資料３

技術・脅威の動向等を踏まえた対策（関連取組）
（経済産業省）

経済産業省

技術・脅威の動向等を踏まえた対策について

令和８年５月１５日

経済産業省　商務情報政策局

１．高性能AIの出現を踏まえた
サイバーセキュリティ上の対応について

※高性能AIへの対応に関する赤澤経済産業大臣と重要インフラ事業者との意見交換会
　経済産業省説明資料（令和８年５月１日）

（非公表）

（非公表）

（非公表）

（非公表）

２．技術・脅威の動向等を踏まえた対策について

AIエージェント利活用に伴うリスクへの対応

- 企業におけるAIエージェントの導入が加速しており、2030年までに**国内市場約3兆円規模へ拡大見込み。**
- 一方で、AIエージェントはその自律性に伴い、**意図しない不正なシステム操作**や**データ漏えいを引き起こす可能性**があり、サイバー攻撃等による**侵害時の影響は甚大。**
- こうした状況を踏まえ、**AIエージェントの導入企業が実施すべきセキュリティ対策（ガバナンス・データ保護・アイデンティティ管理等）**について、**民間企業が参照可能なガイドラインを策定**する。

AIに関連する既存のガイドライン等の整備状況（イメージ）

統一的な指針として：AI事業者ガイドライン(総務省/経済産業省 2026年3月改訂版公開)

AI開発者 / AI提供者 / AI利用者

AIセーフティに関する評価観点ガイド
(AISI 2025年3月改訂版公開)
AIセーフティ評価の観点、想定され得るリスク・評価項目例、評価の実施者等に関する考え方、評価に関する手法の概要を提示。
※他、AIセーフティに関するレッドチーミング手法ガイドも別途存在。

AIのセキュリティ確保のための技術的対策に係るガイドライン
(総務省 2026年3月初版公開)
「AIセーフティにおける重要要素」及び「AIセーフティ評価の観点」を踏まえ、AIの「セキュリティ確保」を取り扱う。脅威への技術的対策例を整理。

AI利用者である**民間企業が参照可能な実務的なガイドラインは存在せず。**

ガイドラインの方向性（イメージ）

1. AIエージェント導入パターン分類
2. AI導入時のリスクアセスメント、及びパターンごとの主要リスク整理
3. リスクに応じた対策の実装例

対策の実装例は、AIエージェント単体において実装される対策に限らず、下記に例示されるような、AIエージェント導入時にそのリスクに応じて求められる、**組織的対策及び企業のIT環境全体において実装すべき技術的対策等を想定**

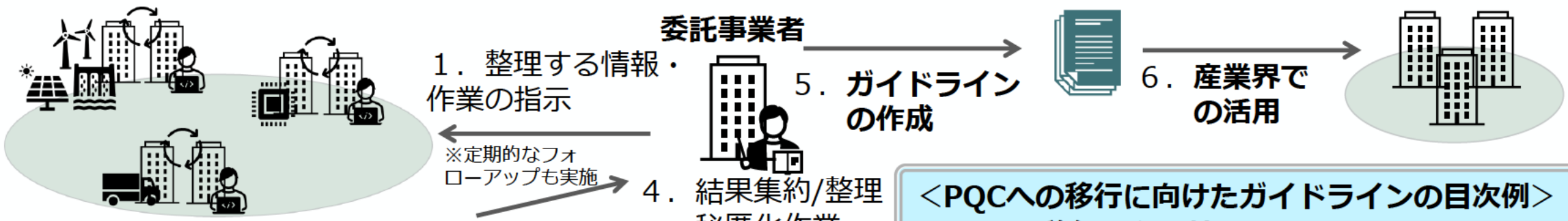
- ガバナンス
- データ保護
- アイデンティティ管理

（出典）日本経済新聞記事「エージェントもAIで守る」（2025年10月1日） https://www.nikkei.com/article/DGKKZO91645480Q5A930C2TB3000/

