補足資料

「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF)改訂に関する調査支援等業務」に係る一般競争入札

補足説明資料

2026年3月11日
独立行政法人情報処理推進機構 (IPA)
デジタルアーキテクチャ・デザインセンター (DADC)

更新履歴

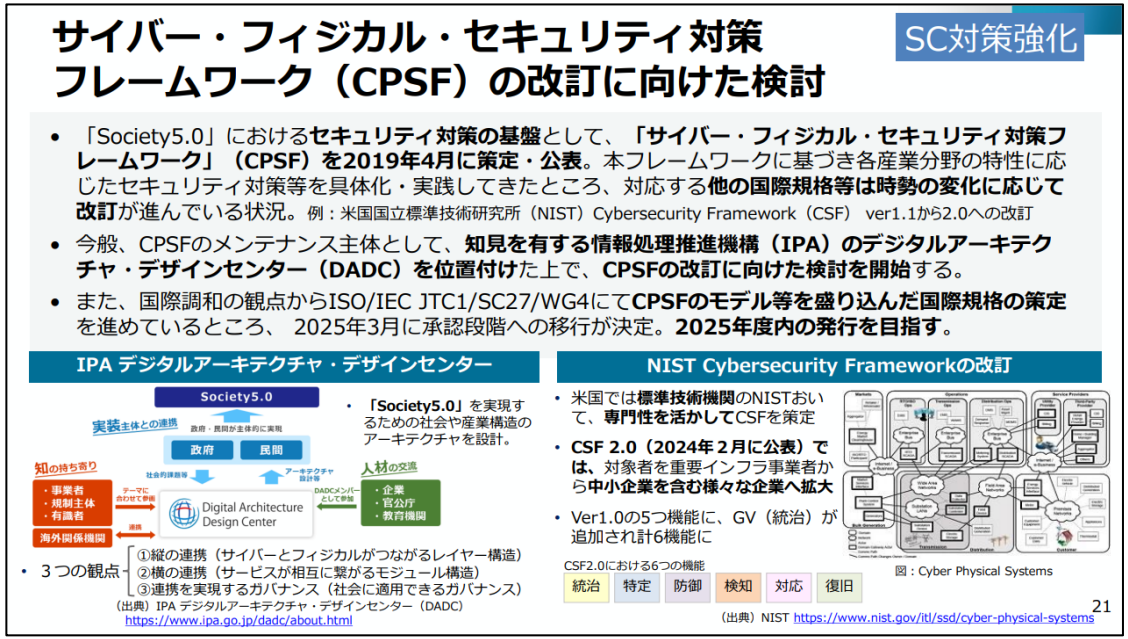
<table>
<tr><th>更新日付</th><th>更新内容</th><th>備考</th></tr>
<tr><td>2026年3月12日</td><td>19頁
【修正前】
<table>
<tr><th>作業概要</th><th>最終成果物名</th><th>想定枚数</th><th>形式</th></tr>
<tr><td rowspan="2">CPSF改訂に向けた調査を結果を報告する。</td><td>調査報告書 (概要版)</td><td>100～200枚程度</td><td>powerpoint</td></tr>
<tr><td>調査報告書 (詳細版)</td><td>30～50枚程度</td><td>word</td></tr>
</table>
【修正後】
<table>
<tr><th>作業概要</th><th>最終成果物名</th><th>想定枚数</th><th>形式</th></tr>
<tr><td rowspan="2">CPSF改訂に向けた調査を結果を報告する。</td><td>調査報告書 (概要版)</td><td>30～50枚程度</td><td>powerpoint</td></tr>
<tr><td>調査報告書 (詳細版)</td><td>100～200枚程度</td><td>word</td></tr>
</table></td><td></td></tr>
</table>

0. 目次

1. はじめに

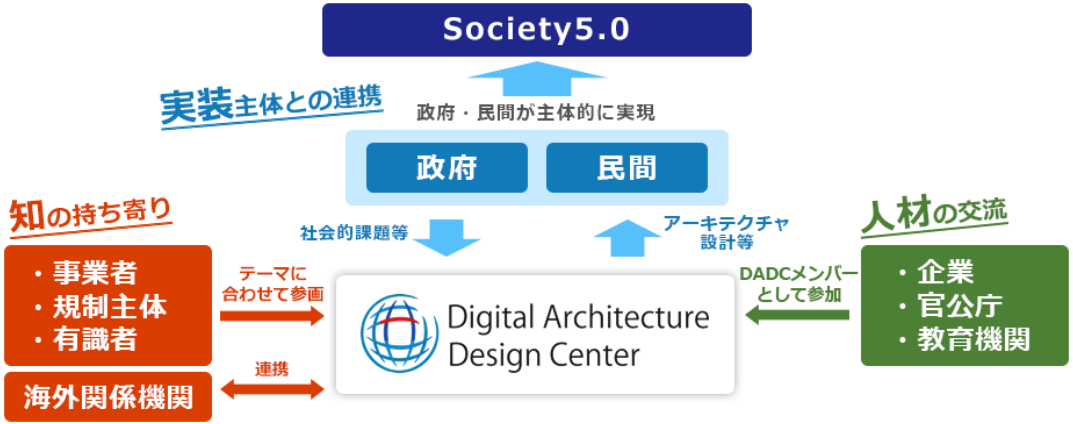
令和7年5月23日に開催された第9回産業サイバーセキュリティ研究会（009_03_00.pdf）において、サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の改訂に向けた検討を開始する宣言。

