L-005

IoT セキュリティ成熟度モデルの サイバー・フィジカル連携型セキュリティ基盤への適用

A Study on Applying IoT Security Maturity Model to Digital Twin-Assisted Security Platform for Cyber-Physical Systems

杉山 敬三†
Keizo Sugiyama

1. はじめに

筆者らは、デジタルツイン(DT)を用いて、サイバー攻撃のフィジカル空間への影響を評価しセキュリティ対策を行うサイバー・フィジカル連携型セキュリティ対策基盤[1]を提案している。本基盤は、複合施設などのエリアにおいてモビリティや人流管理などの目的に応じて構築される DT(以降、サービス DT)のセキュリティ強化を目的としており、各種サービス DT 群と連携してセキュリティ対策を行う DT(以降、近傍 SDT)、及び、セキュリティ DT 広域連携プラットフォーム(以降、SDTPF)から構成される。しかしながら基盤自体が攻撃を受ける可能性があるため、基盤のセキュリティレベルを向上させる必要がある。

セキュリティに関して自己評価を行うためのガイドラインとして、セキュリティ成熟度モデル(SMM ： Security Maturity Model)が存在する。本稿では、IoT SMM デジタルツイン・プロファイル[2]を参照し、本基盤のセキュリティ成熟度の目標レベルと実施項目について検討する。

2. IoT セキュリティ成熟度モデル(SMM)の概要

成熟度モデルは元々ソフトウェア開発とプロセス改善の文脈で開発された概念であるが、セキュリティ分野を含む様々な領域へ拡張された結果、セキュリティプロセスの成熟度を評価するための各種 SMM が開発されている。

2.1 SMM

SMM は、組織がセキュリティ機能を評価して理想とするモデルとのギャップを明確にし、投資の優先順位を決めるために利用されることを想定している。成熟度を決定するのは、セキュリティメカニズムの強度ではなく、目標に対する適切さである。システムの成熟度の進捗は、①セキュリティ対策の深さや一貫性、および保証の度合いである包括(Comprehensiveness)レベル、②業界やシステムのニーズに対する適合度であるスコープ、の 2 軸を考慮して評価し、関連する実施項目の優先度付けを行う。SMM に関する具体的な規定やフレームワークは複数の組織や標準化団体により提供されている。

2.2 IoT SMM

2.2.1 IoT SMM の概要

IIC(Industrial IoT Consortium)は 2019 年に、IoT システムに必要なセキュリティ成熟度の目標レベルを設定できるよう IoT SMM を公開した。IoT SMM は、図 1 に示すように、①ガバナンス(Governance ： 戦略に相当)、②有効化(Enablement ： 計画に相当)、③強化(Hardening ： 戦術に相当)、の 3 つの領域とそのサブ領域、18 のプラクティス(実施項目)を階層的に設定している。また、成熟度は 1(最小限)から 4(形式化されている)の 4 レベルとしている。

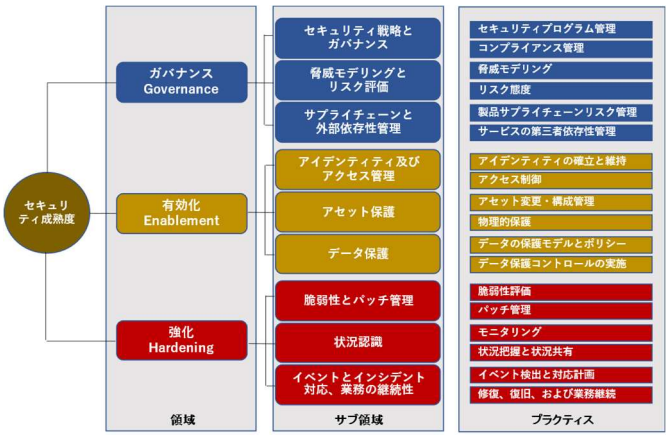

図 1　IoT SMM の階層構造

2.2.2 IoT SMM デジタルツイン・プロファイル

IIC と DTC(Digital Twin Consortium)は 2022 年に、IoT SMM デジタルツイン・プロファイルを発表した。同プロファイルは、IoT SMM において DT 技術を使用するシステムやプロジェクトに焦点を当てたものである。DT では特に、実世界のアセットに対する仮想表現の忠実度と、時間経過に伴い表現の完全性を維持する能力が課題となる。DT システムのスコープにおいて、全プラクティスに共通する考慮事項を、包括レベル毎に表 1 に示す。