耐量子計算機暗号（PQC）への対応に向けた検討

- 量子コンピュータの進展による既存暗号の危殆化のリスクに備え、各国において、**耐量子計算機暗号（PQC）への移行に係る検討**が進められている。我が国でも、**政府機関等におけるPQC移行を原則として2035年までに行う**ことを目指し、2026年度に工程表を策定する旨を公表。
- 経済産業省でも、**産業界によるPQCへの円滑な移行を後押し**すべく、移行に向けた第一歩となるクリプトインベントリ※の実施に係る実証事業を開始。その成果物として、**移行に向けたステップの全体像**や**PQCに対応した製品情報**を含む、**PQCへの移行に向けたガイドラインを公表**（2027年春頃）予定。
  ※自社が保有する情報・システムに適用される暗号の棚卸し
- さらに、当該成果物の発信等を通じ、PQCへの対応を巡る**国際的な議論への貢献**も目指す。

クリプトインベントリの実施に係る実証事業のイメージ



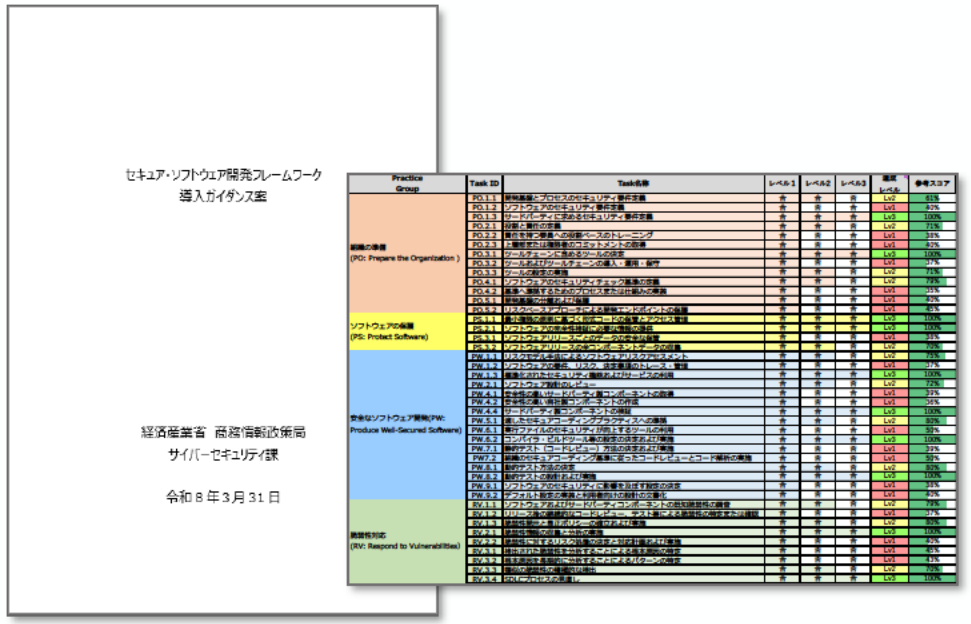
＜PQCへの移行に向けたガイドラインの目次例＞

- **PQC移行の必要性**・リスク
- 移行に向けたステップの**全体像**
- クリプトインベントリ**作成の手順**
- **実証事業の結果**（具体的な事例など）
- 関連情報（**PQC対応製品情報**）など