- 「Society5.0」におけるセキュリティ対策の基盤として、CPSFを2019年4月に策定・公表。本フレームワークに基づき各産業分野の特性に応じたセキュリティ対策等を具体化・実践してきたところ、対応する他の国際規格等は時勢の変化に応じて改訂が進んでいる状況。
  （例：NIST CSF　ver1.1から2.0への改訂※CSF 2.0（2024年２月に公表）では、対象者を重要インフラ事業者から中小企業を含む様々な企業へ拡大）
- 今般、CPSFのメンテナンス主体として、知見を有するIPA／DADCを位置付けた上で、CPSFの改訂に向けた検討を開始する。



（参考）DADCの役割

DADCは、政府・民間の依頼に応じ、産学官の関係者を柔軟かつ円滑に巻き込みながら、グローバルな動向を踏まえ、協調領域を中心に中立透明にSociety5.0 ※1を実現するためのアーキテクチャ※2を設計している。



※１Society5.0の実現：
サイバー空間 (仮想) とフィジカル空間 (現実) を高度に融合させたCPS（フィジカル空間からセンサーとIoTを通じてあらゆる情報がサイバー空間に集積し、人工知能 (AI) などを活用してビックデー タを解析し、高付加価値をフィジカル空間にフィードバック）により、経済発展と社会的課題の解決を両立する、人間中心の社会

※２ アーキテクチャ：
「ソフトウェア」だけでなく「人・業務・機械・ルール等」を含むSociety5.0の社会を実現するための見取り図

2.1 プロジェクトの目的

本プロジェクトでは、2019年策定のCPSF 1.0を、現下の技術・社会動向に即して改訂し、サイバー・フィジカル社会における「安全・安心・信頼性」の確保に資する基盤的枠組み・指針を整備することで、重大インシデントの未然防止を目指す。

- **サイバー空間（情報空間）とフィジカル空間（現実空間）の高度な融合が進展する中、サイバーフィジカルシステム（CPS）は、社会や産業インフラの中核として、その役割を一層強めつつある。**
- **その一方で、技術の進展やグローバル化、サプライチェーンの複雑化、ロボティクス技術の実装拡大や国家安全保障上の要請の高まり等により、従来のセキュリティ枠組みでは十分に対応し得ない、多様かつ高度なリスクや管理上の課題に直面している。**
- **本プロジェクトは、「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」1.0版の成果を踏まえつつ、ISO/IEC 5689[*1]、NIST Special Publication 1500-201（サイバーフィジカルシステムのためのフレームワーク）[*2]、NIST Cybersecurity Framework 2.0（CSF 2.0）[*3] などの国際標準指針や、ロボティクス技術の実装拡大や国家安全保障上の要請といった最新動向、さらにグローバルなビジネス環境の変化を反映し、今後の産業界や社会実装に資するセキュリティガバナンスおよびリスク管理フレームワークとしてCPSF1.0版を改訂する。**

※1 ISO/IEC 5689：
ISO/IEC SC 27にてCPSF等に基づく国際標準(ISO/IEC 5689)の策定を推進。CPSFの3層モデルをベースにサイバーフィジカルシステム(CPS)の概念モデルを定義し、当該モデルに沿う形でセキュリティやプライバシー等の観点から想定される懸念事項や必要な対応を整理。

※2 NIST Special Publication 1500-201（サイバーフィジカルシステムのためのフレームワーク）：
2017年6月、米国商務省国立標準技術研究所（NIST）エンジニアリングラボラトリ（Engineering Laboratory）に設置されたサイバーフィジカルシステム公開ワーキンググループ（CPS PWG）によって、1.0版が公表されました。2024年2月、米国商務省国立標準技術研究所（NIST）により、あらゆる組織が、サイバーセキュリティのリスクを管理し、軽減することを支援するために設計され、CSWP 29として公表された。

※3 NIST Cybersecurity Framework 2.0（CSF 2.0）：
2024年2月、米国商務省国立標準技術研究所（NIST）により、あらゆる組織が、サイバーセキュリティのリスクを管理し、軽減することを支援するために設計され、CSWP 29として公表された。