3. サイバー・フィジカル連携型セキュリティ基盤への IoT SMM の適用

ここでは、表 1 に示した包括レベルのうちレベル 3 を目標とし、図 1 に示したプラクティスの中で、システム設計や運用の観点で特に考慮すべき実施項目を取り挙げる。

3.1 ガバナンス領域

3.1.1 脅威モデリング

脅威モデリングでは、システムの機能を危険にさらす可能性のある既知の特定の要素を明確化する。

本基盤における脅威モデリングでは、フィジカル空間の各種デバイス、サイバー空間のサービス DT、近傍 SDT、SDTPF を対象に攻撃者を想定する。デバイスへの物理攻撃や制御システムなどを標的とした敵対的攻撃も対象とし、攻撃による影響が他システムや他空間に波及する場合も含め、CCDS-STRIDE モデル[3]などの手法を用いてシステム横断的に脅威を特定する。特定された脅威は継続的にカタログ化・優先順位付けを行い、近傍 SDT におけるリスク分析やシミュレーションに利用する。

†株式会社 KDDI 総合研究所　KDDI Research, Inc.

表 1　IoT SMM デジタルツイン・プロファイルの包括レベルと共通的な考慮事項

包括 レベル 1(最小限)	包括 レベル 2(アドホック)	包括レベル 3(一貫している)	包括 レベル 4(形式化されている)
DT モデルは、組織において低影響で非クリティカルなユースケースのみに使用	DT モデルは、組織において低インパクトまたは中程度のインパクトのユースケースにのみ使用	DT モデルは、組織への影響が大きいユースケースに使用	異なる DT 間の相互作用が理解・考慮されているユースケースに使用
同じ組織内で DT とアセットの両方を持つシンプルな DT の実装	同じ組織内で一貫したタイプの複数の DT とアセットを持つ、やや複雑な DT の実装	異なるタイプの複数の DT を持つ、より複雑な DT の実装	組織間で様々に連携した DT を持つ、複雑な DT の実装
DT の信頼性はアセットに対し低くても問題なく、DT・アセット間の同期頻度を高くする必要はない	DT とアセットの関連性は高くする必要があるが、頻繁な更新は必要ない	DT とアセットの関連性は高く保ち、適切な頻度で更新する必要がある	アセットに対する DT の忠実度は重要な側面であり、更新頻度は高くなければならない
本レベルを達成するために実施すべき項目			
組織は、自身のニーズ、システム、または組織にあわせてカスタマイズされていない、既製のセキュリティ対策を使用	組織は、DT モデルの使用に伴うリスクを考慮し、アセット OT とデジタルツイン IT のセキュリティを別々に考慮	組織は、他組織のデータ使用時のデータリスクを考慮して組織間でのアクセス制御を管理し、異なる DT 間の関係や異なるベンダによる実装を考慮	組織は、自身のポリシーと手順の設計時に他組織のセキュリティ遵守に対する影響を常に考慮し、セキュリティポリシーと手順を定期的に見直し
達成の指標			
IT の実施項目は文書化され、アセットと DT に別々に適用	・静的なシステムレベルのセキュリティ要件を実装 ・アセットの物理セキュリティはサイバーセキュリティとは別に管理	・組織間の静的なセキュリティ要件を実装 ・種類の異なる DT に対し別々のセキュリティプランを所有	積極的に進化または変化する組織間のセキュリティ要件とそのポリシーおよび手順の実装

