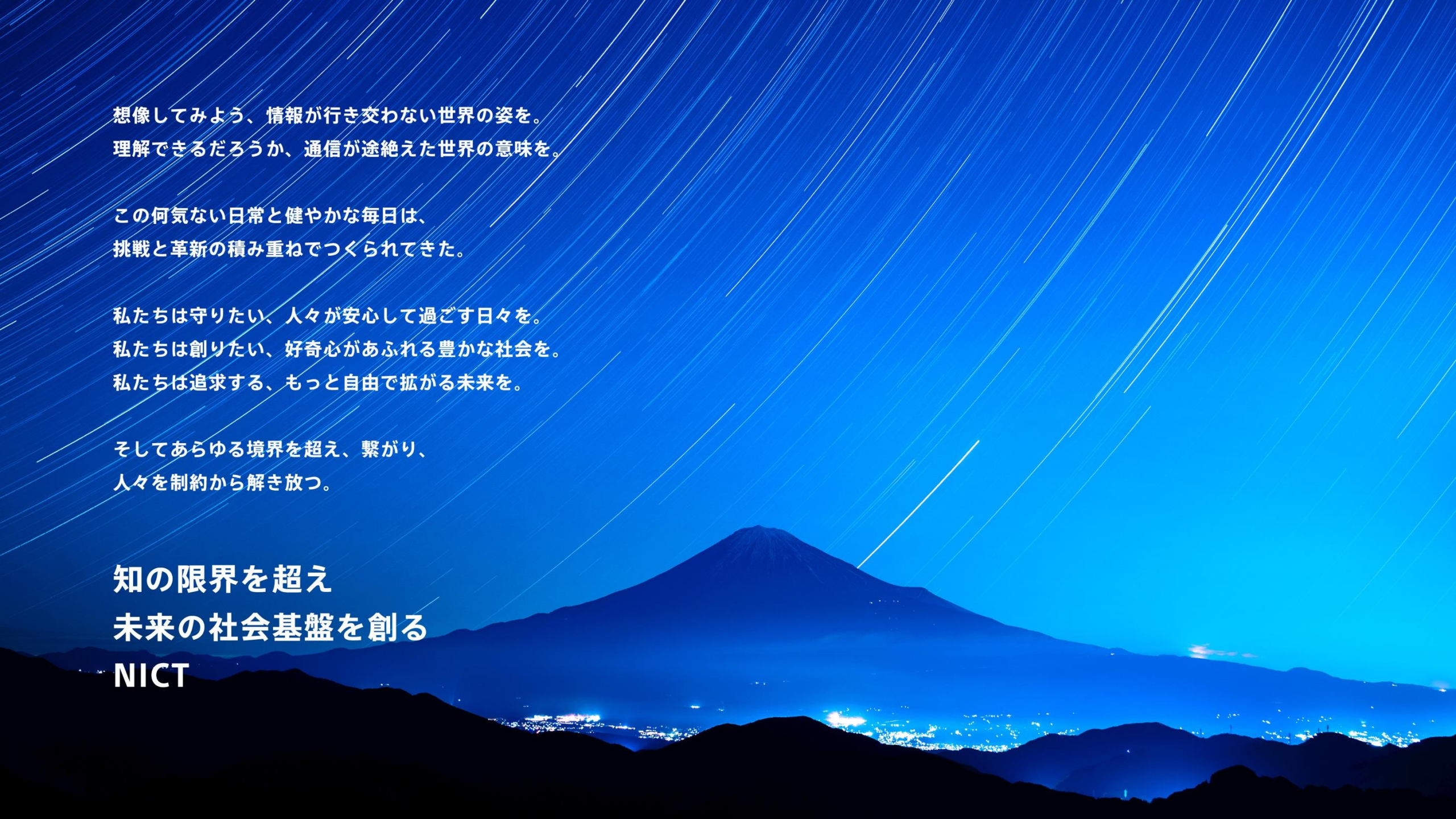
サイバーセキュリティに関する国内外動向の調査報告書

2026年3月31日

国立研究開発法人 情報通信研究機構
イノベーションデザインイニシアティブ
https://www2.nict.go.jp/idi/



想像してみよう、情報が行き交わない世界の姿を。
理解できるだろうか、通信が途絶えた世界の意味を。

この何気ない日常と健やかな毎日は、
挑戦と革新の積み重ねでつくられてきた。

私たちは守りたい、人々が安心して過ごす日々を。
私たちは創りたい、好奇心があふれる豊かな社会を。
私たちは追求する、もっと自由で拡がる未来を。

そしてあらゆる境界を超え、繋がり、
人々を制約から解き放つ。

知の限界を超え
未来の社会基盤を創る
NICT

■ 背景

近年、ICTインフラの普及と高度化が加速している。2020年の新型コロナウイルスの世界的な流行はリモートワークやオンライン授業を普及させ、各種オンラインサービスの利活用を社会に浸透させた。さらに、2022年11月にOpenAI社が公開したChatGPTは世界的な生成AIブームを巻き起こし、今や生成AIは社会基盤の一部となりつつある。

ICTインフラがグローバル社会に広く浸透する中、サイバーセキュリティの脅威はより複雑かつ深刻になっている。生成AIの普及は、AIを活用したサイバー攻撃対策の強化といった正の側面を持つ一方、生成AIモデル自身が攻撃対象となる、あるいは攻撃に悪用されるといった負の側面をもたらしている。また、国際情勢の急速な変化に伴い、政府機関が提供するサービスを機能停止にするといった地政学リスクに起因する攻撃も増加している。

このようなサイバー脅威へ効果的に対処するため、産官学が連携してサイバーセキュリティを強化し、その研究開発成果を広く社会に還元することで、イノベーションを創出することが極めて重要となる。

■ 目的

本調査は、最新のサイバーセキュリティ分野の動向として、AI技術がもたらす技術の進展や課題、2025年5月に成立したサイバー対処能力強化法及び同整備法に関連したアクティブ・サイバー・ディフェンス、そして、従前より重要な課題となっている人材育成等について、今後の日本における研究開発戦略立案に資する課題を抽出し、整理することを目的とする。

■ 調査概要

調査概要は以下のとおりとなる。

