経済産業省

資料３

事務局説明資料
産業サイバーセキュリティ研究会
WG３第10回

令和８年3月12日

経済産業省　商務情報政策局

サイバーセキュリティ課

産業サイバーセキュリティ研究会とWGの設置による検討体制

産業サイバーセキュリティ研究会

第１回：平成29年12月27日
第２回：平成30年　5月30日
第３回：平成31年　4月19日
第４回：令和　2年　4月17日※
第５回：令和　2年　6月30日
第６回：令和　3年　4月　2日
第７回：令和　4年　4月11日
第８回：令和　6年　4月　5日
第９回：令和　7年　5月23日
第10回：令和 8年　4月　3日

※電話開催

＜構成員＞　※2026年4月開催時点

伊藤　栄作　三菱重工業株式会社取締役社長

遠藤　信博　日本経済団体連合会サイバーセキュリティ委員長、日本電気株式会社特別顧問

片野坂真哉　日本情報システム・ユーザー協会会長、ANAホールディングス株式会社　取締役会長

星野　理彰　NTT株式会社　代表取締役副社長、副社長執行役員 CTO

寺田　航平　経済同友会副代表幹事、寺田倉庫株式会社　代表取締役社長

東原　敏昭　株式会社日立製作所取締役会長　代表執行役

船橋　洋一　公益財団法人　国際文化会館 グローバル・カウンシル チェアマン

村井　純(座長)慶應義塾大学教授

渡辺　佳英　日本商工会議所特別顧問、大崎電気工業株式会社取締役会長

＜オブザーバー＞
国家サイバー統括室、警察庁、金融庁、デジタル庁、総務省、外務省、文部科学省、厚生労働省、農林水産省、国土交通省、防衛省、防衛装備庁

WG１（実効性強化・国際連携）

- ガイドライン等の実効性強化
- 国際的な制度調和に向けた連携

第１回：平成30年　2月　7日
第２回：平成30年　3月29日
第３回：平成30年　8月　3日
第４回：平成30年12月25日
第５回：平成31年　4月　4日
第６回：令和　2年　3月（書面開催）
第７回：令和　2年10月（書面開催）
第８回：令和　3年　3月15日
第９回：令和　4年　4月　4日
第10回：令和 6年　3月14日
第11回：令和 7年　4月14日
第12回：令和 8年　3月10日

WG２（地域・中小企業支援）

- 地域・中小企業等における対策支援

第１回：平成30年　3月16日
第２回：平成30年　5月22日
第３回：平成30年11月　9日
第４回：平成31年　3月29日
第５回：令和　2年　1月15日
第６回：令和　2年　8月25日
第７回：令和 3年2月18日
第８回：令和 4年3月23日
第９回：令和 5年3月27日
第10回：令和6年3月25日
第11回：令和7年4月15日
第12回：令和8年3月　3日

WG３（産業振興・人材育成）

- セキュリティ産業振興、研究開発
- 人材育成・確保

第１回：平成30年4月　4日
第２回：平成30年8月　9日
第３回：平成31年1月28日
第４回：令和 元年8月　2日
第５回：令和　2年3月（書面開催）
第６回：令和 3年3月10日
第７回：令和 4年4月　6日
第８回：令和 6年4月　3日
第９回：令和 7年4月17日
第10回：令和8年3月12日

前回いただいた御意見と本検討会について（産業振興）

- 本日、今年度の進捗を報告するとともに、今後の政策の方向性を示す。全体的に御意見いただきたい。

供給能力強化に関する意見

① 海外製品が市場を占める中、**国産開発品の普及には信頼性と事業主体の明確化が必要。**

② 国産製品の普及には**開発だけでなく運用（保守・監視・サポート）の体制が重要**。

③ 国内SIerが**海外実績のある製品を優先し、国内ベンダーが商流に入りにくい状況がある**ため、国内ベンダーの商流参入を促す仕組み（調達・評価・導入支援等）も設計が必要。

④ **新領域（例：AIエージェント等）の育成が必要**。AIスタートアップが、**日本で起業したくなる制度づくりが必要**。

⑤ **官民ファンドによる迅速なシーズ投資と早期見極め**の仕組みが必要。

人材に関する意見

① 国内のセキュリティ人材不足が続いているが、経産省としての**育成ロードマップ**を検討するべき。

② 既存事業等と取組が重複しないよう、何をキャンプで、何を他機関で実施するのかを整理すべき。

③ 生成AI悪用の脅威が拡大している中、**AIセキュリティ人材に求めるスキルセット（技術＋法・倫理）**の定義や育成方法の検討が必要。

④ **異分野人材をセキュリティに転換**するための制度設計が必要。

⑤ **セキュリティ・キャンプ 修了生コミュニティの整備**の運営方法や狙う成果の整理が必要。

⑥ **セキュリティ・キャンプ コネクト**で、狙う層やレベル、規模など検討が必要。

国際に関する意見

① ASEAN 各国政府・関係者は日本のガイドライン提供など、政策面での**情報発信強化**を必要としている。ガイドラインの**英語での発信強化**が必要。

② 国として、**国内ベンダーの海外展開支援制度**（共同出展・PR・マッチング等）を検討すべき。

③ 国の全面管理でも民間の厳格な自己責任でもなく、経済産業省の支援を軸に、**国際サプライチェーン全体のセキュリティ底上げ**が重要。

目次

最近国内外で発生した主な事案

① 機微技術情報等の窃取

- 2021年以降、中国を背景とするグループ「Salt Typhoon」による、**政府や軍事インフラを含む世界中のネットワークを標的に、公開された脆弱性等を利用してアクセスし、データ窃取**等を行う活動が観測されている。（2025年8月 国家サイバー統括室及び警察庁が国際アドバイザリーに共同署名）

② 事業活動の停止

- 2025年9月、英自動車大手ジャガー・ランドローバー社において、**サイバー攻撃の影響により生産・小売活動が停止**。英国非営利団体は「約3,900億円以上の経済損失が生じた、英国史上最も被害の大きいサイバー攻撃である」と報告。
- 2025年9月、アサヒグループホールディングス㈱において、**ランサムウェア攻撃の影響により**国内の酒類や飲料、食品の**受注・出荷業務が停止。主要工場での製造も一時停止**するとともに、情報漏えいの可能性も確認。
- 2025年10月、アスクル㈱において、**ランサムウェア攻撃の影響により受注・出荷業務が停止**。ネット通販の配送をアスクルのグループ会社に委託する良品計画㈱等においてもネットストアでの受注・出荷業務が停止。情報漏えいも確認。

③ 重要インフラの機能停止等

- 2025年12月、ポーランドの**風力・太陽光発電所、熱電併給プラント等を標的とした、冬季の電力高需要期を狙ったとみられる大規模なサイバー攻撃キャンペーン**が行われた。攻撃者についてはロシアが支援するAPTグループとの関連が指摘されている。

④ サプライチェーン・委託先等への攻撃を起点とした情報漏えい

- 2025年3月、日鉄ソリューションズ㈱において、**ネットワーク機器へのゼロデイ攻撃を原因とした不正アクセス**を受け、同社のサーバー内に保存されていた、過去の**業務委託元などの取引先の個人情報を含む情報の漏えい**可能性を確認。

デジタル技術の発展によるサイバー攻撃の高度化・複雑化

- AI等のデジタル技術の発展の影響もあり、**サイバー攻撃実施のハードルは下がることで、今後ますますサイバー攻撃が増加・高度化・複雑化するおそれ**がある。

デジタル技術の発展によるサイバーリスクの増加

ITシステム、クラウド等の活用拡大、OT製品の急増など**サイバー空間の利用拡大**等に伴い、サイバー攻撃を受ける**システム側の侵入口が増加**。

NICTER において2025年に観測した**サイバー攻撃関連の通信数は増加傾向**(約7,010億パケット)。
家庭用ルータや録画機器等が感染の標的になる等、**IoTボットが多様化**。

スピアフィッシングやビジネスメール詐欺等の実行を支援する**サイバー犯罪用の生成 AI ツールの登場**

2025年における**フィッシングの報告件数**は**前年比約40%増の245万件超**と**引き続き急増**。

AIを通じた情報漏えい・サイバー攻撃リスク

- ウクライナの政府機関に対し、**生成AIを利用するマルウェアによる世界初のサイバー攻撃**が発生。マルウェアには攻撃指示は記述されず、外部の生成AIサービスと通信して攻撃指示を作成する仕組み。パターンマッチングによる**検知が従来型マルウェアより難しい**とされる。
- 業務管理ソフトの**AI連携機能（MCPサーバー）の欠陥の悪用**や、営業支援システムで用いられる**AIチャットボット連携機能の侵害**により**顧客情報等流出**事案が発生。
- AI活用による更なる効率化の観点から、**AIエージェント**の活用・検討が進むが、**大きな権限が設定**されることで、**乗っ取られた際の被害が甚大**になるリスクが指摘。

サイバー攻撃のエコシステム（ダークウェブ）の存在

- **ダークウェブの闇市場**では非合法で個人や企業の機密データ、**マルウェアを容易に作成できるツールキットなどが取引**されており、**サイバー犯罪を助長**している。
- ランサムウェア攻撃に必要な一式をサービスとして提供するRansomware-as-a-Service（RaaS）の普及により、**専門知識を持たない攻撃者でも攻撃が容易に**。

（出典）(独)情報処理推進機構（IPA）「情報セキュリティ10大脅威 2025」解説書、
(国研)情報通信研究機構「NICTER観測レポート2025」、フィッシング対策協議会「月次報告書」、各種報道情報　等

地政学動向の変化に伴うサイバーリスクの高まり

- サイバー攻撃が巧妙化・深刻化する中、地政学リスクの増大とも相まって、**安全保障にも関わるサイバー事案の脅威が高まっている**状況にある。

サイバー攻撃の変遷

■公開サーバへの攻撃
・特徴：ウェブサーバ・外向けサービスへの大量送信　等
・効果：ウェブサイト等の停止
・事例：エストニア・2007年

■機微情報の窃取の危険
・特徴：情報システムへの権限外アクセス・利用
・効果：機密情報の漏えい・悪用
・事例：Black Tech・2023年

■有事に備えた重要インフラ等への侵入（破壊準備）
・特徴：最深部・制御系システムに至る高度な侵入能力
・効果：インフラ機能の停止
・事例：Volt Typhoon・2023年　等

