経済産業省

資料５

第2回パブリックコメントで寄せられた御意見に対する考え方（案）
～概要～

平成31年4月4日

経済産業省　商務情報政策局

サイバーセキュリティ課

サイバー・フィジカル・セキュリティ対策フレームワークの第2回パブコメ概要

- **サイバー・フィジカル・セキュリティ対策フレームワーク**（以下「**CPSF**」という）の第二原案に対するパブリックコメントを平成31年1月9日～2月28日に実施。
- 海外からの関心が高く、英語版パブコメも実施。
- **国内27、海外13（米国7、欧州6）の組織・個人より、約500件の意見提出**あり。

主な御意見

① **三層構造**に関する御意見
② **トラストの仕組み**に関する御意見
③ **リスクベースアプローチ**及び**マルチステークホルダーアプローチ**に関する御意見
④ **プロファイル**に関する御意見
⑤ **データ保護**に関する御意見
⑥ **ソフトウェアセキュリティ**に関する御意見
⑦ **機器のセキュリティ確保**に関する御意見
⑧ **CPSFの解説書整備**を求める御意見
⑨ **用語の定義**に関する御意見
⑩ **セキュリティ対策例の内容**に関する御意見
⑪ **一般消費者も視野に入れるべき**との御意見

主な御意見とそれに対する考え方①：三層構造に関する御意見

いただいた御意見

- **三層構造**に関する御意見。
  - 第2層と第3層は変えずに、**第1層をフィジカル空間と定義するのが妥当**であろう。【12-1】
  - フレームワークの内容は多少、難解ではあるが、米国の標準との整合性をもちながら、**三層構造の導入により新たな視点**を加えられている。【22-3】
  - フレームワーク原案にて提唱されているモデルは、**三層**（「企業間のつながり」、「フィジカル空間とサイバー空間のつながり」、「サイバー空間におけるつながり」）と**6つの構成要素**（ヒト、ソシキ、システム、モノ、データ、プロシージャ）を特定しているが、デジタル産業エコシステムにおける主要な関係者や関係性を理解するための**有用な概念を提供**している。【23-4】
  - 「3層」の層という表現を他のものに変更する**「層」という言葉を使っているために理解のための説明が１つ必要**になってしまっています。【31-2】

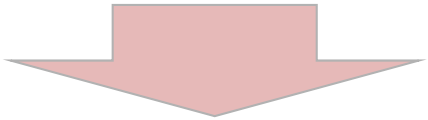
御意見に対する考え方

- 三層構造は、**新たな社会を適切に捉えるモデル**として理解する肯定的な意見が多数。
- 「企業間のつながり」、「フィジカル空間とサイバー空間のつながり」、「サイバー空間におけるつながり」の3つの視点を**「層」と定義**。引き続き丁寧に説明。

主な御意見とそれに対する考え方②：トラストの仕組みに関する御意見

いただいた御意見

- **トラストの仕組み**に関する御意見。
  - **信頼の創出、信頼の証明および信頼チェーンの構築と維持という概念は非常に明確に考案**されている。【19-10】
  - 企業に対して個人同様の証明書を発行して相互に信頼できる**トラストフレームワークの構築**を求める。【27-5】
  - エコシステム内には、製造業者によって開発されているデバイスおよびIoTシステムの独立した**検証、認証**の役割があるはずです。これにより、**サプライチェーン全体に透明性とある程度の保証**がもたらされます。【40-6】



御意見に対する考え方

- CPSFは、新たな社会「Society5.0」におけるセキュリティ対策の全体的な枠組を提示。
  信頼性確保の具体的な仕組みについて、各SWGの活動も含めて今後検討。

主な御意見とそれに対する考え方③：リスクベースアプローチ及びマルチステークホルダーアプローチに関する御意見

いただいた御意見

- **リスクベースアプローチ**及び**マルチステークホルダーアプローチ**に関する御意見。
  - 提案されているフレームワークは、セキュアなIoTまたはサイバー/物理ソリューションを作成する際の開発者に対する技術的考慮事項に対する包括的な見解を提供している。しかしながら、リスク管理は効果的なサイバーセキュリティにとって根本的であると強く信じているため、**リスクベースのアプローチを反映し、リスク管理プロセスの実装を優先するためのポリシーが必要**とされている。【21-2】
  - IoTは、世界の経済や社会を変革する態勢を整えており、日本のSociety5.0の重要な構成要素でもある。IoTが提示する課題は、コラボレーティブなセキュリティアプローチをこれまで以上に重要にしており、世界中の政府は、IoTセキュリティの将来を形成するための重要な選択をしている。経済産業省がこの問題の重要性を認識し、**マルチステークホルダーのアプローチを用いてこの問題に取り組むための行動を起こしていることを嬉しく思う**。【24-1】