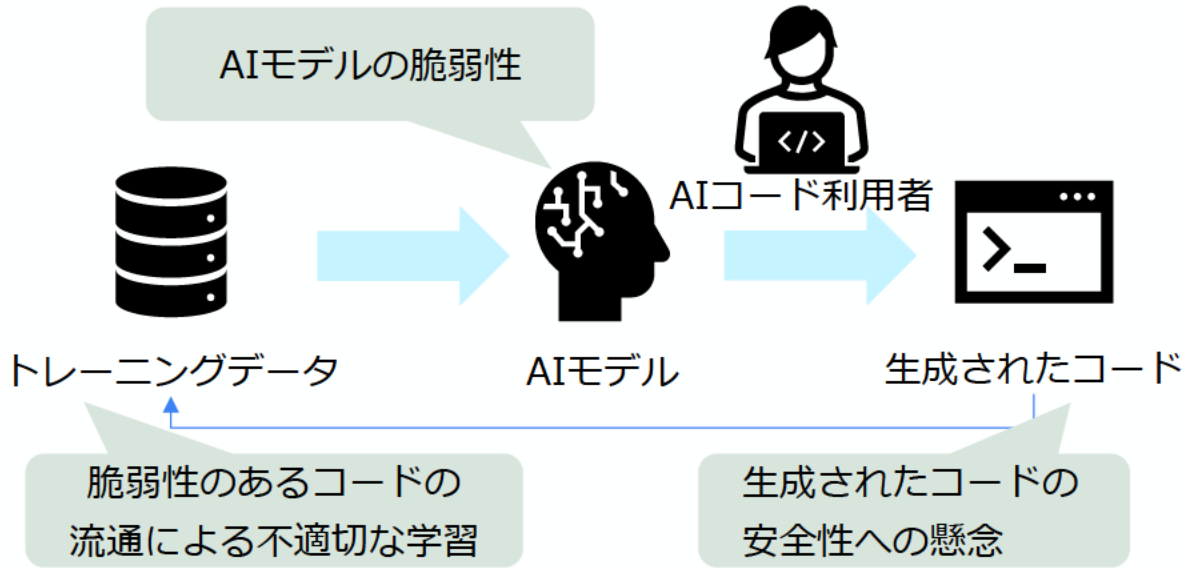
参考資料

(参考)AI駆動ソフトウェア開発に伴うリスクへの対応

- **「ソフトウェアに関するQUAD共通原則」の履行**を目標に、NISTの「**セキュア・ソフトウェア開発フレームワーク**」（**SSDF**）を効果的に**導入・実践するための具体的な方法や手順等をまとめた国内事業者向け文書を成案化**予定（2026年度を予定）。
- 今後、AIコーディングをはじめとする**「AI駆動開発」の台頭に伴うリスクへの対応の在り方**の検討や、**中小ベンダによるSSDF導入・実践の促進**（費用対効果の高いツールの整理等）を進めていく。
- また、国際動向に応じた連携や、**我が国の成果の海外展開**等も引き続き進めていく。



▲ SSDFガイドとチェックリスト（案）



▲ AI駆動開発（AIコーディング）におけるリスクのイメージ

(参考)先進的サイバー防御機能・分析能力強化のための研究開発

- 高度かつ未知の攻撃にも対処可能な**攻撃の早期発見技術**や、AIを活用したシステムの脆弱性の検知・評価技術など**防御力向上に資する技術**の開発・社会実装に向け、**約300億円／５年の研究開発プロジェクト**を立ち上げ、2024年７月からプロジェクト開始。

実施体制

一般社団法人サイバーリサーチコンソーシアム

研究開発の体制

理事会
※**FFRI、日立製作所、富士通、三菱電機、NTT、NECから理事を選出**

代表理事（FFRIセキュリティ 鵜飼社長）

一般社団法人
（サイバーリサーチコンソーシアム）

一般社団法人から再委託

大手民間企業、スタートアップ、大学・国研（計19者）も参画
※その他、情報通信研究機構等、関係機関とも連携

事業規模など

- 事業規模　：　290億円以下（2024年7月～2029年3月）
- 契約形態　：　委託事業

主な研究開発内容

1）サイバー空間の情報を収集・調査する状況把握力の向上

- アーティファクト分析技術／攻撃者からより多くの情報を獲得するための技術／高度かつ未知の攻撃にも対処可能な攻撃の早期発見技術

2）サイバー攻撃から機器やシステムを守る防御力の向上

- AIを活用した脆弱性探査技術／AI等を活用した防御能力の評価・向上技術／AIを活用したOTペネトレーションフレームワーク技術
- 耐量子計算機暗号技術／耐タンパー性向上技術

3）共通基盤の整備

- 情報の効果的な連携に関わる技術
- 高度サイバー人材の評価・管理に関する技術

4）セキュアな量子情報通信技術の開発

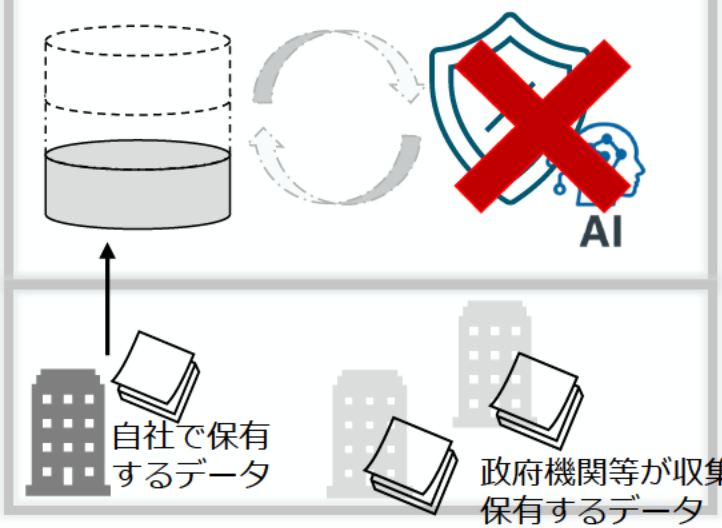
- Y-00のデジタルコヒーレントの開発／Y-00の高速光ファイバ通信の開発／Y-00の高速光ワイヤレス通信の開発

