

デジタル化する工場のサイバーセキュリティ

工場(OT)環境におけるセキュリティアーキテクチャのリファレンスモデル化の重要性

PwCコンサルティング合同会社 シニアマネージャー 上村 益永
PwCコンサルティング合同会社 マネージャー 大貫 経介



1. OT環境のセキュリティ対策が急務

OT(Operational Technology:生産ラインやシステムの制御・運用技術)環境へのサイバー攻撃による被害が顕著になりつつある今日、日本国内に留まらず、海外も含めた工場へのセキュリティ対策が急務です。しかし、工場の数が多く、かつ事業の異なる工場を持つ企業がセキュリティ対策を早く確実に実装することは容易ではありません。本稿では、この課題を解決するための重要施策として、セキュリティアーキテクチャの実装・運用におけるリファレンスモデルの活用を紹介します。

2. OTセキュリティに求められるもの

OT環境にセキュリティアーキテクチャを実装する際、まずは企業に存在する制約条件を認識することが重要です。以下に代表的な例を挙げます。

制約条件

一つ目:工場の機能要件を優先する必要がある

工場では、組み込み系のシステムに使用されているレガシーOS上でしか動作しないソフトウェアを使用し続けることがあります。事業を営む上でそのソフトウェアの使用を優先せざるを得ず、OSのアップグレードができないといった側面があるのです。加えて、製品の生産性を重視するため、費用対効果の観点でセキュリティ専任の人員を各工場に常駐させることが困難となることも、こうした制約を生む要因です。

二つ目:生産に影響を与えることができない

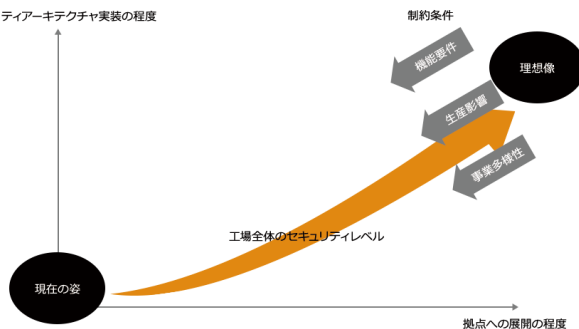
企業の多くは製品を生産・加工するために工場を稼働させています。このことから、セキュリティアーキテクチャの実装により、工場の稼働を遅延、停止することは避ける必要があります。

三つ目:工場ごとに事業や規模が異なる

企業の多くは生産効率や人件費削減などの理由から、国内外に複数の工場を持っています。そして、その規模や事業内容、ロケーションは各々異なります。つまり、特定の工場だけにセキュリティアーキテクチャを実装して終わりではなく、工場全体に実装していくことを考慮した設計や実装が求められるのです。

こうした工場が持つ制約条件を考慮した上で、機能要件を満たしつつ、国内外の複数工場を対象にOTセキュリティ水準を向上させるという複合的な取り組みが求められます。セキュリティインシデントが発生した場合の包括的かつ迅速な対応も重要な要件となります。

図表1: OTセキュリティの理想像と制約条件の関係
セキュリティアーキテクチャ実装の程度



3. リファレンスモデル化による恩恵

OT環境特有の制約条件下、セキュリティアーキテクチャを実装するには、膨大な期間とコスト、運用負荷がかかることが想定されます。そこで、セキュリティアーキテクチャの設計と実装をリファレンスモデル化することで、工場の特徴に応じて柔軟に設計・実装をすることが可能になります。以下にリファレンスモデル化による主な恩恵を記します。

■ セキュリティ品質の安定化

リファレンスモデルを活用することで設計や実装が一定レベルで共通化されるため、工場の規模の大小や事業の特徴に関わらず、セキュリティの品質が安定します。

■ コスト削減

毎回個別に設計や実装をする必要がないため、これまで工場ごとの個別設計・実装に要したコストを削減できます。

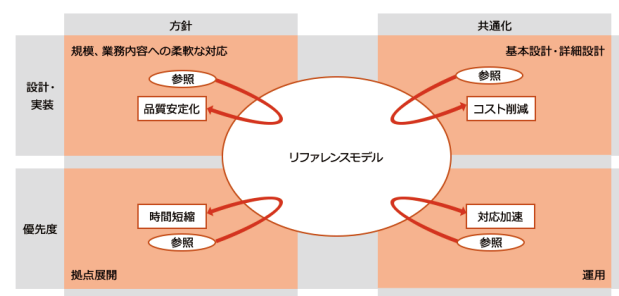
■ 時間短縮

前述の通り、個別に設計や実装をする必要がないため、セキュリティアーキテクチャ実装のスピードアップにつながります。

■ レスポンスの迅速化

設計や実装を共通化しておくことで、セキュリティアーキテクチャ実装後の運用も工場全体で共通化することが可能になります。万が一、複数の工場でインシデントが発生した場合でも、リファレンスモデルをベースに共通認識を持った状態で工場間のコミュニケーションができるため、被害が発生している端末の情報から類似端末を特定したり、必要な対応をとったりしやすくなります。

図表2: リファレンスモデルが達成すべき要件と恩恵



4. リファレンスモデルが達成すべき要件

では最後に、セキュリティアーキテクチャをリファレンスモデル化するための要件について考えてみましょう。

■ 規模や業務内容に縛られない設計・実装方針

各工場の規模や業務内容によって設計・実装方針が変わってしまうと、工場ごとに作業の重複が発生してしまい、セキュリティアーキテクチャの品質が安定しません。そのため、規模や業務内容などに縛られない設計・実装方針であることが求められます。

■ 基本設計と詳細設計の区分け

一方、リファレンスモデルで全てを共通化してしまうと、実装が上手くいかない工場が出てくる可能性があります。そのため、基本設計までを共通化し、工場の特性を考慮して詳細設計できるようにしておくことが望ましいです。これにより、工場全体の設計と実装の品質を安定させた状態で、コストの削減や期間の短縮が可能になります。

■ 実装の優先度を決める判断基準の明確化

工場が多ければ多いほどリファレンスモデルが有効性を発揮しますが、闇雲に工場全体への実装を進めても非効率になってしまいます。長期的な目線で工場への展開にレバレッジをかけるために、工場の規模や業務内容などを判断要素とし、どの工場に展開していくべきかの優先度を決めるための判断基準を持つことが求められます。

■ 根幹となる運用の共通化

実装後の運用について考えてみると、もちろん枝葉の運用は工場によって差異はありますが、根幹となる運用は共通化しておく必要があります。インシデント発生時の被害拡大を防止することを想定して、有事の際はネットワークを分断できるようにしておき、生産を停止しないことや守るべき資産を守るような態勢を構築することが必要です。つまり、セキュリティアーキテクチャの設計・実装にあたり、優先度に基づいたインシデント対応ができるよう考慮しておくことが重要になります。

多くの企業が日本国内外に工場を持つ一方、工場へのセキュリティ人員の配置や設計・実装に費やすことができるリソースは限られています。このような中で工場全体へセキュリティを浸透させていくためには、セキュリティアーキテクチャのリファレンスモデル化が有益です。

お問い合わせ

PwCコンサルティング合同会社
〒100-6921 東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel : 03-6250-1200(代表) Mail : jp_cyber_inquiry@pwc.com