2.2 プロジェクトの内容

本プロジェクトは、CPSF1.0版の成果を踏まえつつ、ISO/IEC 5689、NIST Special Publication 1500-201（サイバーフィジカルシステムのためのフレームワーク）、NIST Cybersecurity Framework 2.0（CSF 2.0） などの国際標準指針や、ロボティクス技術の実装拡大や国家安全保障上の要請といった最新動向、さらにグローバルなビジネス環境の変化を反映し、今後の産業界や社会実装に資するセキュリティガバナンスおよびリスク管理フレームワークとしてCPSF1.0版を改訂する。

具体的には以下の業務について取り組む。

a. 分析および調査の実施

b. 改訂版CPSF２.0（案）の作成

c. ワーキンググループ審議およびパブリックコメントによる意見収集

d. ご意見の反映および改訂版CPSF 2.0の策定

2.2.1 a. 分析および調査の実施の要件

CPSF 1.0版改訂に際し、対象範囲（スコープ）を定義する。

- CPSF 1.0版の現状分析を実施し、課題および対応方策を体系的に整理する。
  - 改訂方針
    - ✓ CPSFの国際標準化の取り組みとしてISO/IEC TS5689の策定が進められている。CPSF1.0およびISO/IEC TS5689の両方をインプットとする。
    - ✓ 3層構造モデルはISO/IEC TS5689の三層モデルを堅持しつつ、CSF1.0から2.0に改訂されている内容を取り入れる。
    - ✓ CSF1.0では機能・カテゴリ・サブカテゴリのみであったが、CSF2.0では実装例・参考情報が追加となっている。これを参照しながら添付B、Cなどの諸外国制度とのマッピングを更新する。必要に応じてNIST CSF2.0以外（ISA/IEC 62443、NIST SP 800-53/171など）も参照しエッセンスは盛り込む。
    - ✓ 英訳と世界向けの60日パブリックコメントは必須とし、世界各国の関係機関から広くコメントを募る。
    - ✓ ITセキュリティとOTセキュリティの分離と連携、FSIRTの必要性についてもCSF2.0を参照しつつ、CPSFの文脈で記載する。
- 国際標準指針および最新動向を調査の上、CPSが直面する多様かつ高度なリスク並びに管理上の課題を明確化する。
  - 主な調査対象
    - ✓ 国際標準指針：NIST SP 1500-201、NIST CSF 2.0、ISO/IEC 5689 等
    - ✓ CPS最新動向など：例（電力系統の高度化など ）

2.2.1 a. 分析および調査の実施の要件（CPSF 1.0版の現状分析）

CPSFは、現行版のストーリーに基づき、リスク源（脆弱性）を抽出した上で、複数の国際規格から導き出された対策要件や対策例と適切にマッピングし、自組織におけるセキュリティ対策を実施できる構成である。

①リスク源（脆弱性）の洗い出し

前提	「Society5.0」「Connected Industries」
目的	Society5.0におけるサプライチェーン（＝バリュークリエイションプロセス）全体のセキュリティ確保
脅威	定型的・直線的なサプライチェーンが直面していたものと比べ、（Society5.0では）これまでとは異なる複雑なものであり、脅威によって発生した被害が影響する範囲も広くなっていく **＃独立したシステム内でのデータフローと比べ、Society5.0では多方向のつながりとなると理解**
リスク源の整理	• 三層構造モデルを参照し、バリュークリエイションプロセスをモデルに落とし込む • 三層の「機能」を参照し、分析範囲を明確化 • 三層の「構成要素」から、分析対象を明確化 • 「機能」における「セキュリティインシデント」対して、「４つの観点」を踏まえ、リスク源と対応方針を整理
脆弱性	• キー「機能」の「セキュリティインシデント」に対し「脆弱性ID」を割り当て ✓ (例：L1-1-a-ORG) ✓ 体系：３層ー機能番号ー通番ー構成要素
マッピング	• 「脆弱性ID」に対して、「対策要件ID（重複あり）」のひもづけ