■世界規模の通信監視（スパイ活動）
・特徴：政府・重要インフラ等のネットワーク潜伏
・効果：通信内容・移動情報・認証情報等の窃取
・事例：Salt Typhoon他・2021-2025年


Joint Cybersecurity Advisory

Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System

Executive summary

国家関与が疑われるサイバー動向に関する報道

- **国家関与が疑われるサイバー攻撃事案への対抗**
  - 米国司法省は、米国やアジアの政府機関等に対するサイバー攻撃等に関与したとして、**中国公安部職員２人を含む中国人12人を起訴**したと発表。（2025年３月）
  - 米国政府は中国系APT「Volt Typhoon」及び「Salt Typhoon」による米国重要インフラへの長期潜伏と侵入を深刻視し、**「米国は報復的サイバー攻撃も辞さない」と明確に警告**。CISAは、中国政府支援の攻撃者がITネットワークからOT（制御系）への横展開を可能にする長期的侵入を進めていると指摘。（2025年5月）

- **台湾当局・重要インフラ等に対するサイバー攻撃**
  - 中国による**台湾当局へのサイバー攻撃が1日平均280万件**発生（前年比約17%増）。台湾当局が、中国の「オンライン・トロール（迷惑行為）部隊」による**台湾社会の分断を狙ったSNSでの偽情報の投稿**を警告。
  - **エネルギー施設への攻撃は前年比約11倍**であり、医療関連施設への攻撃も54%増加。半導体や軍需関連企業も標的となった。

（出典）各種報道発表・報道情報等を基に作成。

NSA、CISA、NCO、NPA他 “Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System”

（参考）IPA「情報セキュリティ10大脅威」

情報セキュリティ10大脅威 2026	
順　位	組織向け脅威
1位	ランサム攻撃による被害
2位	サプライチェーンや委託先を狙った攻撃
3位	AIの利用をめぐるサイバーリスク
4位	システムの脆弱性を悪用した攻撃
5位	機密情報を狙った標的型攻撃
6位	地政学的リスクに起因するサイバー攻撃（情報戦を含む）
7位	内部不正による情報漏えい等
8位	リモートワーク等の環境や仕組みを狙った攻撃
9位	DDoS攻撃（分散型サービス妨害攻撃）
10位	ビジネスメール詐欺

初選出

中小企業の被害が全体の6割以上を占める

相対的にセキュリティ対策の弱い中小企業を起点に、大企業含むサプライチェーンを共有する企業を攻撃

（出典）独立行政法人情報処理推進機構（IPA）「情報セキュリティ10大脅威2026」、
警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和７年９月）」を基に作成。

サイバー対処能力強化法及び同整備法の全体像

- 国家安全保障戦略（令和４年12月16日閣議決定）では、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるとの目標を掲げ、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④**NISCの発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置** 等の実現に向け検討を進めるとされた。
- これら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、令和６年６月７日からサイバー安全保障分野での対応能力の向上に向けた有識者会議を開催し、同年１１月２９日に提言を取りまとめ。
- この提言を踏まえ、令和7年2月7日に**「サイバー対処能力強化法案」及び「同整備法案」**を閣議決定。国会での審議・修正を経て、**同年５月16日に成立、同月23日に公布**。

概　要

総　則
- 目的規定、基本方針等（第１章）

官民連携（強化法）
- 基幹インフラ事業者による
  - 導入した一定の電子計算機の届出
  - インシデント報告

  （第２章）
- 情報共有・対策のための協議会の設置（第９章）
- 脆弱性対応の強化（第42条）

（その他、雑則（第11章）、罰則（第12章））

通信情報の利用（強化法）
- 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得（第３章）
- （同意によらない）通信情報の取得（第４章、第６章）
- 自動的な方法による機械的情報の選別の実施（第22条、第35条）
- 関係行政機関の分析への協力（第27条）
- 取得した通信情報の取扱制限（第５章）
- 独立機関による事前審査・継続的検査 等（第10章）

→ 分析情報・脆弱性情報の提供等（第８章）←

アクセス・無害化措置（整備法）
- 重大な危害を防止するための警察による無害化措置
- 独立機関の事前承認・警察庁長官等の指揮 等（警察官職務執行法改正）
- 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- 自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用）　等（自衛隊法改正）

組織・体制整備等（整備法）
- サイバーセキュリティ戦略本部の改組、機能強化（サイバーセキュリティ基本法改正）
- 内閣サイバー官の新設（内閣法改正）　等

施行期日　公布の日（令和7年5月23日）から起算して1年6月を超えない範囲内において政令で定める日　等

サイバーセキュリティ戦略の全体像

- 令和７年12月23日に閣議決定された「サイバーセキュリティ戦略」には、**サイバー人材の確保・育成や、国産を核とした新技術・サービスの創出が重要な方向性の一つ**として位置づけられている。
- 経済産業省では、本戦略に基づき、**サイバーセキュリティ産業振興や人材育成**等に取り組む。

「国家安全保障戦略」及び**サイバー対処能力強化法等**に基づく取組を含め、サイバー空間上の脅威に対応するための取組を一体的に推進するため、中長期的な視点から、**今後５年の期間を念頭に**、実施すべき諸施策の目標や実施方針を内外に示す

情勢

厳しさを増す国際情勢と国家を背景としたサイバー脅威の増大

社会全体のデジタル化の進展とサイバー脅威の増大

AI、量子技術等の新たな技術革新とサイバーセキュリティに及ぼす影響

施策の方向性

1. 深刻化するサイバー脅威に対する防御・抑止

- ✓ 厳しいサイバー安全保障環境に対応するため、官民連携・国際連携の下、事案対処等の従来の施策に能動的サイバー防御を含む多様な手段を組み合わせることで、攻撃者側にコストを負わせ、脅威を防御・抑止
- ✓ 政府から民間への積極的な情報提供

国が要となる防御・抑止

官民連携エコシステムの形成

国際連携の推進・強化

2. 幅広い主体による社会全体のサイバーセキュリティ及びレジリエンスの向上

- ✓ 様々な主体に求められる対策及び実効性確保に向けた方策の明確化・実施（政府機関等が範となり対策）
- ✓ デジタル化とセキュリティ確保の同時推進

政府機関等の対策強化

重要ｲﾝﾌﾗ事業者・地方公共団体等の対策強化

ｻﾌﾟﾗｲﾁｪｰﾝ全体のﾚｼﾞﾘｴﾝｽ確保

全員参加によるサイバーセキュリティ向上

ｻｲﾊﾞｰ犯罪対策を通じた安全・安心の確保

3. 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

- ✓ **産学官を通じたサイバー人材の確保・育成**
- ✓ **国産を核とした、新技術・サービスの創出**

効率的･効果的な人材の育成･確保

新たな技術･サービスのエコシステム形成

先端技術(AI、量子技術等)への対応･取組

官民連携・国際連携の下、広く国民・関係者の理解を得て、国が対策の要となり、官民一体で我が国のサイバーセキュリティ対策を推進
これにより、厳しさを増すサイバー空間を巡る情勢に切れ目無く対応できる、世界最高水準の強靱さを持つ国家を目指す

サイバーセキュリティ政策に関する国際的な動向

- 欧米を中心に、①セキュア・バイ・デザイン*の概念に基づく**製品のサイバーセキュリティ対策に対する要請**や、②**企業のサイバーセキュリティ対策**水準の整備・可視化、③国内のサプライチェーン全体をカバーする**中小企業向けサイバー対策促進支援**の取組が進展。

＊ IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていることを指す。

①IoT・ソフトウェア製品に対するセキュリティ要件

EU サイバーレジリエンス法

- デジタル要素を備えた製品（ソフトウエア含む）の製造者に対し、**①セキュリティ特性要件に従った上市前の設計製造、②上市後に積極的に悪用された脆弱性・インシデントの報告等を義務付け**。
- 報告義務の運用開始は2026年9月、その他は2027年12月開始予定。

PSTI法

- 英国内で主に消費者向けIoT機器の製造や流通、販売を行う事業者に対し、**3つのセキュリティ要件※を含むセキュリティ対策の遵守を義務付け**。
- 2024年4月に適用開始。

※共通パスワード設定の禁止、脆弱性情報の提供、セキュリティサポート期間の明示。

②企業のサイバーセキュリティ対策水準の整備・可視化

サイバー・エッセンシャルズ

- 英国NCSCが全ての**企業を対象に**一般的なサイバー攻撃への防御策を提供することを目的として設計した、自己適合、第三者診断の**二段階で構成される認証制度**。
- 一部政府及び公的機関の調達において必須要件として課される場合がある。

※豪州においても、すべての組織を対象とする４段階の基準（エッセンシャル・エイト）が存在。
※米国においても、米国防省がその請負業者等と共有する機密性の高い情報の保護を目的に設計したサイバーセキュリティ成熟度モデル認証（CMMC。2023年12月に2.0版が発効。）が存在。

③中小企業向けサイバーセキュリティ対策促進支援

サイバー・アクション・ツールキット

- 英国NCSCが**個人事業主・小規模組織向けにサイバーセキュリティ対策支援ツールを無料で提供**。（2025年10月公表）

サイバー・エッセンシャルズ取得支援

- 英国NCSCがサイバー・エッセンシャルズの**認証取得を支援するツール**（準備計画策定支援、自己評価質問票等）を提供。

小規模事業者サイバーセキュリティパイロットプログラム

- 米国中小企業庁が州政府を通じて、サイバーセキュリティ対策が困難な**中小企業向けにサイバーセキュリティ対策の研修やコンサルティングを提供**。

目次

「サイバーセキュリティ産業振興戦略」の概要（2025年3月公表）

- サイバーセキュリティ対策の必要性が高まる中で、①**企業が適切なセキュリティ製品を選択できるようにする**、②**我が国へのサイバー攻撃の特異性にも対応し安全保障を確保する**、③**拡大するデジタル赤字解消に貢献する**との観点から、我が国セキュリティ産業振興が不可欠。
- 現状、**国内で活用される製品の多くを海外製が占めており**、ユーザーは、**これまでの利用実績や価格を重視**。結果として我が国セキュリティ産業は、「**買い手がつかないので儲からない**」「**儲からないので事業開発や投資が十分なされず競争力が低下**」**という悪循環**に陥っている。
- こうした現状を打破するため、**製品開発の出口をまず確保**した上で、**シーズの発掘・事業拡大を後押し**する、**包括的な政策対応**を提示。