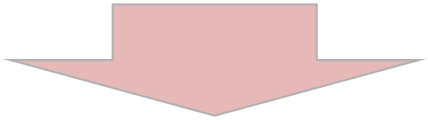
御意見に対する考え方

- **CPSFでは、リスクベースアプローチ及びマルチステークホルダーアプローチを採用**することで、新たな社会「Society5.0」におけるセキュリティ対策の全体的な枠組を示したことに対して肯定的。

主な御意見とそれに対する考え方④：プロファイルに関する御意見

いただいた御意見

- **プロファイル**に関する御意見。
  - “実態に則したセキュリティ対策の項目を列挙したプロファイルの作成に…"とあるが、**プロファイルの例を提示**してほしい。【27-7】
  - 三層構造アプローチでリスク源の網羅性を体系的に担保しようとしているのかなと感じた。ただ、実際に本ガイドラインでセキュリティチェックを実施する際に、Society5.0がまだ進んでいない企業は自企業用に落とし込む必要がある。そのため、**業界ごとのセキュリティガイドラインがとても重要**になってくると感じた。【34-24】



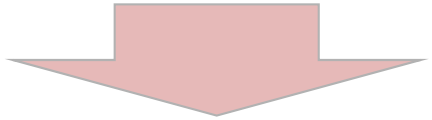
御意見に対する考え方

- CPSFは、新たな社会「Society5.0」におけるセキュリティ対策の全体的な枠組を提示。具体的なセキュリティ対策例は、産業分野や個社ごとに異なるものであり、**各SWG等において、ガイドライン等を引き続き検討**。

主な御意見とそれに対する考え方⑤：データ保護に関する御意見

いただいた御意見

- **データ保護**に関する御意見。
  - 我々は、消費者がIoTおよびサイバーフィジカルシステムを使用、展開する際に、プライバシー認証スキームが消費者との信頼関係を築く上で重要な役割を果たすと考えている。この目的のために、我々は、フレームワークが安全で技術的な解決策と並んで、**データを保護するという強い文化**をよりよく促進していくことを望んでいる。【21-3】
  - **データ保護については、管理責任の所在（部署単位）を明確化**すべきではないか。【34-63】
  - データの暗号化については、暗号の強度レベル以前に**機密レベルの定義**が必要ではないか。【34-64】



御意見に対する考え方

- CPSFでは、「データ」を第３層サイバー空間のつながりにおける信頼性の基点と設定し、対策要件及び対策例を提示。**データ区分に応じてどのようにデータを適切に保護すべきかなどの詳細については、各SWGの活動も含め今後検討。**

主な御意見とそれに対する考え方⑥：ソフトウェアセキュリティに関する御意見

いただいた御意見

- **ソフトウェアセキュリティ**に関する御意見。
  - 資産管理に関する第2原案のカテゴリには、すべてのハードウェアとソフトウェアの一覧を管理し、製造日や製造条件などの記録を作成するためのガイダンスが含まれている。また、ソフトウェアが一覧化されるだけでなく、適切にライセンスされ、最新化されているかどうかも確認するため、透明性の高い検証可能な**ソフトウェア資産管理(SAM)のプラクティスを採用**するためのガイダンスも含むべきである。ライセンスされていないソフトウェアは、マルウェアの発生に関連するリスクを軽減するような重要なセキュリティ更新プログラムを受け取る可能性が低いため、その使用により有害なサイバーセキュリティインシデントのリスクが高まる。信頼できないソースからのライセンスされていない技術には、悪意のあるアクターによって挿入された埋込み型のマルウェアが含まれる可能性がある。【23-6】
  - デバイスソフトウェアの更新を認証する：METIフレームワークはユーザー認証には対応していますが、**機器の「自動的な」ソフトウェアアップデートの認証を要求**するようには見えない。これがないと、攻撃者は接続をハイジャックし、悪意のあるソフトウェアをIoT機器にダウンロードする可能性がある。【24-2】

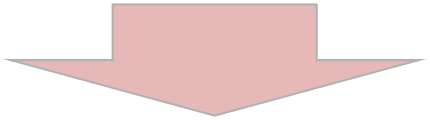
御意見に対する考え方

- ソフトウェアの信頼性を確保するための仕組みは重要であり、特に、オープンソースソフトウェア（OSS）の活用も進展。**ソフトウェアの信頼性をどう担保するのかについて、各SWGの活動も含め今後検討**。
- なお、ソフトウェアアップデート認証について、対策例に追記。