調査対象トピック	1～5における国内外の研究開発動向、政策・規制動向、産業動向、国際連携動向に関する調査、および各国・地域の比較等を通じた分析の実施 1. 生成AIによるサイバーセキュリティの攻撃および対策手法の進化 2. 生成AIモデルのセキュリティ確保に関する動向 3. アクティブ・サイバー・ディフェンスに関する動向 4. サイバーセキュリティ人材の育成に関する動向 5. 生成AI時代のサイバーセキュリティについての各国・企業等の動向
調査対象国・地域	主として「日本、米国、欧州、イスラエル、中国、カナダ、インド」 • 欧州は主に「EU、英国」を対象としている • 一部の調査において、その他の国も対象としている
調査方法	ウェブサイト、論文、法令・ガイドライン、調査レポート、ニュース記事等の公開情報
調査対象期間	主として2020年～2026年3月

※ 本報告書は調査時点の公開情報に基づくものであり、内容の完全性・最新性を保証するものではありません
※ 本報告書において出典の記載がない箇所は、複数の関連文献・公開情報を照合した上で、分析・判断した結果として記載しています

目次

略語集

本報告書で使用する主な略語は、以下のとおりとなる。

- AI法《人工知能関連技術の研究開発及び活用の推進に関する法律》
- CISA《Cybersecurity and Infrastructure Security Agency》
- CRA《Cyber Resilience Act》
- ENISA《European Union Agency for Cybersecurity》
- GPAI《Global Partnership on Artificial Intelligence》
- NIS2指令《Network and Information Systems 2 Directive》
- NIST《National Institute of Standards and Technology》
- OWASP《Open Worldwide Application Security Project》

1. 生成AIによるサイバーセキュリティの攻撃および対策手法の進化

調査概要

■ 調査目的

生成AIの急速な普及により、サイバーセキュリティ分野では攻撃・防御の両面で新たな影響が顕在化している。そこで、生成AIによるサイバーセキュリティの攻撃および対策手法の進化を整理し、現状と課題を把握する。