今後の成長に向けた課題（As-Is）

導入実績が重視される商慣習

- 新規製品が販売されても、実績が重視されるため、調達先が存在せず、事業として成り立たないため、企業が育たない

十分な開発投資が行われにくい事業環境

- 安定的な収益基盤が見通しづらいため、製品開発・研究開発への投資が限られる
- セキュリティ製品の販売はSIerが商流を担っており、製品ベンダーで対応できる余地は限られている

セキュリティ産業全体を支える基盤の不足

- 人材育成や国際市場の開拓等、産業全体を支える基盤は重要であるものの、個社での対応が難しい

目指すべき方向性（To-Be）と実現のための主な政策対応

スタートアップ等が実績を作りやすくなる／有望な製品・サービスが認知される

- 「スタートアップ技術提案評価方式」等の枠組みを活用し、**政府機関等が有望なスタートアップ等の製品・サービスを試行的に活用**（中長期的には主体・取組を拡大）
- **有望な製品・サービス・企業の情報を集約・リスト化**し、政府機関等へ情報展開する／業界団体とも連携して審査・表彰を実施

有望な技術力・競争力を有する製品・サービスが創出され、発掘されやすくなる

- セキュリティ関連の技術・社会課題解決に貢献する技術・事業を発掘するための「コンテスト形式」による**懸賞金事業**等を実施（中長期的には安定供給確保策も検討）
- **約300億円の研究開発プロジェクト**を推進し社会実装を後押し
- 我が国商流の中心である**SIerと国産製品・サービスベンダーとのマッチング**の場を創出

供給力の拡大を支える高度人材が充足する／国際市場展開が当たり前になる

- 高度専門人材の育成プログラムを拡充／セキュリティ人材のキャリア魅力を向上・発信
- 海外展開を支援／標準化戦略を促進／関係国との企業・人材交流を促進

今後のロードマップ

①３年以内：「企業・人材数の増加」　②５年以内：「我が国企業のマーケットシェアの拡大」「重要技術の社会実装」
③10年以内：「安全保障の確保やデジタル赤字の解消への貢献を実現」**【KPI：国内企業の売上高を足下から3倍超（約0.9兆円⇒3兆円超）】**

※前提として、サイバーセキュリティ市場の「需要」の拡大につながるような各種の取組も同時に推進。

（参考）政府戦略文書等との関係

新しい資本主義のグランドデザイン及び実行計画2025年改訂版（令和７年６月13日閣議決定）（P44-45）

Ⅲ．投資立国の実現　３．ＧＸ・ＤＸの着実な推進（２）ＤＸ　④サイバーセキュリティ

IoT製品に関する「セキュリティ要件適合評価及びラベリング制度」を早期に政府機関等における調達の選定基準に含める。模擬プラントの整備、大規模演習環境の構築を通じて、高度化するサイバー攻撃に対応できる人材の育成、「サイバーセキュリティお助け隊サービス」の普及や見直しを通じた中小企業への支援を進める。

また、**政府機関等におけるスタートアップ製品・サービスの積極的な活用**や**信頼性の高いサービス提供事業者の認定制度の整備**、**研究開発プロジェクトの拡充に向けた検討**等を着実に実施する。あわせて、未知の脅威情報や脆弱（ぜいじゃく）性を検知する国産ソフトを開発し、政府端末等へ順次導入を図るとともに、情報収集やＡＩ活用による高度分析の結果の民間活用により、国内ベンダによる製品化を加速させる。

デジタル関連産業のグローバル化促進のための施策（令和７年９月19日デジタル関連産業のグローバル化促進のための関係閣僚会議決定）（P1-2）

１．国際競争力を持つデジタルソリューションの創出及び海外展開の促進

進展著しいAI、及びそれを支えるデータの利活用を強力に進めつつ、製造業や行政を含むサービス業等の分野において、高い品質のデータを元に、国際競争力を持つAIを核とするデジタルソリューションを創出する。そうした幅広い AI 開発の基盤となる汎用モデル等の開発も進めるとともに、**デジタル化の進展に伴い重要となるサイバーセキュリティ産業の振興を図る。**

（略）

（国際競争力を持つデジタルソリューションの創出）　（項目抜粋）

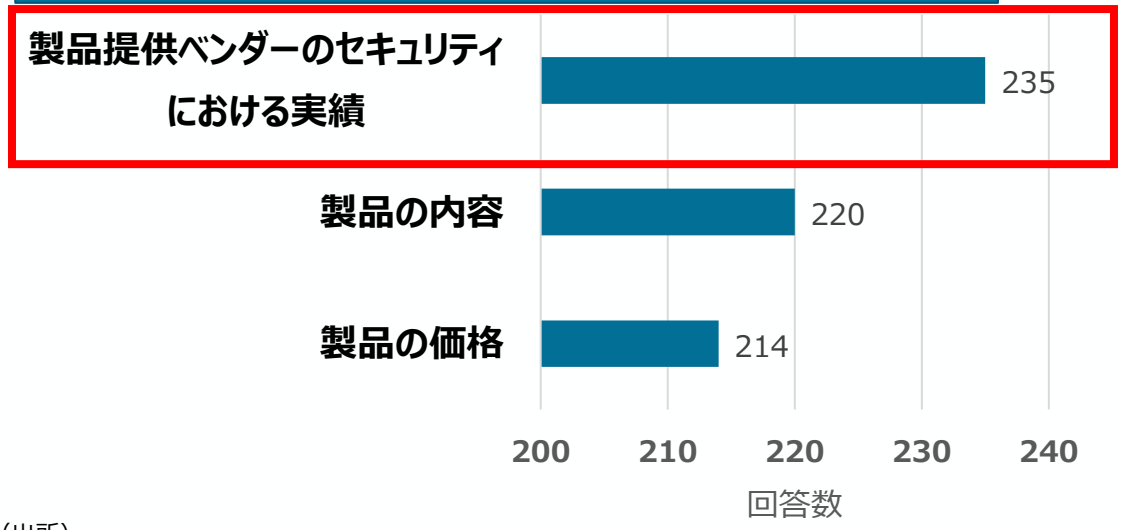
・公共調達や研究開発支援、セキュリティが確保された製品の認証等によるサイバーセキュリティ産業振興

目次

IPAによる有望セキュリティ・スタートアップ製品・サービス等の積極的な調達実証事業

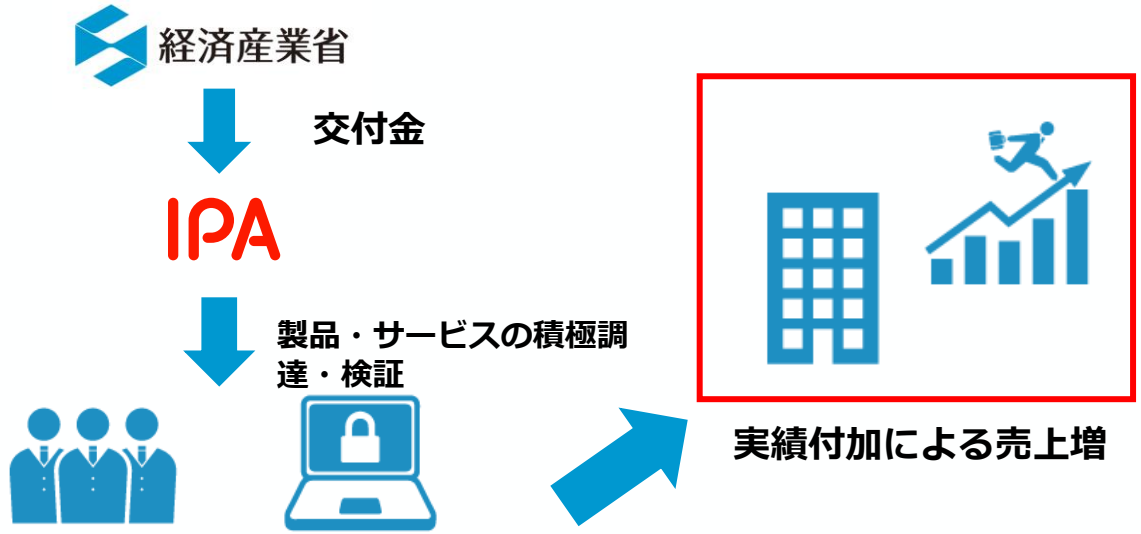
- 現状、**国内で活用される製品の多くを海外製が占めており**、ユーザーは、**これまでの利用実績や価格を重視**。我が国**セキュリティ産業が更なる成長を遂げるには、導入実績が重視**される等という商慣習を踏まえた上で、新規参入のハードルとなっている点を打破する政策が必要。
- 2025年９月19日にデジタル関連産業のグローバル化促進のための関係閣僚会議決定においても、国内スタートアップ企業の実績をつくり新規参入におけるハードルを低減するために、**セキュリティに知見を持つIPAが国内の有望なスタートアップの製品・サービスを優先的に調達等する施策**が提言された。
- 2026年３月頃からIPAで順次調達を開始（R７年度補正予算　12.4億円）。今後、**製品・サービスの有効性検証を行うための環境整備の構築を行い、調達した製品の評価を行う実証事業**を実施予定。

製品を選定する際に最重要視する項目
（上位３項目、国内ユーザー企業からのアンケート）



（出所）
富士キメラ総研「2023 ネットワークセキュリティビジネス調査総覧〈市場編〉」を基に作成。
https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165
https://www.jnsa.org/result/surv_mrk/2025/2024_securitymarket.pdf

製品･サービスの調達スキーム



国産ベンチャーマッチングイベント推進

- 日本ネットワークセキュリティ協会が中心となり、SIerと国産ベンチャー製品のマッチングを推進。2025年10月に「国産セキュリティ推進フォーラム」を開催し(経産省も共催)、**約80名が参加して国産技術振興の課題を議論。今後はテーマを絞った小規模なマッチングイベント**を予定。
- 防衛装備庁とも連携し、**２月に自衛隊とのマッチングイベントを実施**。引き続きニーズに応じた情報収集と支援を行う。

SIerと国産製品のマッチング

✓日本ネットワークセキュリティ協会(JNSA)が中心となり、我が国商流の中心となっているSIerと国産ベンチャー製品とのマッチングを推進。2025年10月には、経産省とJNSAが共同で「国産セキュリティ推進フォーラム」を初開催。