(参考)AIを活用した先進的なセキュリティ製品等の開発・提供支援

- 今後、AIを活用した先進的なセキュリティ製品・サービスの開発が期待される。他方、AIモデルの開発には必要な**計算環境の整備、データセットの収集・蓄積などが課題**となる。
- こうした課題を解決し、AI等を用いた先進セキュリティ製品等の開発を促進するため、**必要な計算環境の整備、データセットの収集を含めたプロジェクトへの支援**に向けた検討を行う。併せて、**関係省庁との連携**の下、企業側のニーズに応じて、政府機関等で集約した情報等を適切な情報保全等の下で**国内セキュリティ事業者等に対して開放**することも検討する。

現状の課題（As is）

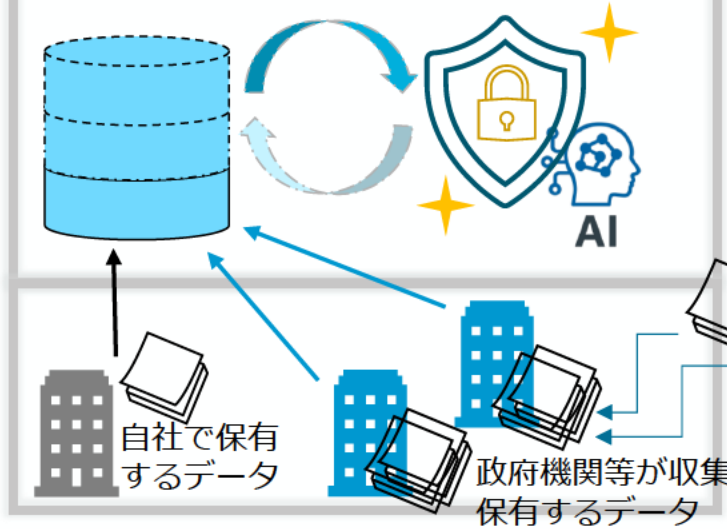
AIを活用した先進的なサイバーセキュリテイ製品・サービスの開発



- AIを開発するために必要な**学習データ**（脅威情報等）**の入手が困難**
- **計算資源の確保が困難**

目指すべき姿（To be）

AIを活用した先進的なサイバーセキュリテイ製品・サービスの開発



- **脅威情報等必要なデータセットを収集・蓄積**（必要に応じて政府機関等が開放）
- **必要な計算環境を整備**

(参考)フロンティア育成・懸賞金事業(サイバーセキュリティ関連技術の募集)

- セキュリティ対応力強化が求められる中、現場に無理なく導入できる技術・製品の開発を促しながら、**スタートアップ企業等に実績の機会を提供**するため、**サイバーセキュリティ関連技術を募集する懸賞金事業**を2026年度～2027年度にかけて実施する予定。

懸賞金事業の目的

- ✓ **国内企業のセキュリティ対応力強化**を目的に、懸賞金事業により**先進的なサイバーセキュリティ技術**を募集。
- ✓ 高度化する脅威**迅速・実効的に対応し、現場に無理なく導入・定着できる技術開発・製品化**を重視。
- ✓ 革新的な製品・サービスの創出と発掘を促し、我が国の**DX推進と経済成長**に寄与することを目指す。

