1. IoT セキュリティ・セーフィティ・フレームワークのパブリックコメント(案)

全体的な印象として、セーフティ観点(安全性)に対する分析方法や基準などが抜けている印象である。また、第1層と第3層との関連性が見えないため、第2層のセキュリティ・セーフティの定義に漏れがあるように思える。フィジカル・サイバー空間を正確に転写する機能の信頼性だけをフォーカスするだけでなく、対象機器のとなるサプライチェーンや安全性の要求、セキュリティゴールを明確にできるフレームワークにならないと全体的なフレームワークとして成り立たないように思える。 リファレンスとするアーキテクチャの定義が明確にないため、IoTのリファレンスアーキテクチャを明確にすることが必要と考える。NISTのベースラインを参考としていると考えるが、目的、目標とする部分を明確にする必要があると考える。

抽象度の高いフレームワークであり、中身についてはこれからユースケースを集めて有用性を高めていくとのことであるが、ユースケースの具体的な記述方法が提案されていないので、活用可能性が見こない。ユースケースの共有はどのようにしてすすめるかなど、各企業や各団体との連携方法なども定義が必要に思える。

第1軸にて「回復困難性の度合い」の概念が抽象化し過ぎているため、フィジカル空間に対することと、サイバー空間に対することとが一まとめにされており、各々の空間で軸を分けた軸の定義を行い、安全性の要求とセキュリティゴールについての定義を細分化することが必要と考える。この部分は、フィジカル空間を生み出すための第1層との関係性が重要な要素と思える。

「経済的影響の度合い」においては、モノを作る部分、モノを動かす部分、モノを運用する部分の３つの視点でサプライチェーンを見える化し、サプライチェーンにおけるリスク分析を実施するべきと考える。金銭的換算においては、事例が必要となるが事例や定義をどのように定義していくのか？の指針の定義が欲しいと考える。

「セキュリティ・セーフティ要求の観点」では、4層に分けられている。その他、社会的なサポート等については、「セキュリティ・セーフティ要求の観点」を包括するような位置づけと考えられ、何故この部分が必要になるのかを説明するべきと考える。もしくは、層の構成上、認定レベルなどを設けて、コスト資産した後に対応する位置づけにする必要があるように思える。

「セキュリティ・セーフティ要求の観点」においては、運用前の部分と運用中の部分の関係性の明確化が必要に思える。通常、機能安全においても、セキュリティ設計においても、リスク分析を行う場合に想定されるユースケースから、被害や事故、損失を分析した上で、事象に対する対策を想定し、検討する事が一般的である。運用するシステムの想定が曖昧であり、利用・運用のユースケースの洗い出しがあって、運用前の確認要求となるような層の定義が必要に思える。セキュリティの場合、悪意ある第三者からの攻撃によって新たなインシデントが発生することも考えられ、運用時の対応に関しての定義が必要に思える。

運用者に対する確認要求については、サービスを提供する人なのか？オペレータなのか？どちらを想定しているのかが明確に見えない。また、運用中の部分から運用者を特に外している理由が明確でないため、定義が曖昧なように見える。305-308に記載された部分として、使用者の定義があるが、使用者と想定しているのは、サービス利用者なのか？サービス提供者なのか？が明確になっていないと思われる。

「セキュリティ・セーフティ要求の観点」部分で最も抽象的となっている部分として、想定ユーザや想定ケースが抜けている点である。運用前の部分については、製造メーカーを想定していると思われるが、運用中の部分は、製造メーカーでないケースが想定されるため、運用中の部分がどのようなサプライチェーンであるかを明確にし、運用ケースの定義が必要と考える。

誤解を避けるために“セーフティの確保”の”セーフティ”が“セキュリティ・セーフティ”の意味であれば“セキュリティ・セーフティ”にしてほしい。（工場、社会インフラ等の安全の意味であれば“安全”とすべきと考える。）

"フィジカル・サイバー間をつなげる機器・システムのカテゴライズ"とありますが、機器、システムの粒度を明確にしないとカテゴライズを明確にするべきだと考える。

2. 以下、コメントを検討するための分析内容

2.1. 本フレームワークの必要性

2.1.1. -1-1 CPSF概論

第1層、第2層、第3層の信頼性の基点においては、各層内の信頼性と各層間の信頼性のどのように証明するのか？の概論がないと第2層における信頼性の基点が定義できないのではないか？

2.1.2. -1-2 第2層の位置づけ

セキュリティとセーフティの関係や検討に対する検討内容が明確になっていない。この定義では、セーフティの確保が大前提としており、機能安全の観点からの対策やサイバーセキュリティ対策を組み合わせてた対応が必要となるが、具体例必要に思える。

IoT機器のセーフティ・セキュリティの対策において、転写する機能の信頼性確保に焦点があるが、フィジカルな機器のセーフティ・セキュリティとデータに対するセーフティ・セキュリティに対する信頼性(堅牢性)を定義するべきなのではと思われる。

2.2. 本フレームワークの想定読者

想定読者が明確でない。Sevicer、Developer、Mantiner、Userと示すべきと考える。

2.3. . 本フレームワークの基本構成

2.3.1. -2 フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理

機能安全の安全性から考えた場合、人命/身体の確保が重要な要素。セキュリティの場合は、資産(プラバシーなど)が重要な要素。この 2 つの視点を明確にするべきと考える。
機能安全、セキュリティ分析においても、最初の被害分析部分は、類似している。しかしながら、実際に起きる事故の原因が異なると思われるので、同一なフレームで検討するのは難しいと考える。

2.3.2. -2-1 第1軸：発生したインシデントの影響回復困難性の度合い

限定的なダメージ、重大なダメージ、致命的なダメージの 3 つの度合で計ることとなっているが、セキュリティ観点で考えた場合、情報漏洩が起こった場合の 2 次的な被害はどのように扱うのか？が定義されていないと考える。

2.3.3. -2-2 第2軸：発生したインシデントの経済的影響度の度合い(金銭的価値への換算)

金銭的な価値への換算をどのようにするのか？そもそも金額に換算することが難しいと考える。
第1層、第2層、第3層の各層の繋がり、サプライチェーン、サービスなどの関わるので、第2層のみで計ることが難しいと考える。

図3の経済的影響の度合い部分は、誰をターゲットにしているか？が明確でない。サプライチェーンの想定と実際にサービスを行う人とサービスを利用する人の明確化が必要なのではないかと考える。

2.3.4. -2-3 フィジカル・サイバー感を繋げる機器・システムのカテゴライズ

マッピングするにあたっての基準となる考え方やリスク、重要度を計るための機能安全、セキュリティの基準の具体例を示すべきではないか？と考える。

2.3.5. -3-2 第2の観点：運用中のフィジカル・サイバー間を繋ぐ機器・システムの確認要求

280-281の部分は、何故セキュリティ・セーフティを確保することが可能か？の具体的な説明が必要なのでは？と考える。