■ 調査内容

#	調査項目	調査内容
①	生成AIによるサイバーセキュリティの攻撃および対策手法の進化に関する研究開発動向	セキュリティおよび人工知能に関する主要な学会*での発表論文の調査を行い、調査項目に関わる論文の投稿数や第一著者の所属機関の国・地域、主要な研究機関の研究内容について分析 * 具体的な学会は参考文献を参照
②	生成AIによるサイバーセキュリティの攻撃および対策手法の進化に関する国際連携動向	①の発表論文における国際共著の割合や傾向を調査
③	生成AIによるサイバーセキュリティの攻撃および対策手法の進化に関する産業動向	AI/GPTモデルを搭載した製品、AIの利用・悪用に関連する団体・規格を調査
④	生成AIによるサイバーセキュリティの攻撃および対策手法の進化に関する政策・規制動向	AIの利用、悪用に関連する各国・地域の政策・規制の概要を調査

■ 調査結果

生成AIの利用、悪用、評価に関連する主要な学会の論文数は2023年以降に大幅な増加が見られる。第一著者の所属機関の国・地域は米国と中国で約8割を占め、国際共著の論文は全論文の約2割となる。

様々な分野で生成AIを活用したセキュリティ製品が登場しつつあるものの、敵対的操作といったリスクも存在し、社会実装はまだ初期段階にある。

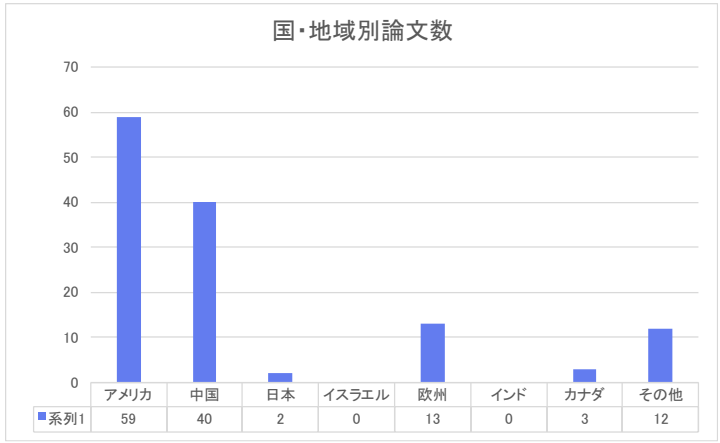
各国・地域では、サイバーセキュリティ分野におけるAIの活用を促進する一方で、その悪用に対する規制や対策の強化が進められている。

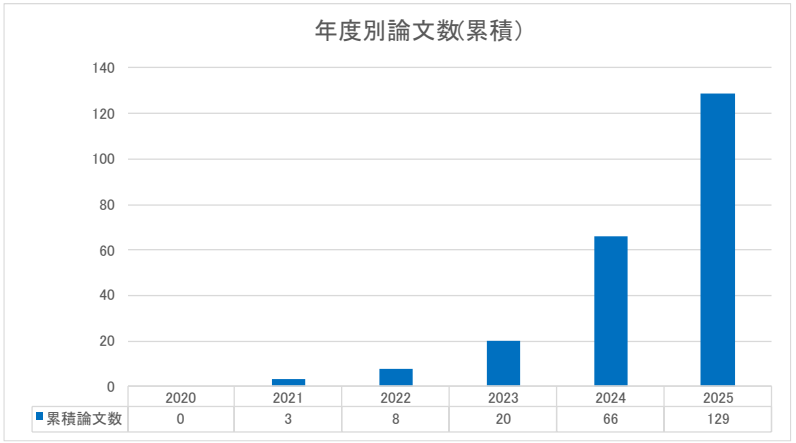
日本においては、2025年12月23日に閣議決定された「サイバーセキュリティ戦略」で、AIの活用と悪用への対策に関する政策の方向性が示されている。しかし、研究開発や製品化の面では他国・地域が先行しているのが現状であり、今後一層の強化が必要となる。