✓本フォーラムでは、製品・サービスを開発する事業者やスタートアップ、それらを取扱うSI事業者や販売代理店、国内サイバーセキュリティ企業への投資に特化したファンド運営者、ベンチャーキャピタリストなど約80名が参加し、国産振興に係わる課題やその解決策を議論。

✓今後は、テーマを絞ってより小人数でのマッチング精度を高めたイベントを開催(2026年4月予定)。事前事後のアンケート調査により、マッチング精度を可能な限り高めつつ進める。

JNSA

防衛装備庁と国産技術のマッチング

✓防衛装備庁と協力し、2026年2月3日に陸海空自衛隊等とのマッチングイベントを開催予定。

✓防衛装備庁のニーズ等を踏まえ、次回のマッチング機会に備えて引き続き支援を行う。

防衛省・自衛隊

サイバーセキュリティ関連技術に関する懸賞金事業

- セキュリティ対応力強化が求められる一方、特に中小企業では、コストの負担や人材不足により対策が進みにくい状況。また、提供側も導入実績が重視される商慣習から、スタートアップ企業等が実績を築きにくいといった課題が存在。
- こうした状況を踏まえ、**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**を募集する。
- ✓ 従来の人手依存やルールベース運用では対応しきれない高度化する脅威に対し、**迅速で実効的に解決する技術**や**現場に無理なく導入・定着させるための技術開発・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。

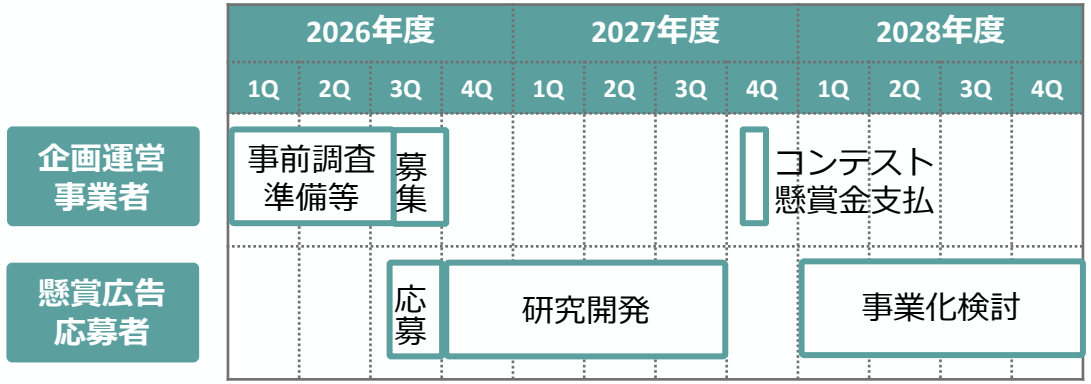
懸賞金テーマ：サイバーセキュリティの技術

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）

懸賞金事業の想定スケジュール

以下のスケジュールを想定し、現在、募集に向けた事前調査を実施。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。



経済安全保障重要技術育成プログラム：先進的サイバー防御機能・分析能力強化事業の拡張

- 経済安全保障重要技術育成プログラム（先進的サイバー防御機能・分析能力強化）事業として、我が国のサイバー領域における状況把握力・防御力を向上させる目的として、2024年7月から2029年3月までの期間で研究開発が既に進められているところ、

① サイバー対処能力法等が2025年５月に成立・公布し、これまで以上にサイバー安全保障に資する技術が不可欠となり、

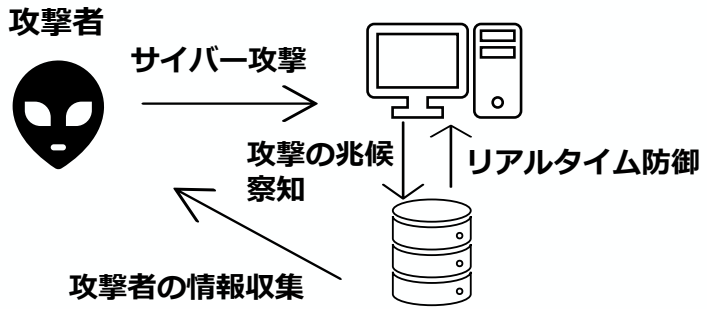
② AIの急激な進歩により攻撃手法が多様化し、AIを用いたセキュリティ技術の研究の必要性も増大、

③ 地政学リスクを含むサイバーリスクが高まる中、国内産業基盤の強化を通じた供給力を早急に拡大する必要性が増大している。

- **現行のプロジェクトに新たな研究開発項目を追加し、 2026年5月以降から開始予定。**（プロジェクト全体額は、290億円から376億円を超えない範囲に増額）。

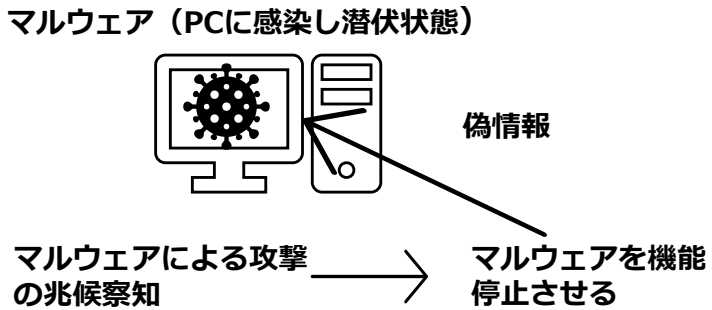
（１）サイバー空間の情報を収集・分析する状況把握力の向上

- 攻撃前におけるリアルタイムな攻撃の検知・特定に繋がる、攻撃者の特定のための情報収集技術開発
- IoT機器に利用されるファームウェアの大規模な収集・分析による各種セキュリティリスクの可視化・評価に係る技術開発



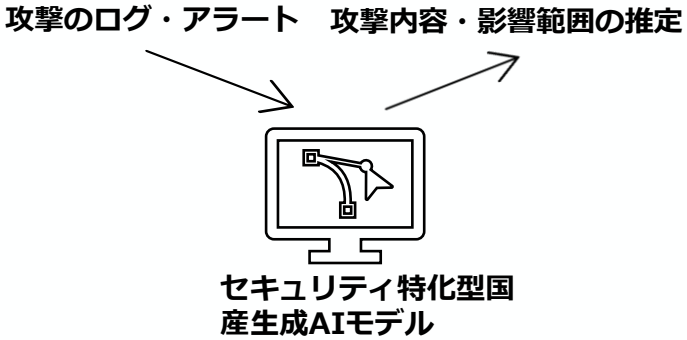
（２）サイバー攻撃から機器やシステムを守る防御力の向上

- 攻撃兆候の察知時に、リアルタイムで既に侵入しているマルウェアを機能停止させる技術
- 攻撃元の情報の正確性を評価・担保する技術



（３）共通基盤の整備

- 国産セキュリティ特化AIモデルの実現
- 高度サイバー安全保障人材の評価・管理に関する研究開発
- 攻撃の兆候を早期に発見して迅速に対処する技術の研究開発が可能な共通基盤の構築



（参考）先進的サイバー防御機能・分析能力強化事業（改定構想の概要資料（案））

背景

- サイバー空間の「公共空間化」が進展し、サイバー空間において提供される多様なサービスが複雑化するに伴いサイバー空間内やサイバーとフィジカルの垣根を超えた主体間の「相互連関・連鎖性」が一層深化している。
- 近年では、**人工知能（AI）を活用した攻撃に代表される新たなサイバー攻撃のリスクや、量子計算機の活用の広がりに伴う既存暗号の危殆化によりデータが漏洩するリスクが顕在化**している。**これに対応するため、進歩したAIを用いたセキュリティ技術の研究の必要性も増大している。**
- **地政学リスクを含むサイバーリスクが高まっていることにより、国内産業基盤の強化を通じた供給力を早急に拡大する必要性が増大している。**
- 「自由、公正かつ安全なサイバー空間」を確保するためには、これらをとりまく不確実性の変容・増大によって生じるリスクを適切に把握した上で対応していくことが必要となっている。
- **加えて、サイバー対処能力強化法及び同整備法が2025年5月に成立・公布したことにより、これまで以上にサイバー安全保障に資する技術が不可欠である。**
- 先進的なサイバー防御機能や分析能力を強化していくことは、経済安全保障の確保・強化の観点から重要であるため、**サイバー空間の状況把握力や防御力の向上に資する技術や、セキュアなデータ流通を支える暗号関連技術等を開発**し、我が国のサイバー領域における状況把握力・防御力を飛躍的に向上させることを目的とする。

想定される利用ニーズ

- サイバー空間の情報把握力や防御力を向上させる技術については、民生利用・公的利用の両面において実施されている**特定、防御、検知、対応、復旧**といったサイバーセキュリティに関するオペレーションにおいて実装されることが想定される。
- セキュアなデータ流通を支える暗号関連技術については、民生利用・公的利用の両面において、**大量のデータの高速伝送が必要である一方で秘匿化が求められる回線での活用が想定**されることや、**量子計算機が活用されるデバイスに対して暗号機能が付加されることが想定**される。

研究開発の内容

（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（**攻撃リアルタイム検知の為の情報収集技術、IoT機器ファームウェアの収集分析とリスク可視化** を追記）
- 攻撃主体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（**攻撃兆候の察知時に既に侵入しているマルウェアを機能停止させる技術、攻撃者の真のサーバを高精度で短時間に特定する技術** を追記）
- 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

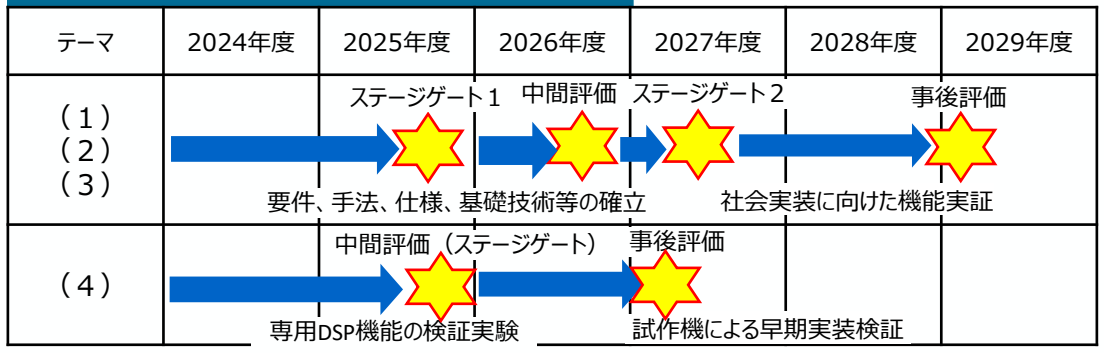
（３）共通基盤の整備

- 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（**高度サイバー安全保障人材の育成に資する研究開発・ツールの開発** を追記）
- **国産生成AIモデル等を活用した国産セキュリティ情報共有基盤の整備**