マッピング

②対策要件のカテゴリー

カテゴリー	NIST Cybersecurity Framework Ver.1.1 の23個の「サブカテゴリー」をマージして20個にしたもの

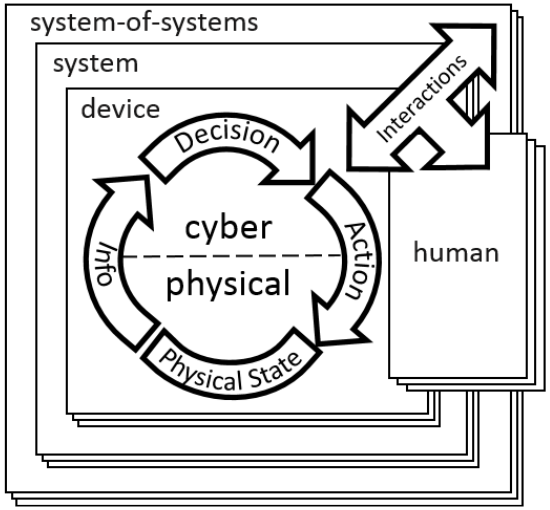
③対策要件および対策例

対策要件および対策例	原案（納品物）の対策要件に、３つの国際規格から抽出した対策要件および対策例を追加 ・添付D-1：NIST Cybersecurity Framework のサブカテゴリー ・添付D-2：NIST SP 800-171 の要求事項 ・添付D-3：ISO/IEC 27001 の管理策群
対策例補足情報追記	３つのレベル： High-Advanced／Advanced／Basic 実行主体： O「組織」,S「システム」,O/S「システム及び組織」 参照するガイドライン： NIST（SP800-171）、NIST（SP800-53 Rev.4）、ISO/IEC 27001:2013付属書A、IEC 62443-2-1:2010 、IEC 62443-3-3:2013
対策要件	・②「20のカテゴリー」に「対策要件ID」を割り当て ・（例：CPS-AM-1）体系：CPS-(20カテゴリー)ー(通番)
マッピング	・「対策要件ID」に対して、「脆弱性ID（重複あり）」のひもづけ

2.2.1 a. 分析および調査の実施の要件（国際標準指針ー１）

NIST SP 1500-201 の概要整理

「１．Introduction」では、CPS（サイバーフィジカルシステム）を以下のように定義しています。
「サイバーフィジカルシステムは、計算、通信、センシング、アクチュエーションをフィジカルシステムと統合し、環境とのさまざまな程度の相互作用（人との相互作用も含む）を伴う、時間に敏感な機能を遂行します。」
（原文：This document defines a CPS as follows: Cyber-physical systems integrate computation, communication, sensing, and actuation with physical systems to fulfill time-sensitive functions with varying degrees of interaction with the environment, including human interaction.）



CPS 概念モデル

モデルの説明（ IPA_gpt4.1を用いた日本語訳）
この図は、システム・オブ・システムズ（SoS）（例えばCPSインフラストラクチャ）の中でのデバイスやシステム間の潜在的な相互作用を強調するために提示されています。CPSは、単一のデバイスのようにシンプルな場合もあれば、サイバーフィジカルデバイスが1つまたは複数集まって構成されるシステムであったり、複数のシステム（それぞれが複数のデバイスから構成されている）からなるSoSとなる場合もあります。
このパターンは再帰的であり、捉え方によって異なります（つまり、ある観点でデバイスとみなされるものが、別の観点からはシステムとみなされる場合がある、ということです）。最終的に、CPSは意思決定フローと、情報フローまたはアクションフローのいずれか少なくとも1つを含んでいなければなりません。情報フローは、物理世界の物理的状態の測定をデジタルで表現するものです。一方、アクションフローは物理世界の物理的状態に影響を及ぼします。これによって、小規模・中規模から都市や国、世界規模までの協調が可能になります。

原文：
This figure is presented here to highlight the potential interactions of devices and systems in a system of systems (SoS) (e.g., a CPS infrastructure). A CPS may be as simple as an individual device, or a CPS can consist of one or more cyber-physical devices that form a system or can be a SoS, consisting of multiple systems that consist of multiple devices.
This pattern is recursive and depends on one’s perspective (i.e., a device from one perspective may be a system from another perspective). Ultimately, a CPS must contain the decision flow together with at least one of the flows for information or action. The information flow represents digitally the measurement of the physical state of the physical world, while the action flow impacts the physical state of the physical world. This allows for collaborations from small and medium scale up to city/nation/world scale.

2.2.1 a. 分析および調査の実施の要件（国際標準指針－２）

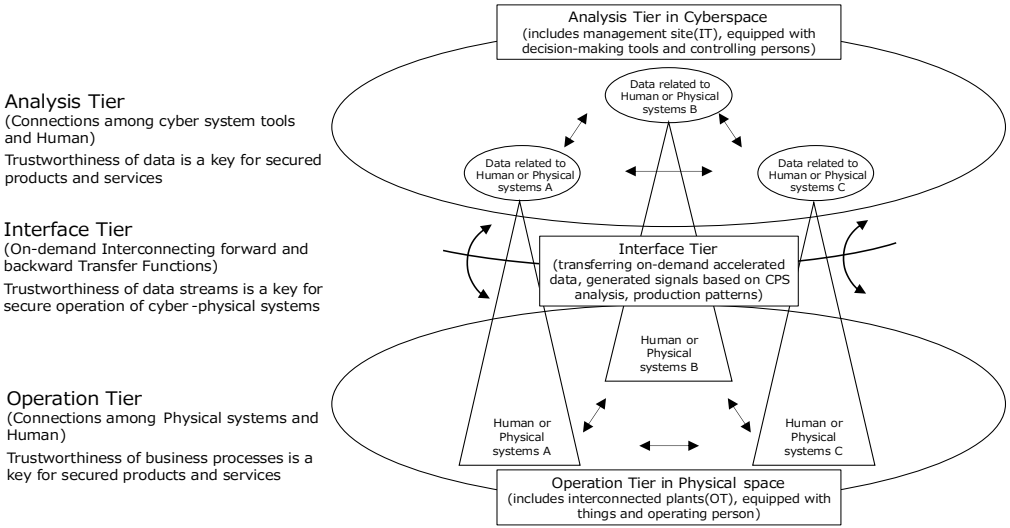
2024年に公表されたNIST Cybersecurity Framework（CSF）2.0と1.0との違い