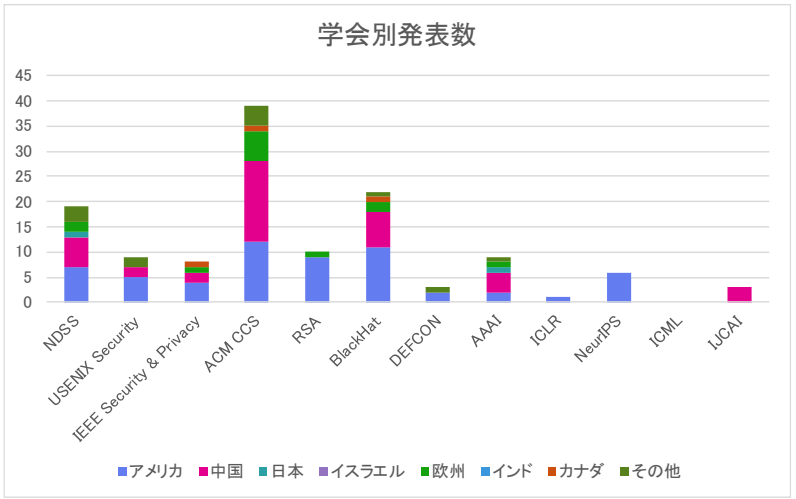
- **投稿数は指数関数的に増加しており、特にサイバーセキュリティを主題とする学会を中心に、米国・中国の企業、大学、研究機関の存在感が大きい。**

分析結果

- 年度別の投稿数
  - ➢ 指数関数的に増大（全129件）
- 国・地域別の投稿数
  - ➢ 米国、中国が非常に多数
- 学会別発表数
  - ➢ サイバーセキュリティを主テーマとする学会での発表が多い







- 各国・地域で主要な研究機関、大学、企業
  - ➢ 米国： Google、The University of Texas、University of California、New York Universityなど
  - ➢ 中国： Zhejiang University、Chinese Academy of Sciences、Wuhan University
  - ➢ 欧州： CISPA（ドイツ）
  - ➢ その他（シンガポール）： Nanyang Technological University、National University of Singapore

※ 論文調査における国名は、著者の所属機関の所在地に基づいて分類しており、著者の国籍は考慮していない。以降のスライドも同様

- **米国が「利用・悪用・評価」を幅広く網羅する一方、中国の研究はソフトウェアの静的解析ツール（SAST）等への「利用」領域に85%が集中するという傾向が見られた。**

・「利用」、「悪用」、「評価」の観点で研究発表を分類し、各国の傾向を分析

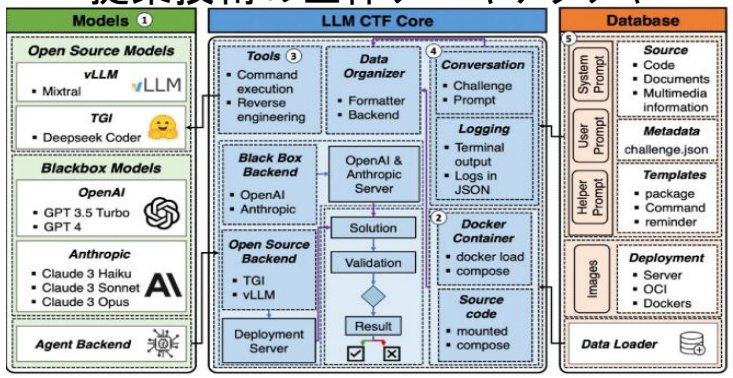
米国の傾向と研究例

傾向：利用が多いが、悪用、評価も一定数発表されている

NYU CTF Bench: A Scalable Open-Source Benchmark Dataset for Evaluating LLMs in Offensive Security [1]

