発行されない限りは収集できないため、ネットワークには接続していても動作していない保守用の機器や、冗長構成における待機系の機器の資産情報は収集できないかもしれない。そのため、未稼働で生産ラインシステムへの影響が少なく、且つ、管理情報を発行しない機器に対してはアクティブ型で情報を収集することもオプションとして検討する。アクティブ型としては、OT機器ベンダー固有の管理プロトコルや、IT運用で利用ケースが多いSNMPが挙げられる。これらのパッシブ型をベースに、必要に応じてアクティブ型の採用も補足機能として視野に入れると、安全で網羅性の高い資産を収集できる。

２つめは、OT機器群の多様性で複雑なネットワーク構成への対応である。従来はネットワークにつなげていなかったOT機器群をネットワーク化したすると、各ネットワークセグメントには数台程度のOT機器が属する一方で、ネットワークセグメントが多数存在するケースが一般的だ。その場合、ネットワーク全体では、IPアドレスが重複していたり、パッシブ型やアクティブ型だと出入口に設定されているファイアウォールを超えて情報を収集できなかったり、一筋縄では情報収集できない。この場合、それぞれのネットワークセグメントにパッシブ型で情報を収集するためのセンサーを設置する。しかし、センサーの導入コストや運用コストが増大する懸念も考えられる。もしくは、各ネットワークセグメントに設置されているネットワーク機器がNetFlowのような管理情報を収集し管理ツールへ転送できる機能を搭載していれば、センサーのような追加のハードウエアは不要で、既存の環境を活用しながら資産情報を収集できるケースがある。IPアドレスの重複に対しては、ネットワーク全体の情報を収集したのち、ネットワークセグメントごとにIPアドレスを識別する仕組みも必要となる。

上記のポイントを配慮しながら、第一段階としては、パッシブ型で収集したOT機器の情報をもとにセキュリティフレームワークと照合することで、遵守の度合いが明確になる。第二段階として、アクティブ型の情報収集方式の採用、センサーの設置やNetFlowの活用を取り入れることで、情報収集できない機器を対象に含めたり、あるいは収集するネットワークの範囲を拡大したりすることによって、網羅性を高めることにつながっていく。



稼働機器/設備資産：一覧（SCADAfence Platform）

SCADAfence (Japan)
〒103-0023 東京都中央区日本橋3-3-3
Info-jp@scadafence.com
www.scadafence.com/ja

SCADAfence

稼働機器/設備資産：個別詳細（SCADAfence Platform）

OTの現場に即したベストプラクティスを運用の基盤にする

NISTには異常とイベントの分類があり、例えば「ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。（DE.CM-1）」、「悪質なコードは、検知されている。（DE.CM-4）」や「権限のない人員、接続、デバイス、ソフトウエアのモニタリングが実施されている。（DE.CM-7）」などのサブカテゴリーで構成されている。

これらをOT機器の脆弱性として検知するためには、機器ベンダーごとに多様に存在する独自プロトコルを解釈し、且つ、事前に登録した脆弱性情報とのパターンマッチングがポイントとなる。

代表的な独自プロトコルは、Modbus、Omron FINS、Siemens S7、EtherNet/IPやMoxaをはじめ多種多様あるが、工場や生産ラインシステムの目的や用途に応じて複数使われているケースも多い。そして、これらのOT機器どうしがやり取りする通信内容をパッシブ型などの情報を収集して解読する。一般的なIT運用ツールでも独自プロトコルのパケットを収集できるが、通信内容を解読することは困難だ。

脆弱性情報とのパターンマッチングによる検知では、例えば、BlackEnergy、IndustroyerやUrgent11などの産業業界での攻撃パターンを把握しておくことでセキュリティ問題を未然に防ぐことにつながる。さらには、OT機器に対する停止コマンドやプログラム変更コマンドなど通常は実行されない操作コマンドなどにも気付く必要がある。また、未確認の外部の機器へアクセスや、インターネットなどの外部ネットワークとの不要な通信など、疑わしい通信を検知することも重要である。

そして、脆弱性を検知した際には、ファームウェアへのパッチ適用やバージョンアップをはじめ、通信の遮断などの対処にもつなげる必要がある。工場や生産ラインシステムでは、OT機器のアップグレードは緊急停止にもつながり稼働率の低下を招きビジネスインパクトが大きいため、実際には現場で随時対処を検討していく必要があるだろう。

これらの仕組みを取り入れることがセキュリティフレームワークの実装にもつながる。しかし、OT機器向けのセキュリティに対する優先度が低い、セキュリティ運用へ投入する人員が不足している、あるいは専門的な知識が不足していると、ゼロから構築していくのは容易ではない。

この場合、これらの仕組みを導入するにはベストプラクティスを既に搭載したソリューションを取り入れるほうが効率的だ。自社の環境で導入されているOT機器ベンダーが採用している独自プロトコルの解釈が出来ること、自社の業種や業界の特性に応じた攻撃パターンの検知、そしてOT機器に対するセキュリティ運用が初心者であっても使いやすい操作性といった点を考慮してソリューションを選択することが肝要だ。