（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

想定スケジュール



サイバーセキュリティ・サービス事業者の信頼性強化に向けた制度

- デジタル化の進展や地政学リスクに伴うサイバーリスクの増加等を踏まえ、**今後サイバーセキュリティ・サービス**（とりわけ、顧客の機微情報やシステムへのアクセスを許容する形態のもの）**に対するニーズが増加することが見込まれる**中、**サイバーセキュリティ・サービス提供事業者の体制・措置等に起因する事案等が生じている**ことに鑑みると、**サービス提供事業者の「信頼性」の一層の強化（厳格な社内体制の整備等）が求められる。**
- また、政府機関や安全保障に関係する事業者等においては、**高度な「信頼性」を有するサイバーセキュリティ・サービス事業者を選定・活用するニーズ**が想定される。
- こうしたことを踏まえ、既に技術・品質の基準に基づき登録を行っている現行の「**情報セキュリティサービス審査登録制度**」**に登録しているサイバーセキュリティ・サービス提供事業者**を対象に、**「事業者の信頼性」を確認**する認定制度を創設するべく、検討を進めていく（2026年4月頃に制度の方向性を提示し、制度の詳細設計を進め、**2027年度中の運用開始を目指す**。）。

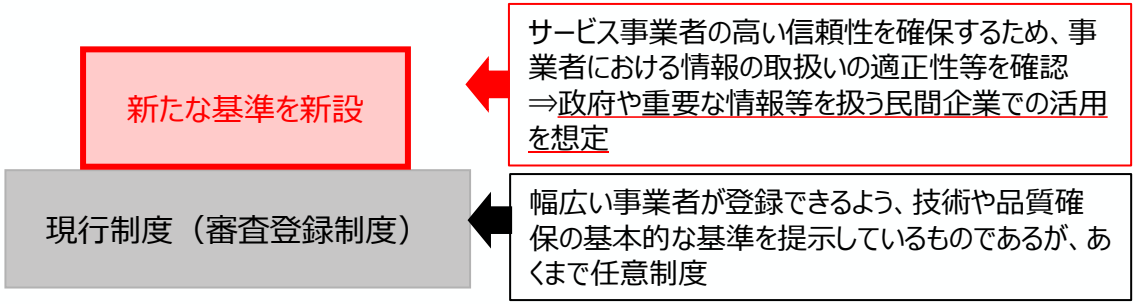
現行制度のサイバーセキュリティ・サービスの種類

（１）情報セキュリティ監査サービス
（２）脆弱性診断サービス及びペネトレーションテスト（侵入試験）サービス
（３）デジタルフォレンジックサービス
（４）セキュリティ監視・運用サービス
（５）機器検証サービス

＜制度（イメージ）＞

○サイバーセキュリティ・サービス認定制度

リストに掲載された企業から申請を受け、信頼性を確認、認定。



目次

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

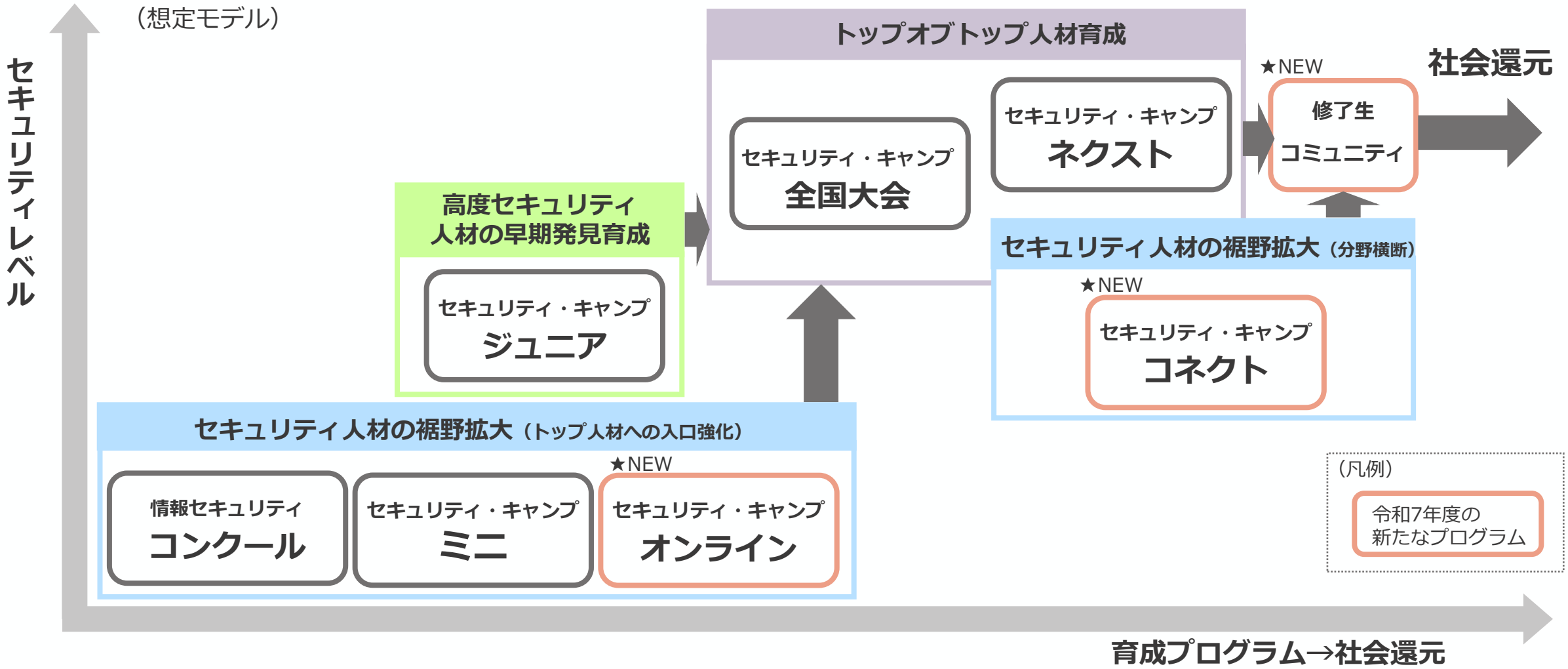
(3)情報処理安全確保支援士(登録セキスペ)

- **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。

(1)セキュリティ・キャンプの目的・全体像

- 産業界にも資する高度なセキュリティ人材の育成を目的としてセキュリティ・キャンプを継続的に実施。
- 近年のサイバーセキュリティ脅威の拡大に対応すべく、人材の裾野拡大に向け、**令和7年度は、新たなプログラム（セキュリティ・キャンプ コネクト、セキュリティ・キャンプ　オンライン）を導入するとともに、修了生支援を開始。**

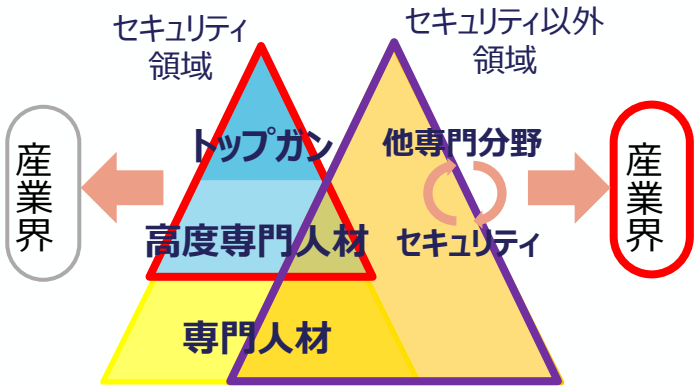


(1)セキュリティ・キャンプ コネクト

- サイバーセキュリティの脅威の拡大により、**あらゆる領域**の人材においてもセキュリティを学ぶ必要性が高まっている。また、全国大会では応募者増に対し講師不足から参加枠が横ばいとなっており、受入れ拡大が難しい状況。
- そこで、令和7年度より、**セキュリティと他分野の専門性を併せ持つ人材を育成する新プログラム「セキュリティ・キャンプ コネクト」**を実施。25年度はプレ開催、本開催を実施し、合計52名が参加。

セキュリティ・キャンプ コネクトの目的

✓ セキュリティと他分野を掛け合わせ、**多面的な視点からセキュリティを検討できる人材を育成し、社会で活躍できる人材の輩出。**



参考：AI×セキュリティ

✓ AIに触れる学生を対象に、**AI技術に内在するセキュリティ課題を体系的に学ぶ**カリキュラム

参考：法律×セキュリティ

✓ 法律を専攻している学生を対象に、**サイバーセキュリティに強い法律家を目指す学生向け**カリキュラム

本開催

✓ 令和8年3月26日～ 29日に実施。
✓ テーマは以下の6つ
- 法律：サイバー関連の法律課題
- AI：AI技術に内在するセキュリティ課題
- 脅威：攻撃者視点での脅威情報収集
- デバイス/OS/IoT：各製品開発におけるセキュリティ課題

✓ 本開催より、クラス横断型のカリキュラム「**コネクトワーク**」を導入。多種多様な分野の受講生同士の交流を通じて、新たな視点からセキュリティ課題を検討。

令和８年度以降の取組

✓ 受講生からのフィードバックや時流・産業界のニーズに応じて、**カリキュラムは毎年検討を行う**ことを想定。
✓ 本年度は応募が高倍率となり受入れ可能数を超過したため、受講生の**支援対象の拡大に向けた運用改善**等も検討予定。

(1)セキュリティ・キャンプ修了生のコミュニティ整備

- **修了生の更なる成長やキャリア形成、習得した知見の社会還元及びセキュリティ人材のキャリアの魅力発信を支援**するため、**修了生や講師等のネットワークを形成・維持**し、お互いを高め合える場として、修了生のコミュニティを整備。