LLMのサイバー攻撃能力を評価するベンチマーク「NYU CTF Bench」と攻撃の自動実行フレームワークを開発し、主要なLLMの性能と限界を実証的に検証

提案技術の全体アーキテクチャ



評価

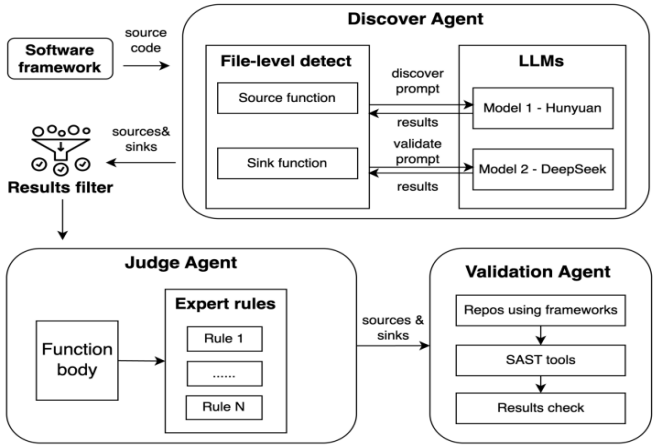
中国の傾向と研究例

傾向：利用に係る研究が大半を占める（85%）

More Flows, More Bugs: Empowering SAST with LLMs and Customized DFA [2]

静的解析ツール（SAST）にLLMを統合して、大規模なコードベースからより多くの脆弱性を発見する方法を提案

提案技術のワークフロー



利用

・「利用」（誤検知、コード修正など）、「悪用」（フィッシング、サイバー攻撃自動化など）、「評価」（リスク分析、性能評価など）

[1]: https://neurips.cc/virtual/2024/poster/97547
[2]: https://blackhat.com/us-25/briefings/schedule/#more-flows-more-bugs-empowering-sast-with-llms-and-customized-dfa-45259

1. 生成AIによるサイバーセキュリティの攻撃および対策手法の進化
② 生成AIによるサイバーセキュリティの攻撃および対策手法の進化に関する国際連携動向

- **研究開発で調査した129本の論文を対象に、著者の所属機関が所在する国を分析した。その結果、全体の約20%が2か国以上の研究者による国際共著論文であり、特に米国が多くの国と共同研究を行っていることが明らかとなった。**
- **複数の国の機関から資金提供・支援等を受けている事例も見られ、単一の資金源に依存するリスクの分散や、より大規模な研究の実現を可能にするといった利点をもたらすと考えられる。**

■調査論文における共著の国・地域の組合せ

分類	論文数	共著の国の組合せ
2か国の共著	19/129件 14.7%	• 米国 – 中国 (4件) • 米国 – カナダ (3件) • 米国 – ドイツ • 米国 – シンガポール • 米国 – オーストラリア • 米国 – カタール • 米国 – 英国 • 米国 – 韓国 • 中国 – ウクライナ • 中国 – シンガポール • ドイツ – オランダ • ドイツ – シンガポール • スコットランド – ルクセンブルク
3か国以上の共著	5/129件 3.8%	• 中国 – 米国 – 日本 • ドイツ – オランダ – 米国 • オーストラリア – オランダ – 中国 • ドイツ – オランダ – 英国 – 米国 • シンガポール – 中国 – ドイツ – オーストラリア

■国際共著における研究資金提供・支援の事例

＜Using AI Assistants in Software Development: A Qualitative Study on Security Practices and Concerns [1]＞

- 著者の国・地域: ドイツ、オランダ、英国、米国
- 資金提供・支援等:
  - EU: European Union Horizon Europe program Cybersecurity Sec4AI4Sec Award (#101120393)
  - ドイツ: VolkswagenStiftung Niedersächsisches Vorab (ZN3695)
  - ドイツ: ドイツ研究振興協会 (DFG/German Research Foundation) Excellence Strategy (EXC 2092 CaSa – 390781972)
  - オランダ: オランダ科学研究機構 (NOW/Dutch Research Council) Kennis– en Innovatieconvenant (KIC) HEWSTI Award (KICH1.VE01.20.004)
  - 英国: 工学・物理科学研究会議 (EPSRC/Engineering and Physical Sciences Research Council) REPHRAIN: National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (EPSRC Grant EP/V011189/1) Equitable Privacy (EPSRC Grant EP/W025361/1)
  - 米国: 米国国立科学財団 (NSF/National Science Foundation) Standard Grant (CNS-2247141、CCF-2312321)

＜A Decade-long Landscape of Advanced Persistent Threats:Longitudinal Analysis and Global Trends [2]＞