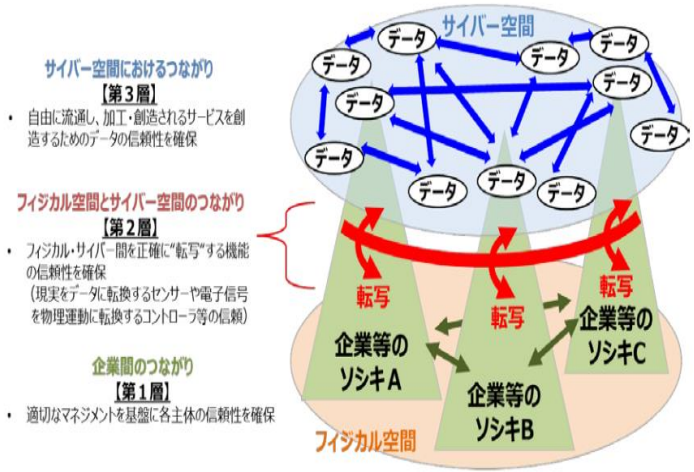
- 2014年のCSF 1.0発表以降に情報技術環境や脅威の在り方が大きく変化したことを踏まえ、従来の「重要インフラ」を主な対象としていた適用範囲を、**あらゆる業種・規模の全組織に大幅に拡張**するとともに、**「Govern（統治）」を新たにコア機能として追加**。
- 具体的には、多様な構成要素が連動することで、「全社横断の意思決定・一貫した方針・役割分担」を明確にしなければリスク管理が機能しなくなったことや、**個別のシステム対策や現場依存型管理だけでは、「ガバナンス不全」「責任の不明確化」により被害が拡大するリスクが顕在化**し、インシデントの発生後に分かる「方針不備」「報告・監視の遅れ」等の経営責任問題が国際社会で厳しく追及されるようになる経緯があった。
- このため、サイバーセキュリティが全社経営・社会的責任と不可分になった現代において、**「経営層による方針決定・責任の明確化・役割分担・説明責任・継続的な監督と改善」を基軸としたトップダウンのマネジメントサイクルが必須**となったため「ガバナンス（Govern（統治））機能」が必要となった。
- これにより、**サイバーセキュリティリスク管理が組織全体のリスク管理（エンタープライズリスク）と有機的に連携・統合**されるとともに、管理体制全般に対する注視、説明責任の明確化、さらには（一部の技術的な対策や個別部門の活動ではなく）組織的リーダーシップの抜本的な強化が実現されている。

2.2.1 a. 分析および調査の実施の要件（国際標準指針－３）

ISO/IEC 5689における三層概念モデルの例（図３）

- 当初日本から提案していたモデルは、複数のCPS(cyber-physical systems)が複合的に機能する場合を示すものとして提示されている。いわゆる「Society 5.0」は、CPSFにおいては多数の組織やシステムが複雑に連携することで形成される「バリュークリエイションプロセス」を擁するものとされているため、単体のCPSに係る概念モデルから派生させつつこちらのモデル(下記左)を示している。
- こちらのモデルはCPSFの内容を基本的にそのまま活用しているが、前頁に示したCPS概念モデルとの対応関係を踏まえ、一部の文言の修正等を行っている。

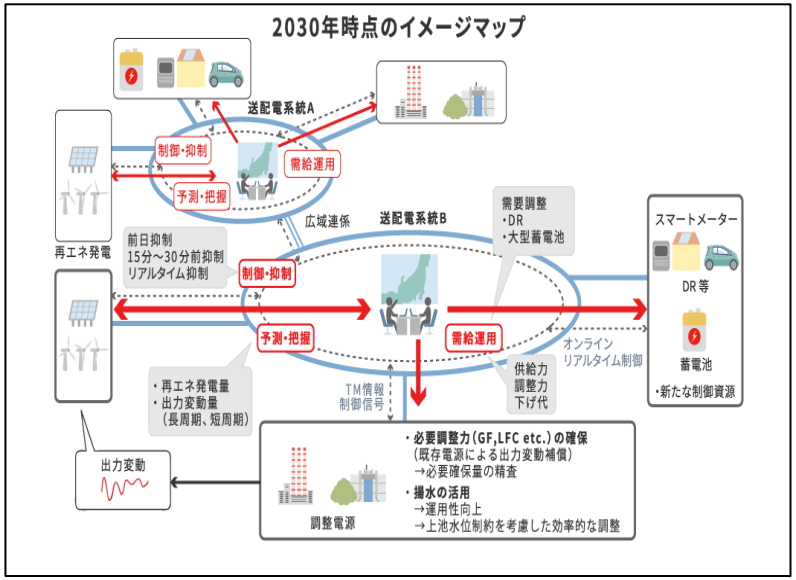




2.2.1 a. 分析および調査の実施の要件（最新動向の調査－１）

地政学リスクがもたらす多面的・複合的な脅威は、CPSの信頼性・安全性・レジリエンス（耐障害性）を著しく損なう可能性があり、今後の社会インフラ運用において極めて重要な論点となっている。