修了生の交流活動

✓ 修了生や講師等との年度を超えた交流の場の提供、修了後の活動成果発表を通じた修了生の認知度向上及び産業界での活躍に向けたきっかけの提供を目的として、**「キャンプフォーラム」**を継続的に実施。
（直近では令和８年２月中旬に実施）

（過年度の開催状況）

修了生コミュニティ立上げに向けて

✓ 交流の入り口となる基盤整備として、**公式SNSプラットフォームの運用をスタート**。（令和８年３月下旬開始予定）
✓ 運用開始後の支援策について、以下３つのコンセプトを基に、修了生に対するアンケートも踏まえ、具体化に向けた検討を実施。

知見の蓄積・深化	修了生の継続的な学び、最新技術や研究成果の共有等の機会を提供し専門性を高める。
活動状況の共有	修了生同士が相互に知見、修了後の活動状況等を共有・公開し、セキュリティ人材としての価値を高める。
知見の社会還元	講師等としてのキャンプへの参画や政府機関・組織等の活動への協力等を通じた知見・技能の社会還元。

令和８年度以降の取組

■ 公式SNSプラットフォームの運用開始を契機として、**コミュニティに参加しやすい環境を整備**
➢ オンラインのLT大会・キャリア相談会、イベント紹介並びに公式SNSによる宣伝など

■ **修了生のキャリア支援と可視化並びに技術支援の強化、キャリアの魅力発信、交流の深化**などによる活性化
➢ ワークショップの実施、インターン・社会見学（未踏発企業など）の情報提供、修了生のキャリアの把握並びに外部イベントへの出展による地方在住の修了生の取り込みなど

■ **持続可能な体制の確立、社会貢献**を見据えた**コミュニティの推進・拡張**
➢ 企業・省庁・大学等とのコラボイベント実施や、修了生が自ら企画し運営できるよう、修了生を運営メンバーに組み入れの検討など

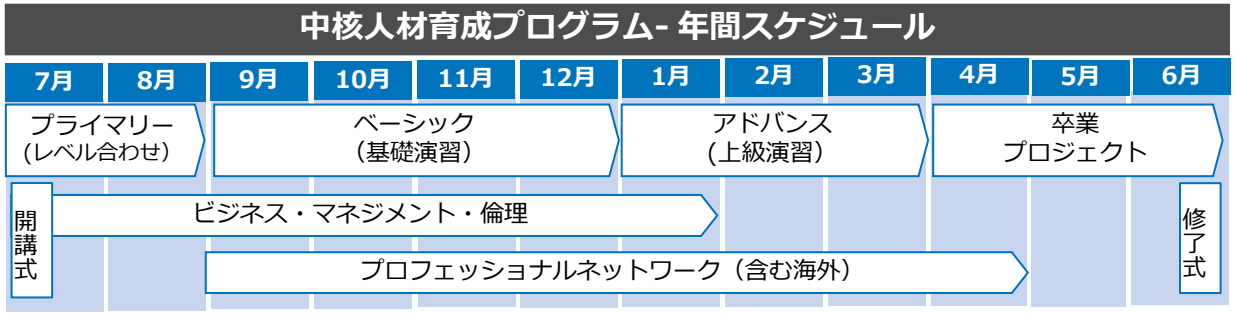
(2)IPA産業サイバーセキュリティセンター（ICSCoE※）

2017年4月設置

- 社会インフラ・産業基盤における防護力の強化のため、OT(制御技術）とIT（情報技術）の知見を結集させた**世界レベルのサイバーセキュリティ対策の中核拠点**として、IPA内に発足。
- ICSCoEでは世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ１年の集中トレーニング等を実施。

□　１年を通じた集中トレーニング「中核人材育成プログラム」

□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣、9期生まで約550名が受講
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人、第８期：57人、第９期：55人）

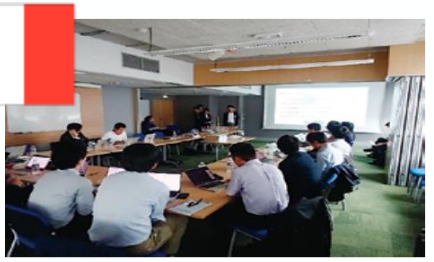


- IT系・制御系に精通した専門人材の育成
- 模擬プラントを用いた対策立案
- 実際の制御システムの安全性・信頼性検証等
- 攻撃情報の調査・分析

現場を指揮・指導するリーダーを育成

□　米・英・仏等の海外とも協調したトレーニングを実施

➢ CISA※が開催する高度なサイバーセキュリティトレーニングである301演習への参加



➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

※ICSCoE：Industrial Cyber Security Center of Excellence
※CISA：Cybersecurity and Infrastructure Security Agency

(2)2025年日本国際博覧会（大阪・関西万博）での支援（修了者の活躍）

- IPA ICSCoEは、大阪・関西万博における設備制御システムのセキュリティを確保するため、開催前から開催中に亘り、以下の支援を実施。
- そのうち、開催中に実施したセキュリティインシデント対応に関する業務では、**中核人材育成プログラム修了者**ほか、計12社18名で対応体制を構築し、**国際的な大規模イベントのセキュリティ確保に寄与**。

開催前（2023年10月～2025年4月）

- 博覧会協会が会場（夢洲）に設置予定の設備制御システムについて、リスク分析を実施。
- 特に対策の優先度が高い施設・重要システムを選定し、それらの実装状況の確認及びセキュリティ検証を実施。

セキュリティ検証
（パケットキャプチャ）

開催中（2025年4月～2025年10月）

- **セキュリティインシデント対応に関する業務**
  - 継続的に会場の見回りを行い、サイバー攻撃等による脅威の兆候を把握・分析し、定期的に博覧会協会へ報告。また、見回りにおいて発見したリスク要因について対策の提案等を実施。
  - 博覧会協会からの要請に基づき、緊急的なインシデント対応として会場への駆け付けを行い、発生事象の分析、対策の提案等を実施。
  - 修了者所属企業（五十音順）
    アズビル㈱、㈱オプテージ、㈱きんでん、ダイキン工業㈱、ダイキン情報システム㈱、大和ハウス工業㈱、中部電力㈱、西日本旅客鉄道㈱

(2)ICSCoEで実施するプログラム拡充に向けた新しい取組

- 産業界のニーズに応え、より一層のプログラムの充実を図るため、模擬プラント/システム構築等の環境整備・短期プログラムの新設に取り組んでいる。

1．電波暗室の整備

- 部屋の内部には今後船舶関連プラントを設置することを念頭に、[外部からの電波を遮断し、部屋内部では電波の乱反射を防ぐ]電波暗室を整備。
- これまで建屋内で実施が困難であったドローンなど電波を使った機器を用いたサイバー攻撃のシナリオが実施可能に。

2．機械製造模擬プラント/システムの整備

- 重要物資として指定されている半導体をはじめ、多くの製造事業者向けに活用が可能な模擬プラント/システムを拡充。
- 工程の多くが自動化されている現代の工場オペレーションに係るサイバーセキュリティ上の課題の洗い出しや対策に係る検討に最適な環境が提供可能に。

3．AIに関する短期プログラムの提供

- AI×OTに係るセキュリティ教育を念頭にしつつ、OTの現場でAI活用が進展することを想定し、AI活用の手法からそれによるリスクや対策までをカバーするプログラムを提供。
- AIが急速に普及する現代において、OTの現場への活用に対して先手を打つ形でプログラムを提供し、セキュリティ確保を前提としたAI導入を促進。

(1)(2)先端技術に対応した人材育成プログラムの供給

- AIの進展を踏まえた人材育成の取組について、**AIに係る安全性確保（Security for AI）**や**AIを活用したサイバーセキュリティ確保（AI for Security）**などの観点から、**育成プログラムを拡充。**
- 模擬プラントを用いた演習を通じ、**ロボット（製造機械）等**や**半導体**領域におけるセキュリティ人材育成を強化予定。

※実施済み及び実施予定を含めた主な提供プログラムの一例

AI

Security for AI

■ **セキュリティ・キャンプ　コネクト**

✓ LLMアプリケーションやAIエージェントの活用が急速に進展する中、AIセキュリティに関心を持つ学生を対象として、理論と実践を体系的に学ぶことができる講義を実施予定。

✓ 令和７年９月にはプレ開催を行い、５名が受講。

■ **AI×OTに関する短期プログラム**

✓ 既に制御システム処理や運用オペレーター支援等でAIが活用され始めており、AI導入のニーズが高まっている。

✓ AI活用に必要な知識（リスクなど）や技術に係る教育を２日間で提供予定。

AI for Security

■ **セキュリティ・キャンプ（全国大会）**

✓ AIエージェントを活用したセキュリティ業務の自動化の基礎を体験し、実際の業務で応用できるスキルの習得に向けたカリキュラムも実施。

✓ ハンズオンを通じて、RAGやエージェント連携、外部サービスとの連携方法、実装時のセキュリティ上の注意点などを学習。

ロボット・半導体

■ **製造機械模擬プラントの新設**

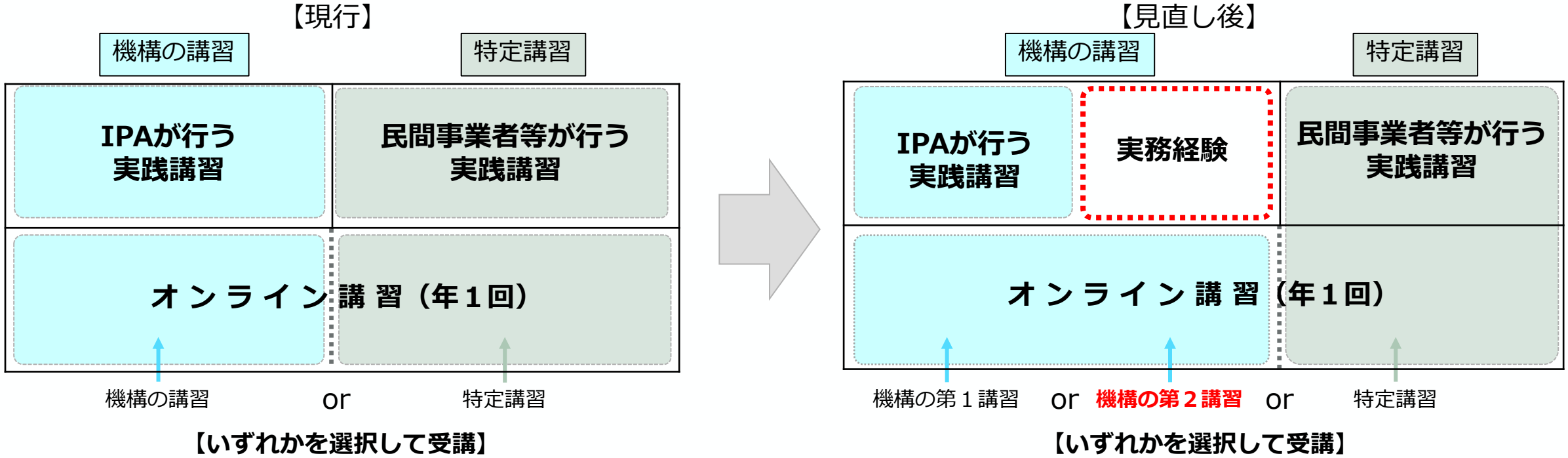
✓ 2025年9月に開催された人工知能戦略本部において「フィジカルAI」の開発・普及等の方針が示され、AI・先端半導体を活用したロボット（製造機械）等の実装が一層進展していくことが想定される。