パターンマッチングによって検知したアラート一覧（SCADAfence Platform）

SCADAfence (Japan)
〒103-0023 東京都中央区日本橋3-3-3
Info-jp@scadafence.com
www.scadafence.com/ja

SCADAfence

パターンマッチングによって検知したアラート詳細（SCADAfence Platform）

まずは部分的にセキュリティフレームワークを採用してみる

NISTでは、どの程度セキュリティ対策を達成できているかを定量的に計測するために、「部分的である」、「リスク情報を活用している」、「繰り返し適用可能である」と「適応している」の4段階を定義し、成熟度評価基準を設けている。

今すぐに適切なゴール設定が難しい場合は、まずは第一段階である「部分的である」を目指すことがOT機器のセキュリティ対策の初手につながる。必ずしも、セキュリティフレームワークにおける全項目で完璧に第四段階を目指す必要も無い。また、生産ラインシステム、工場、拠点、サプライチェーン全体など適用範囲ごとに異なる成熟度合いをゴール設定にしても構わない。組織のビジネス要件、セキュリティリスクの許容度合い、セキュリティ運用に費やせるリソースやコストなどにも配慮しながらゴール設定を定めることがポイントとなる。

このようなきめ細かく柔軟なゴール設定を施すためには、OT機器から収集した資産情報や検知した脆弱性情報をグループ化できること、それぞれのグループに対してセキュリティフレームワークの項目を適用できること、適用したグループごとにセキュリティフレームワークの成熟度合いを指定できることなどが仕組みのベースとなる。

仕組みに加えて、その自動化も必要だ。採用するセキュリティフレームワークの種類や項目範囲にも依存するが、数百から数千件あるセキュリティ要件に対して、グループ分けした対象への適合性の確認作業は高コストであり、人手では照合が困難である。セキュリティソリューションを導入する場合には、自動的な情報収集、グループごとの分類、定義した成熟度合いに応じてセキュリティフレームワークを照合してレポート化できる機能を搭載したものを取り入れると、設定したゴールへの到達度をダッシュボードで把握して管理できる。

システムによる自動計測：フレームワーク要件ごとの設定（SCADAfence Platform）

システムによる自動計測：拠点ごとの達成度合い（SCADAfence Platform）

SCADAfence (Japan)
〒103-0023 東京都中央区日本橋3-3-3
Info-jp@scadafence.com
www.scadafence.com/ja

SCADAfence

まとめ

本資料では、OT向けセキュリティフレームワークを成功させるポイントとして、“適材適所で濃淡を付けてOTの資産情報を収集する”、“OTの現場に即したベストプラクティスを運用の基盤にする”と“まずは部分的にセキュリティフレームワークを採用してみる”の3つを提示した。

これらの3つのポイントを踏まえながらNISTやIEC62443を迅速に取り入れ、そして、導入後は、その成果を定期的に見直していくことで、これまで曖昧だったセキュリティ施策のレベル感が明確になるとともに、外部のビジネス関係者との同じ物差しで会話できると考えている。

限られたセキュリティ予算の中で、セキュリティフレームワークを導入しメンテナンスしていくのは所要時間や費用の負担も大きく、企業としては意思決定も難しいが、本資料が少しでもお役に立てれば幸いである。

筆者紹介：
梅根 庸一：SCADAfence (Japan) シニアソリューションコンサルタント。
Hewlett-Packard社でITエンジニアとしてのキャリアをスタートさせ、インフラ、ネットワーク、仮想環境、クラウド、ユーザーエクスペリエンスなど、時代の変化に沿った監視ソリューションの提案、設計や開発に 一貫して携わってきた。現在は、産業分野のサイバーセキュリティ対策を担当し、セキュリティ責任者、産業機器エンジニア、IT運用オペレーター、ネットワーク担当者といった異なる価値観の視座に立った提案をモットーにしている。国内の産業とセキュリティの 2 つの分野が重なる領域を活性化させ、スマートファクトリやスマートシティの促進をセキュリティ面で下支えするべく、日々、奮闘を続けている。

SCADAfenceについて

SCADAfence は、大規模な産業ネットワーク（OT ネットワーク）をもつ様々な企業が、その運用からサイバーリスクを軽減し、運用健全性を向上させることで、企業の IoT/デジタルトランスフォーメーションの推進を支援します。SCADAfence のパッシブ型プラットフォームは、大規模なネットワーク全体をカバーし、クラス最高レベルの検出精度と、機器・通信の特定及び可視化を行い、ハイレベルなユーザエクスペリエンスを提供します。SCADAfence は OT セキュリティの機能を既存のセキュリティ運用へシームレスに連携し、IT/OT の融合を促進させます。SCADAfence は、ヨーロッパ最大の製造工場を含む、世界でもっとも複雑な産業ネットワークに高度なセキュリティと運用健全性を担保する機能を提供し、製造・ビルマネジメント及び社会インフラの分野における安全かつ効率的なデジタルトランスフォーメーション推進を支援します。詳細は https://www.scadafence.com/ja をご覧ください。