【電力系統の高度化】広域連携



https://www.tepco.co.jp/pg/technology/renewable.html
https://www.meti.go.jp/shingikai/enecho/shoene_shinene/shin_energy/keito_wg/pdf/037_02_03.pdf

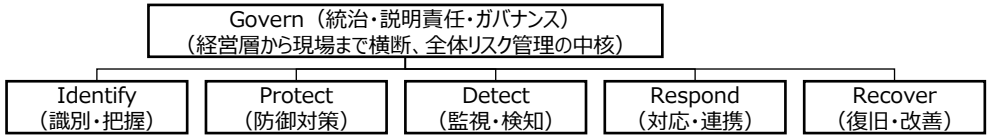
2.2.1 a. 分析および調査の実施の要件（最新動向の調査ー２）

CPSの動向調査　：（例）自動運転方式の比較（Co-pilot利用）

企業	技術アーキテクチャ	センサー構成	地図依存	主戦場	安全データ	規制・量産性
Wayve	End-to-End（Embodied AI）。HDマップ不要で汎化性能を重視。[sg.news.yahoo.com]	カメラ中心（OEM構成に適応）。[sg.news.yahoo.com]	不要（マップレス）	欧州・北米・アジアでAI-500ロードショー（90→500都市）。[sg.news.yahoo.com]	500都市走行で安全適応を実証。安全クリティカル評価にはGAIA-3を使用。[autonews.gasgoo.com]	Nissanと次世代ProPILOTを共同開発、**2027量産計画**。AI安全認証研究（Warwick大学）。[apollogo.com], [technology...gazine.com]
Waymo	LiDAR＋HDマップ＋計画の階層型。高冗長・高精度。[bloomberg.com]	LiDAR＋カメラ＋レーダー	高依存（HD Map）	米国：SF・LA・PHX・Austinほか多数都市で**完全無人商用**。[bloomberg.com], [arstechnica.com]	数百万マイル規模の実績。**TÜV SÜDの第三者監査**完了。[money.usnews.com]	CPUC/DMVが広域商用・無人運行を承認（全米で最成熟）。[bloomberg.com]
Apollo Go（Baidu）	多センサー＋HDマップ＋ロボタクシー専用設計（低コスト車RT6）。[ir.pony.ai]	LiDAR＋レーダー＋カメラ	高依存	中国本土22都市＋香港＋UAE。世界最大の無人運用規模。[ir.pony.ai]	240M km安全走行、14M＋完全無人ライド。[therobotreport.com]	香港など各国で認可拡大。英国でも2026年テストへ。RT6は**3万ドル以下**で量産性高い。[finance.yahoo.com], [nasdaq.com]
Pony.ai	L4向け冗長アーキテクチャ（Fail-Operational）。第7世代でBOM70%削減。	LiDAR＋カメラ＋レーダー（冗長）	中～高依存	中国（北京/広州）で完全無人商用、欧州ルクセンブルクでL4テスト許可。	2M km L4テスト。冗長化システムで高信頼性。	欧州で許可取得し安全信頼性強化。過去米国DMV停止歴あり（現在は再開）。12
Tesla（FSD）	Vision-onlyのE2E的運転支援（**L2：監督必須**）。大量ユーザーデータ学習。[wayve.ai]	カメラのみ	不要	世界中の一般ユーザー車両。ロボタクシーはAustinなどで試験段階。[wayve.ai]	Autopilot利用時6.69Mマイル/1事故（自社データ）。FSDは完全無人の公的安全実績なし。[https://jp...e7fbd.html]	欧州RDWは承認前（2026審査予定）。FSD名称に規制警告も。[selfdrivenews.com]
Cruise（GM）	LiDAR＋HDマップ構成	LiDAR＋カメラ等	高依存	以前はSF中心に展開	過去の歩行者事故が問題に。	**ロボタクシー撤退**、許認可停止後GMのADASに統合。[https://jp...e7fbd.html]

2.2.2 b.改訂版CPSF２.0（案）作成の要件（スコープ）

CPSF改訂版は、サイバーとフィジカル空間を横断し、高度なシステム連携や進展するグローバル事業環境、最新技術にも対応できるリスク管理・ガバナンスの新たな枠組みを構築する。改訂に係る方針については、以下に示す。