✓ こうした状況の中、ロボット（製造機械）等を狙った新たなサイバー攻撃への対応や半導体等の製造分野に広く活用可能な機械製造模擬プラントを新設予定。

(3)登録セキスペの制度見直し（実務経験者に対する講習制度創設の背景）

- サイバーセキュリティ分野で必要とされる知識が技術の進歩により変化している中、**情報処理安全確保支援士には、サイバーセキュリティの専門家としてその知識や技能を最新の状態としておくために、講習受講が課せられている。**
- 一方、情報処理安全確保支援士の中には、**実践講習で得られる知識・技能と同等以上の知識・技能を、企業のサイバーセキュリティ対策の支援等の実務を通じて得られるケース**がある。
- また、更新制度が実施されている中で、**実務から遠のいている情報処理安全確保支援士を実務に向かわせるインセンティブを設定**することが、情報処理安全確保支援士の一層の活用促進、ひいては事業者のサイバーセキュリティ対策向上に資する。

このような講習制度や情報処理安全確保支援士の実務の実態を踏まえ、**実務経験から、講習から習得できる知識・技能と同等以上の知識・技能を得ている情報処理安全確保支援士に対して、受講すべき講習をオンライン講習のみとする、新たな講習制度を創設。**
（当該講習制度の申請受付は、令和８年４月１日から開始予定。）



（参考）登録セキスペの制度見直し（実務経験者に対する講習制度の概要）

実務経験者に対する講習制度とは、**下表の実務経験を積んでいる情報処理安全確保支援士に向けた新たな講習制度**であり、具体的には、当該情報処理安全確保支援士が受講する講習をオンライン講習のみとするもの。

実践講習として求める要素

・ＩＴスキル標準レベル４相当（一つまたは複数の専門を獲得したプロフェッショナルとして、専門スキルを駆使し、業務上の課題の発見と解決をリードするレベル、プロフェッショナルとして求められる、経験の知識化とその応用（後進育成）に貢献するレベル）

・情報処理安全確保支援士試験の出題分野の内容を含む

～ 特定講習（※）募集等要領（抜粋）～　　（※民間事業者等が行う実践講習部分を指す）
・・・特定講習は「ＩＴスキル標準レベル４相当」とし・・・登録セキスペの知識・技能の継続的な維持・向上を図り、実践的な活用力を修得 できるものであることが必要なため、特定講習が対象とする科目は、「情報処理安全確保支援士試験」の出題分野の内容を含むこと・・・

実務経験者に対する受講制度の対象となる実務の方向性

○ＩＴスキル標準レベル４に相当する、情報処理安全確保支援士試験の出題科目に該当するもの
○上記以外で、実務経験者に対する講習制度の対象とすることが望ましいもの
から、ＩＰＡ有識者検討会での議論を踏まえて以下のとおり決定

○ＩＴスキル標準レベル４相当の情報処理安全確保支援士試験の出題科目に該当するもの

対象業務	情報処理安全確保支援士試験出題科目の該当項目
セキュリティ監査／システム監査 セキュリティ統括	1．情報セキュリティマネジメントの推進又は支援に関すること
デジタルシステムストラテジー デジタルシステムアーキテクチャ デジタルプロダクト開発 デジタルプロダクト運用	2．情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること 3．情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること
脆弱性診断・ペネトレーションテスト セキュリティ監視・運用 セキュリティ調査分析・研究開発	2．情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること 3．情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること 4．情報セキュリティインシデント管理の推進又は 支援に関すること
※いずれも、一定期間（６か月/１年）の従事期間を満たした場合に限る。	

○左表以外で実務経験者に対する講習制度の対象とするもの

対象業務	採用理由
セキュリティ経営 デジタル経営	特定講習 募集等要項(*) 別表１において講習の対象外とされる「経営層」について、ITSS＋（セキュリティ領域）分野に従い、左表の従事期間を満たすことで実践講習と同等の役割があると判断
情報セキュリティ規程の整備 情報資産の洗い出しとリスク分析 クラウドサービスの安全利用 セキュリティインシデント対応 従業員向け情報セキュリティ教育	「中小企業向けサイバーセキュリティ対策支援者リスト」に掲載される者が、左記指導テーマに基づく支援業務として、３回以上の中小企業への支援実績がある場合に限り、実践講習と同等と判断
ＩＰＡまたは民間事業者等が行う実践講習の講師	講師として２回以上登壇した場合に限り、実践講習と同等と判断

*出典： 経済産業省「情報処理安全確保支援士特定講習」募集等要領 別表１ https://www.meti.go.jp/policy/it_policy/jinzai/bosyuu250922.pdf

（参考）効率的・効果的な人材の育成・確保に向けた基盤整備

- 産学官で連携し、人材の育成・確保を推進するためには、セキュリティ領域における**多様な職種や各職種に求められるスキルの定義・キャリアパスの可視化**などの**基盤整備が重要**であり、省庁横断で取組を検討中。

人材フレームワーク（国家サイバー統括室）

セキュリティ人材に求められる役割・スキル等を整理した**官民共通の「人材フレームワーク」**の策定を検討中。
（令和８年４月以降に公表予定）

■ NICEフレームワークのカテゴリ別に、13の人材像を整理すれば以下のとおり（グレーは一部含む）。

Oversight and Governance（監督・ガバナンス）	Design and Development（設計・開発）	Implementation and Operation（導入・運用）	Protect and Defense（保護・防御）	Investigation（捜査）
①意思決定・戦略策定				
②戦略推進・プロジェクト管理		②戦略推進・プロジェクト管理		
		③監視		
			④対処	
		⑤情報収集・分析・共有	⑤情報収集・分析・共有	⑤情報収集・分析・共有
			⑥脆弱性評価	
			⑦フォレンジック	⑦フォレンジック
⑧運用管理				
⑨教育・訓練				
⑩法務				
⑪監査				
⑫研究				

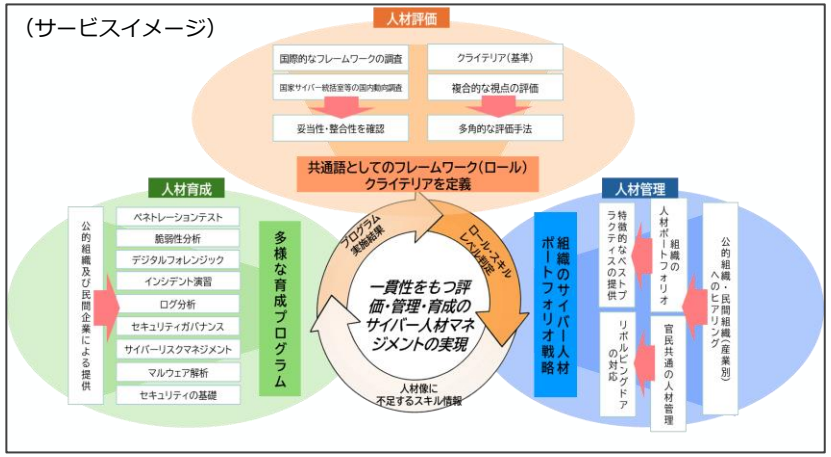
⑦フォレンジック	当該役割を担う人材が所属する組織				
	政府機関	民間企業（サプライチェーン）		民間企業（アウトソース先等）	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	●	●	–	●	–
おもな役割	● サイバーセキュリティインシデントが発生した際に、デジタルデータの証拠保全対象を判断し、適切なツールで証拠保全を行う。 ● 証拠保全の対象としたデジタルデータを分析し、人材像「対処」と連携し、セキュリティインシデントを調査・報告する。 ● 司法執行権を有する政府機関がサイバー犯罪に対する捜査を行う。				
NICEフレームワークにおける対応ロール	デジタルフォレンジック				PD-WRL-002
	サイバー犯罪捜査				IN-WRL-001
	デジタル証拠解析				IN-WRL-002
補足説明	● 適切な証拠保全や原因調査等には専門的なスキルが要求されることから、一般の企業等では自社で当該業務を担う人材を有さず、外部委託により対応することが多い。 ● 経済産業省の情報セキュリティサービス審査登録制度における「デジタルフォレンジックサービス」に従事する人材に相当。				

出典：国家サイバー統括室（NCO）「サイバーセキュリティ人材フレームワークに関する検討会 第2回会合（令和７年12月18日開催）」
資料4 人材像（案）の修正案について

経済安全保障重要技術育成プログラム（高度サイバー人材に関連するサービス）

高度サイバー人材について、知識・スキルの適切な把握を行うとともに、**評価・管理・育成が効率的/効果的に連動するサイバー人材マネジメントスキーム**の構築を検討中。

（サービスイメージ）



デジタル人材スキルプラットフォーム（IPA）

個人のデジタルスキル情報の蓄積・可視化により、デジタル技術の**継続的な学び**を実現するとともに、**スキル情報を広く労働市場で活用**するための仕組みとしてIPAにおいて、**プラットフォームの開発**を検討中。