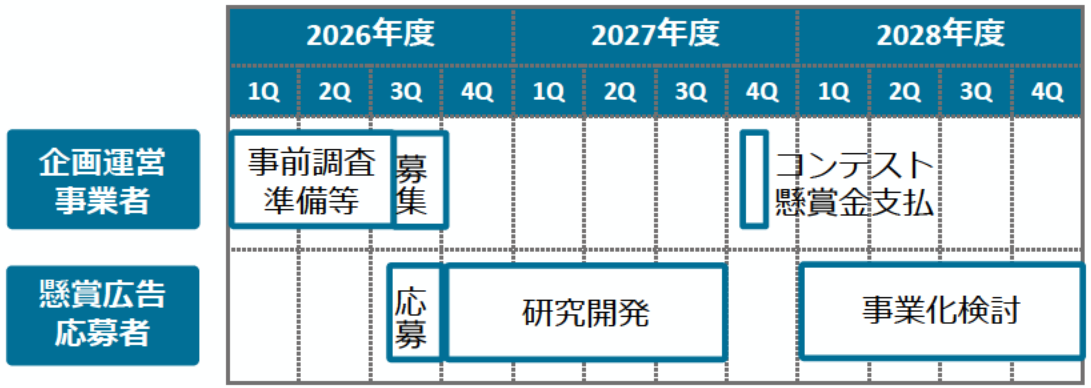
懸賞金テーマ：サイバーセキュリティの技術

以下のテーマ(案)において、効果的・効率的に革新的な**セキュリティ対策技術**の応募を期待。

- ✓ **AI技術を活用した**革新的なサイバーセキュリティ製品・サービスの開発・製品化
- ✓ **SBOM**（Software Bill of Materials：ソフトウェア部品構成表）の効率的な実運用に資するための技術開発・製品化
- ✓ **SSDF**（Secure Software Development Framework：米国NISTが策定したセキュア・ソフトウェア開発フレームワーク）

懸賞金事業スケジュール

以下のスケジュールを想定。2026年末に懸賞広告を公表し、**約1年間の研究開発期間**を設け、**2027年度末**にコンテストを実施予定。



(参考)産業全体を支えるセキュリティ人材の育成

- 我が国サイバーセキュリティ産業のエコシステム構築にあたっては、**産業の基盤となる人材の育成も重要**であり、とりわけ製品・サービスの提供側におけるトップ人材の育成を強化することが必要。

産業を支える人材の育成に向けた主なポイント

産業全体を支える人材の育成

トップ人材の育成
- 起業や新たな技術の開発などを通じて産業界をリードする、トップ人材の育成強化が重要

製品・サービス提供者のセキュリティスキル向上
- 優れた国産製品・サービス創出を担う、サプライサイドで活躍できるセキュリティ人材の育成強化が重要

セキュリティ領域の拡大に対応する人材
- AI等の先端技術の活用が急速に進む中、セキュリティ対策が求められる領域は拡大しており、各領域でセキュリティ対策を担える人材の育成が重要

キャリアの魅力発信
- セキュリティ人材の「量」・「質」を高めるためには、人材のパイプラインの「入口」となる候補者の分母を増やすための取組が重要

基盤整備
- 産学官で連携し、人材育成を効果的に推進するためには、スキル定義やキャリアパスの可視化など、人材育成の環境整備が重要

主な人材育成施策

(1)セキュリティ・キャンプ

- 若年層の**トップ人材**の育成・発掘を目指す事業
  - **AI、デバイス開発**及び法律などの**他領域と、セキュリティの知見を兼ね備えた人材**の育成プログラム(セキュリティ・キャンプ コネクト)を新たに実施予定
  - 継続的なネットワーク形成を通じた**修了生の成長支援**や**キャリアの魅力発信**等を目的として、修了生コミュニティを整備

(2)IPA産業サイバーセキュリティセンター(ICSCoE)

- セキュリティ対策の中核拠点として、OT(制御技術)や模擬プラントの活用を特徴とするハンズオン演習等を実施
  - 半導体をはじめとする**多様な製造事業者向け**の模擬プラントを拡充予定
  - **OT領域におけるAI活用の進展**を想定し、新規プログラムを提供予定

(3)情報処理安全確保支援士(登録セキスペ)

- **セキュアなシステム開発**からセキュリティマネジメントなどのセキュリティに係る**幅広い専門的な知識・技能**を備えた国家資格
  - **資格登録者数の増加**など、**制度の更なる活用**に向け、講習制度を見直し

※**基盤整備**の取組として、NCOによる人材フレームワークの検討や、**高度専門人材育成の強化**に向け、経済安全保障重要技術育成プログラムでも検討中。