前提	• 「Society5.0」
対象	• 適用範囲の拡大と多様な業態への対応 - 産業分野や社会インフラ、自治体、医療、流通など多様な領域が対象 - 大／中小企業、単一組織から複数連携やサプライチェーン全体まで、さまざまな規模や組織構造に柔軟に対応できる汎用的な体系
目的	• あらゆる規模や業種の組織に対し、サイバーセキュリティリスクを一貫して識別・評価・管理・低減するための、包括的かつ実効性の高い枠組みを提供する
脅威	• フィジカル空間（現実空間）およびサイバー空間（情報空間）の全ライフサイクルにおけるリスクを一体的に管理 – CPS特有の複合的なリスク（システム横断・組織横断の情報資産、IoTデバイス、クラウド基盤、OT・ITの連携など） – SoSにおける多層的なリスク（安全性、セキュリティ、プライバシー、信頼性、レジリエンス）
モデル化	• NIST SP 1500-201におけるCPS定義および概念モデルを踏まえ、ISO/IEC 5689における三層概念モデルの例（図３）を参照
脆弱性および対策要件	• 国際標準との一元的整合性の確保（ISO/IEC 5689やNIST CSF 2.0等との整合を図る） • ガバナンスおよび説明責任の徹底（「Govern（統治）」機能をCPSFの中核に据え、経営層から現場に至るまでの階層横断的な管理体制、役割分担、説明責任および意思決定プロセスの明確化・透明化を推進する） • 最新技術および新興リスクへの統合的な対応（上記の脅威に対し、NIST CSF 2.0の構造に則した形で、他のNIST文書等に拠った知見を適切に取り込む） • 現場での適用性および実装支援の強化（NIST CSF 2.0の手法等を踏襲し、誰もが理解し実践しやすいチェックリスト、プロファイル例※１等を整備する） 

※1 CSF 2.0 Profiles： https://www.nist.gov/cyberframework/profiles

2.2.2 b.改訂版CPSF２.0（案）作成の要件

- **新興リスクへの統合的な対応に際し、国際標準に即した主な資料を参照し、自組織におけるセキュリティ対策を実施するための概念を洗い出す。**
- **リスクに関する観点（安全性、セキュリティ、プライバシー、レジリエンス、信頼性）は、NIST SP 1500-201において、CPSの複雑性を適切に管理し、各ドメインを横断して共通に考慮されるべき重要な要素として体系的に整理された9つのアスペクトのうち、「Trustworthiness」に係る懸念事項を活用。**

リスクの観点/	統治	識別	防御	検知	対応	復旧
安全性	・SP1500-201 ・SP 800-160 Vol.1	・IEC 61511/61508	・**CSF2.0**		・**CSF2.0**	・**CSF2.0**
セキュリティ		・**CSF2.0**	・**CSF2.0** ・SP 800-207 ・SP 800-53/171 ・SP 1800-35 ・IEC 62443	・**CSF2.0**	・**CSF2.0**	・SP 1800-25/26（ランサムウェア関係）
プライバシー	・NIST Privacy Framework V1.0	・NIST Privacy Framework V1.0				
レジリエンス					・**CSF2.0**	・**CSF2.0** ・SP 800-160 Vol.2(システム工学・品質保証)
信頼性	・**CSF2.0** ・SP 800-160 Vol.1/Vol.2(システム工学・品質保証)					

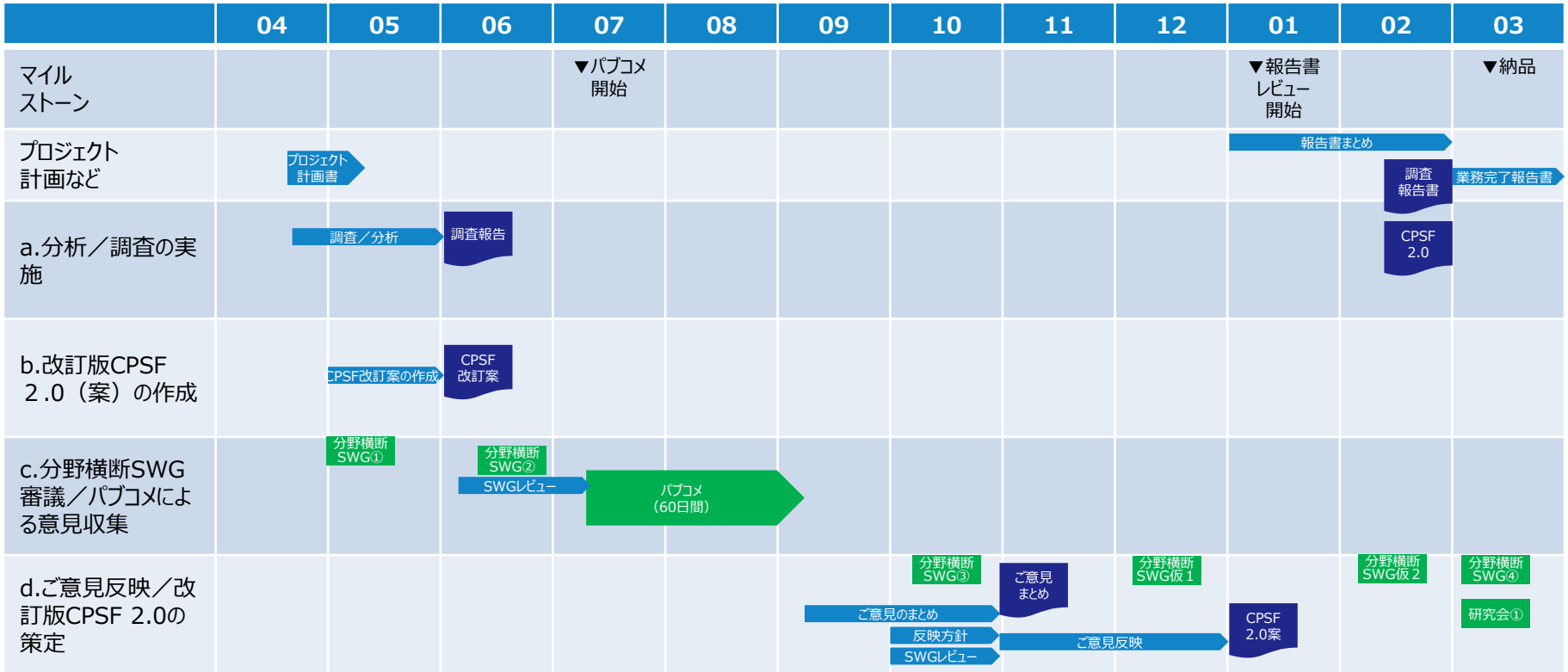
2.2.3 c.審議・パブリックコメントによる意見収集～d.改訂版CPSF 2.0の策定