出典：経済産業省「Society 5.0時代のデジタル人材育成に関する検討会 報告書」

上記のような**基盤整備の動きを注視**し、セキュリティ・キャンプ事業や中核人材育成プログラムなどの**既存プログラムとの有機的な連携**を検討予定。

目次

インド太平洋地域向け産業制御システム・サイバーセキュリティ演習

- 経済産業省とIPA産業サイバーセキュリティセンター(ICSCoE)が、**米国・EU政府等と連携し、毎年開催するインド　太平洋地域向けの1週間の研修プログラム**。これまで2018年度より8回開催。
- 本演習は、**インド太平洋地域の重要インフラ事業者、製造業者等のICSセキュリティの向上を目的**に、**産業用制御システム（ICS）のサイバーセキュリティに焦点**を当て、**ハンズオン演習**や、**日米欧専門家による講演**、**参加者間のネットワーキング**等を実施。
- 2025年は**インド太平洋地域から65名**が**来日して参加**（加えて一部ライブ配信）。これまで以上に**サプライチェーンレジリエンスの強化、日米欧のプレセンスを維持・PR**。

2025年度 演習の概要

- **日時**：2025年11月18日～21日
- **場所**：EU代表部、IPA秋葉原キャンパス等
- **主催**：経済産業省、IPA産業サイバーセキュリティセンター、米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省）及びEU政府（通信ネットワーク・コンテンツ・技術総局、欧州連合サイバーセキュリティ機関、欧州対外行動局）
- **参加者：来日65名＋ライブ配信約100名**　ASEAN加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾の重要インフラ事業者、製造業者、ナショナルCSIRT、政府機関等

ハンズオン演習

日米欧専門家による講演・ワークショップ

インド太平洋地域参加者間のネットワーキング

※写真は2025年度演習の様子

日ASEANサイバーセキュリティ能力構築センター（AJCCBC）との連携

- ASEAN地域でのサイバーセキュリティ能力の向上と各国との連携強化を目指して、2024年11月より、ICSCoE(IPA)は、AJCCBC※と協働し、同地域の政府関係者を対象に、**OTセキュリティを含む重要情報インフラ保護に関する人材育成プログラムを提供。** ※JICA、総務省、タイNCSA等が運営
- ICSCoEがOTセキュリティリスクに関する基調講演、ワークショップ、ハンズオン演習を実施。
- 前頁のインド太平洋地域向け演習との連携を検討中。

2025年度 プログラムの概要

- 日 程：2025年7月21-25日 ※ 7月21-23日 ICSCoEによる基調講演、ワークショップ、ハンズオン演習実施
- 開催地：タイ・バンコク
- 主 催：AJCCBC、 ICSCoE(IPA)、タイNational Cyber Security Agency(NCSA)、JICA
- プログラム提供者：ICSCoE(IPA)、Mahidol University
- 参加者：18名（ブルネイ、カンボジア、インドネシア、ラオス、マレーシア、フィリピン、タイ、ベトナム）

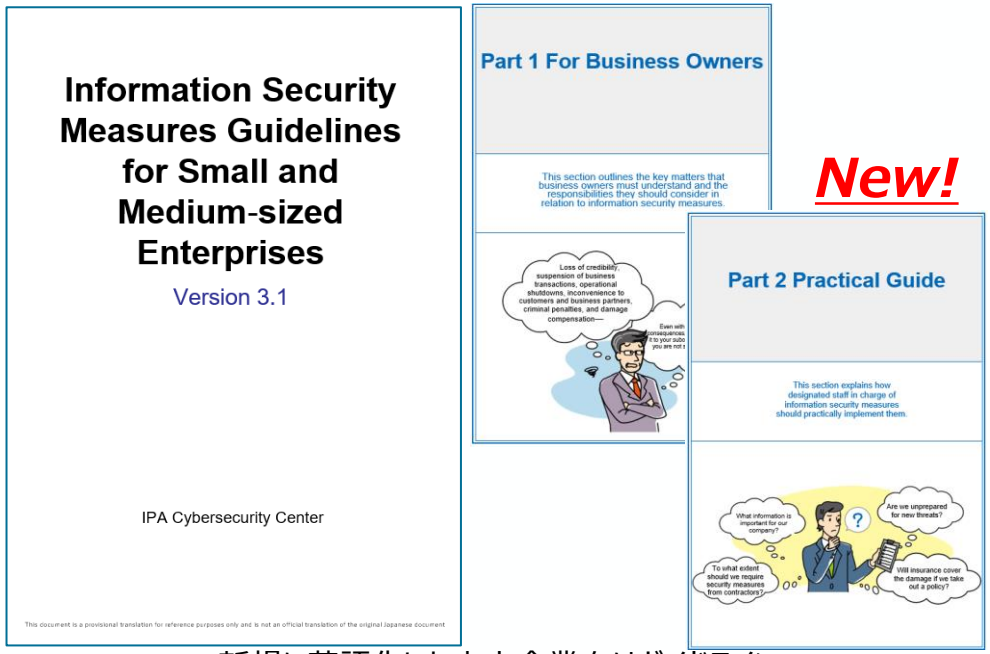
オープニングセレモニーの挨拶の様子


ワークショップの様子


ハンズオン演習の様子

ASEAN向け企業対策支援

- 経済産業省では産業界のサイバーセキュリティ向上に向け、**対象者ごとに具体的な対策を記載したガイドラインを展開している**。他方、一部は**英語版が未発行**であり、発行されている**英語版も国外企業における認知度は低いところ**。
- サイバーセキュリティ対策は、サプライチェーン全体での対策が必要であり、 我が国とサプライチェーンの多くを共有するASEAN地域でのサイバーセキュリティ能力の向上が重要であることから、**ASEAN地域に向けて、施策の情報発信を強化。**
- 具体的には、IPA及びNCOと協力し、**中小企業の情報セキュリティ対策ガイドライン本編の英語版を発行。日本における活用事例の紹介及び産業振興のため、日・ASEANサイバーセキュリティ政策会議にて活用事例を日本企業から発信。**あわせて英語版HPにて情報発信。



新規に英語化した中小企業向けガイドライン

日・ASEANサイバーセキュリティ政策会議の様子

日系サイバー企業のASEAN事業拡大支援

- これまでのASEAN支援で構築した政府間の関係性を活用し、**日系サイバー企業のASEAN事業拡大を支援。**具体的には、JNSAが立ち上げた**民間主導のASEAN向け工場セキュリティ対策のための取組みを政府として後押し**する。
- まずは日系企業が多く進出するタイの日系工場向けにアセスメント及びソリューション提案の体制を、ローカルベンダーを含めて整備。その実績をもとに、ローカル製造業向けに、**現地政府及びローカルベンダーとも連携して国産ツールを含むソリューションの普及に向けた活動（展示会出展等）**を行う。将来的に、タイでの官民連携事業モデルを他のASEAN中位国他に横展開することも視野に進める。

経産省工場ガイドライン活用

- ASEAN各国への経産省工場ガイドライン・チェックリストの普及啓発、現地政府への働きかけ
- 国際標準とも整合性を確保

フレームワーク・ノウハウの提供

JNSA

OT Security WG

- OT含む工場のアセスメントのフレームワーク・ノウハウ提供
- アセスメントで把握されたリスクに対するソリューションも提供（国産ツール・サービスを含む）

現地事業者団体連盟のチャネル活用

ACCOA
ASEAN JAPAN CYBERSECURITY COMMUNITY ALLIANCE (AJCCA)

- JNSAが中心となり立上げた日ASEAN事業者団体連盟のチャネルを活用し、ローカル企業と連携して事業拡大

ASEANの工場セキュリティ・サプライチェーン対策強化に貢献

目次

日本成長戦略会議 デジタル・サイバーセキュリティWG

- 日本成長戦略本部において戦略分野の一つとして指定された「デジタル・サイバーセキュリティ」分野の現状と課題等について議論するための場として、**デジタル・サイバーセキュリティWG**を開催。
- 2026年４月頃に「**官民投資ロードマップ**」（官民投資の促進策）の案を**取りまとめる**予定。

設置趣旨

- リスクや社会課題に対し、先手を打った**官民連携の戦略的投資を促進**し、世界共通の課題解決に資する製品、サービス及びインフラを提供することにより、**更なる我が国経済の成長を実現**する必要。
- 日本成長戦略会議の各WGのうち、**情報化・情報産業に関するWGの1つ**として、「デジタル・サイバーセキュリティWG」を設置。
- 本会議を含む各WGで策定された**官民投資のロードマップを取りまとめ、「日本成長戦略」を策定**する。

スケジュール

2026年

- **２月　デジタル・サイバーセキュリティWGの設置**
  第１回開催
  - 足元のデジタル・サイバーセキュリティ政策の現状の整理
  - 戦略投資の促進に向けた供給力強化/需要創出・拡大に向けた政策の多角的な検討
- **４月　第２回開催**
  - 戦略・ロードマップ案の取りまとめ

検討体制（敬称略）

【WG長】　デジタル大臣、経済産業大臣
【構成員】

井口　譲二	（ニッセイアセットマネジメント株式会社執行役員）
石原　直子	（株式会社エクサウィザーズ はたらくAI＆DX研究所 所長）
岩﨑　尚子	（早稲田大学電子政府・自治体研究所研究院教授）
日下部　進	（GVE株式会社共同創業者兼アドバイザー）
志濟　聡子	（合同会社アイシスコンサルティング代表）
中谷　昇	（日本電気株式会社　執行役　Chief Security Officer）
中室　牧子	（慶応義塾大学総合政策学部教授）
東原　敏昭	（株式会社日立製作所　取締役会長 代表執行役）
村上　明子	（ＳＯＭＰＯホールディングス株式会社執行役員常務グループChief Data Officer、日本経済団体連合会デジタルエコノミー推進委員会　企画部会長）
横山　直人	（株式会社フライウィール共同創業者代表取締役CEO）
和田　隆志	（金沢大学長）

【事務局】　デジタル庁（戦略・組織G）、経済産業省（商務情報政策局）
【関係省庁】
内閣官房（デジタル行財政改革会議事務局、国家サイバー統括室）、総務省、経済産業省（製造産業局）、文部科学省、厚生労働省、警察庁、国土交通省

（参考）デジタル・サイバーセキュリティの全体像

第１回デジタル・サイバーセキュリティWG事務局資料を一部加工