3.2 有効化領域

3.2.1 アイデンティティの確立と維持

アイデンティティの確立と維持は、システムにアクセス可能なエンティティの特定とその権限の制約に寄与する。

本基盤は B5G スライスの利用を想定しており、デバイスの認証・認可に SIM を利用する。SIM を具備しないデバイスではゲートウェイ(GW)の SIM を活用し、DT に接続する際には同 GW をプロキシとして機能させる。

3.2.2 アクセス制御

アクセス制御では、リソースへのアクセスを、必要なアイデンティティやレベルに限定する。

サービス DT、近傍 SDT、SDTPF はブローカに基づく分散システムを想定[1]しており、各システムに期待される役割に基づいて共有リソースへのアクセスを柔軟に制限できるよう、ロールベースのアクセス制御を用いる。例えば、サービス DT の共有リソースに対し、他のサービス DT は読み取りのみ、近傍 SDT は書き込みも可能とするようロールを設定する。また、マルチテナントのシステムの場合、ネットワークレベルだけでなく名前空間の分離や、適切なデータベースロールの設定等により、リソースを隔離する。

3.2.3 アセット変更・構成管理

アセット変更・構成管理では、アセットに対して許可される変更の種類と変更時期、承認プロセス等を制限する。

構成変更を行う際には、該当エンティティだけでなく関連する DT やデバイスへの影響も考慮する。例えば、異常が検知されたデバイスを切り離す場合、デバイスとサービス DT の該当オブジェクトとの同期を停止するのに加え、関連するオブジェクトや属性に対する CRUD 操作により不正確なデータの伝播を防ぎ一貫性を維持する。

3.2.4 物理的保護

物理的保護は、施設等の物理的なセキュリティと安全性を対象に、デバイスの安全な運用の継続を保証する。

デバイスへのアクセス権は当該デバイスに対応するサービス DT の管理主体にのみ付与し、デバイスのなりすましやデータ改ざんを防止するための物理的保護機能に加え、セキュリティ監視機能と連携させるためのログ収集機能を設ける。サービス DT では、デバイスの状態と環境をリアルタイムで監視し、脅威モデリングで特定された物理的脅威を元に異常な挙動を検知する。

3.3 強化領域

3.3.1 脆弱性評価

脆弱性評価は、脆弱性を特定して組織に与えるリスクを決定し、復旧計画の優先度付けに寄与する。

デバイスの脆弱性評価では、物理的な位置や移動の影響を考慮して評価を行う。例えばモビリティの場合、公共空間(道路など)、準公共空間(複合施設内の通路など)、特定空間(店舗内など)で物理的セキュリティやネットワーク環境が異なり、アタックサーフェスが変化する可能性がある。SDTPF には種々の脅威情報や脆弱性情報が蓄積されるため、本基盤自体の脆弱性評価にも活用する。

3.3.2 モニタリング

モニタリングは、システムの状態を監視して異常を特定し、問題解決を支援するために使用する。

近傍 SDT では、SDTPF の保持する広域の脅威観測情報だけでなく、広域でのデバイスプロファイリングなどの手法も適用して、エリア近傍での異常検知や分析を行う。また、分散システム全体として対処・復旧を行うため、異なる管理主体のイベントを突合しその関係性や相関を判断する仕組みや、データのライフサイクルに渡ったトレースの仕組みを設ける。

4. おわりに

筆者らが提案するサイバー・フィジカル連携型セキュリティ対策基盤において、IoT SMM デジタルツイン・プロファイルの包括レベル目標を 3 に設定し、同基盤の設計時における実施項目レベルでの留意点を整理した。

謝辞

本研究成果は、国立研究開発法人情報通信研究機構（NICT）の委託研究（JPJ012368C08101）により得られたものです。

参考文献

[1] 杉山他, ”サイバー・フィジカル連携型セキュリティ基盤におけるデータ連携機能の基本設計”, 第 86 回情処全大, 4D-05(2024).
[2] Geater et al., “IoT Security Maturity Model Digital Twin Profile”, An IIC and DTC Whitepaper (2022).
[3] CCDS,” IoT 機器に対するリスク分析のガイド”, https://ccds.or.jp/certification/document/ccds_risk-analysis-process.pdf