改訂版CPSF2.0策定に向けて、透明性、実効性および社会的納得性の向上を目的として、策定過程における情報公開ならびに双方向的な意見交換を実施する。

- 経済産業省「産業サイバーセキュリティ研究会」「分野横断サブワーキンググループ」における審議（報告）
  - 2026年 5月　：スコープ案のご提示
  - 2026年 7月　：パブリックコメント案のご提示
  - 2026年10月　：パブリックコメントのご意見および反映方針のご提示
  - 2026年12月　：予備①
  - 2027年 2月仮　：予備②
  - 2027年 3月　：CPSF2.0版案のご提示
- パブリックコメント
  - 2026年8月～9月　：　CPSF2.0版案（日本語版･英語版）、60日間実施予定
- 経済産業省「産業サイバーセキュリティ研究会」における審議（報告）
  - 2027年3月　：　CPSF2.0版案のご提示

3.1 全体スケジュール（案）

契約期間は、契約締結日から令和９年3月12日である。



3.2 成果物一覧

成果物は以下の通りとする。

分類	作業概要	最終成果物名	想定枚数	形式
調査報告書等	CPSF改訂に向けた調査を結果を報告する。	調査報告書 (概要版)	30～50枚程度	powerpoint
		調査報告書 (詳細版)	100～200枚程度	word
	CPSF2.0版を作成する。	CPSF2.0版（改定案）	100～150枚程度	Word＋Excel
		CPSF2.0版（パブコメ向け案）	100～150枚程度	Word＋Excel
		CPSF2.0版（最終版）	100～150枚程度	Word＋Excel
	審議会、パブリックコメントなどでいただいたご意見をまとめる。	ご意見取り纏め報告書	100～150枚程度	excel
その他	プロジェクト全体の経過を報告する。	業務完了報告書	30～50枚程度	word

4.1 プロジェクトにかかる管理（案）

本プロジェクトでは下記の方針に従ってプロジェクトの管理を行う。

(1) コミュニケーション管理

- 週１回程度の定例会を実施し、業務の進捗状況の報告する。
- 会議は、3日以内（休日を除く）に議事録を作成し、 IPA／DADC の承認を受ける。
- 実施形態は、原則として、対面およびMicrosoft Teamsによるオンラインミーティングのハイブリッドで実施。

(2) 工程管理

- プロジェクトの作業工程の管理は、PMに集約して管理し、定例会にて報告を行う。

4.1 プロジェクトにかかる管理（案）

(3) 体制・品質・リスク・課題管理

- プロジェクトの作業体制や品質、リスクや課題は、PMに集約して管理する。
  体制・工程の変更、品質・リスクにおける懸念や解決すべき課題が発生した場合には、
  定例会を通じて速やかに報告する。

(4) 変更管理

- 作業変更が生じた場合には、速やかにIPA／DADCの承認を得る。

(5) 情報セキュリティ対策

- 「政府機関等のサイバーセキュリティ対策のための統一基準」 (内閣サイバーセキュリティセンター、令和７年度版)
  やそれに準拠したデジタル庁情報セキュリティポリシーを遵守する。

デジタルアーキテクチャデザインセンター
https://www.ipa.go.jp/dadc