主な御意見とそれに対する考え方⑦：機器のセキュリティ確保に関する御意見

いただいた御意見

- **機器のセキュリティ確保**に関する御意見。
  - **第2層において、機器の調達およびテストフェーズにおけるセキュリティ・バイ・デザインについて言及しているのは素晴らしい。**【19-20】
  - 転写機能がおかしくなったときの方針として、**「データ転写のみ安全に停止する or 切り離す」という観点**が盛り込まれていない。【34-39】



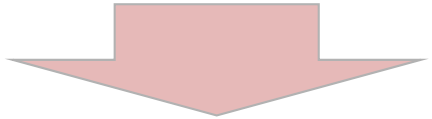
御意見に対する考え方

- CPSFでは、「転写機能」を第２層フィジカル空間とサイバー空間のつながりにおける信頼性の基点と設定し、対策要件及び対策例を提示。**安全も考慮に入れたセキュリティ対策などについても明示。より詳細については、各SWGの活動も含め今後検討。**

主な御意見とそれに対する考え方⑧：CPSFの解説書整備を求める御意見

いただいた御意見

- **CPSFの解説書整備**を求める意見。
  - 分割定義された階層の概念が読む人によって理解が異なる可能性があり、どのレイヤにも属さない隙間が発生する懸念がある。**階層定義に対する十分な解説書またはガイドラインの整備**が望まれる。【22-1】



御意見に対する考え方

- CPSFの策定に関わった方々などによる解説など、**<u>様々な活動が広がることを期待</u>**。

主な御意見とそれに対する考え方⑨：用語の定義に関する御意見

いただいた御意見

- **用語の定義**に関する御意見。
  - 「プロシージャ」 **用語解説を分かりやすく**表示。【7-2】
  - グローバルデジタル社会のための**サプライチェーンリスクマネジメントがISO 27036-3に定義**されているため、留意したほうがよい。【20-5】
  - 用語集における定義をクラウドコンピューティング、ビッグデータ、AI、IoT、IACS等に関する**ISO/IECの語彙とハーモナイズ**したほうがよい。【20-8】
  - フレームワークが関連する**ISO国際規格に見られる用語の定義と用法を参照**することは有用かもしれない。【23-15】
  - ハッシュ値：ハッシュ値の**特色の説明に不足**が見られる。【30-10】
  - セキュリティルール：**セキュリティコントロール(security control)の方がより一般的な表現**であると考える。【30-20】

御意見に対する考え方

- 用語の定義に関しては、いただいた御意見を参考にさせていただきつつ、再度、**国際規格等の定義を参照し、用語集（添付E）を必要に応じて修正**。

主な御意見とそれに対する考え方⑩：セキュリティ対策例の内容に関する御意見

いただいた御意見

- **セキュリティ対策例の内容**に関する御意見。
  - （CPS.CM-3）**ホワイトリスト型マルウェア対策も有効**であるため、**対策例<High Advanced>に併記すべき**である。【26-2】
  - （CPS.RA-3）一般に公開されている脅威情報以外を利用した犯罪・問題が多く発生しているため、情報入手の方法のレベルを上げる必要があると考える。そのため、本対策要件の**<High Advanced> 対策例においては**、一般的に公開されている情報のみを利用するのではなく、**専門家によって調査分析された、ダークウェブ上の情報も視野に入れるべき**。【26-6】
  - （CPS.DS-14）**対策例「物理的な攻撃に対して耐性を有しているか」は <Basic> に移動したほうが良い**のではないか。【34-71】
  - （CPS.AE-2）**<Advanced> の対策例として、組織内だけでなく組織間のデータ連係部分を含めることを注記した方がよい**。【34-73】
  - （CPS.AC-4）**<Basic>の対策例について、他のクレデンシャルについても含めるような文章とした方がよい**のでは。【36-8】

御意見に対する考え方

- セキュリティ対策例に関しては、いただいた御意見を踏まえ、**<u>必要に応じて修正</u>**。

主な御意見とそれに対する考え方⑪：一般消費者も視野に入れるべきとの御意見

いただいた御意見

- **一般消費者も視野に入れるべき**との御意見。
  - **生活者がステークホルダーとして重要な役割を果たすのがSociety5.0の世界**であると考える。生活者に配慮した表記とすべきである。【7-5】
  - **「消費者」あるいは「最終消費者」も付加価値連鎖の一部と見なされているか。**【19-5】

御意見に対する考え方

- **一般消費者は、CPSFにおいても重要なステークホルダーと認識。**