- 著者の国・地域: 韓国、米国
- 資金提供・支援等:
  - 韓国: 科学技術情報通信部 (MSIT/Ministry of Science and ICT) が資金提供する情報通信企画評価院 (IITP/Institute for Information and Communications Technology Planning and Evaluation) 助成金 (No. RS-2022-II221199、No. RS-2024-00437306、No. RS-2024-00337414、No. RS-2025-25457342、No. RS-2025-25394739)
  - 米国: 米国国立科学財団 (NSF/National Science Foundation) Standard Grant (CNS-2126654、DGE-2335798) 、Continuing Grant (CNS-2440819)

[1]: https://dl.acm.org/doi/10.1145/3658644.3690283
[2]: https://dl.acm.org/doi/abs/10.1145/3719027.3765085

③ 生成AIによるサイバーセキュリティの攻撃および対策手法の進化に関する産業動向｜製品・サービス

- **生成AIを活用したセキュリティ製品・サービスは様々な分野で登場し始めており、初期の導入段階となり、計算能力の確保や敵対的操作などのリスク等の課題がある。**

＜GPTベースのツール事例 [1] ＞

製品・サービス分野	AI/GPT Models	機能	効果
フィッシング検出	• Microsoft Copilot for Security • Phish.AI	• メールの内容と送信者の行動を分析 • 異常や言語的な手がかりを検出 • 潜在的なフィッシングの脅威へのフラグ付加	• 企業におけるフィッシング攻撃を45%削減 • 95%以上の高い検知精度を達成
脅威インテリジェンス	• IBM Watson • Darktrace	• 非構造化セキュリティデータを処理 • 攻撃パターンを特定 • 実用的な洞察を提供	• 調査時間を40%短縮 • 高度な持続的標的型攻撃（Advanced Persistent Threat）を検知 • 内部脅威への対応時間を30%削減
マルウェア検出	• GPT-4 (VirusTotal) • Cylance AI	• マルウェアの分類を強化 • ゼロデイマルウェアやファイルレスの脅威を検出 • マルウェアを予測してブロック	• 検知率を38%向上 • マルウェア分析時間を50%短縮 • ランサムウェア感染を70%の精度で検知
コンプライアンス監査	• Google Chronicle • IBM Qradar	• ポリシーの施行を自動化 • コンプライアンス違反のアクティビティを検出 • 監査時間を短縮	• 監査時間を60%削減 • コンプライアンス順守を35%向上
インシデントレスポンス	• GPT-4-based Chatbots • CrowdStrike Falcon	• アラート分析を自動化 • 修正に関するアドバイスを提供 • チームのコラボレーションを向上	• 対応時間を40%短縮 • アナリストの効率と脅威緩和能力を向上
パスワードセキュリティ	• PassGAN • Okta AI	• 脆弱なパスワードを検出 • 適応型認証（Adaptive Authentication）の実装 • 認証情報に基づく攻撃を防止	• 脆弱性を事前に特定 • ユーザーに影響を与えることなく認証セキュリティを強化
侵入検知	• Vectra AI	• ファイルレスマルウェアのような新たな脅威を検出 • ユーザーの行動を分析 • 脅威の優先順位付けを自動化	• 検知時間を65%削減 • 誤検知を減らすことで精度を向上

[1]: Contrast of GPT-based tools in cybersecurity across different case study Abdelzahir Abdelmaboud, Sayeed Salih, Aisha H. A. Hashim, Refan Mohamed Almohamedh, Hayfaa Tajelsier, Abdelwahed Motwakel CC BY-SA 4.0 を改変して作成

③ 生成AIによるサイバーセキュリティの攻撃および対策手法の進化に関する産業動向｜団体・規格

- **2020年以降、国際的な団体における新たなプロジェクト活動や規格の策定が進み、協調的な取組が活発化している。こうした動きの一例として、2020年にはPartnership on AI (PAI) がAIインシデントのデータベース「The AI Incident Database (AIID) 」を公開し、世界各国における2000件以上のインシデント事例が蓄積されている。**

分類		組織	設立	概要
団体	Forum of Incident Response and Security Teams (FIRST)	FIRST Members (113か国、830組織以上)	1995	• インシデント対応、およびセキュリティチームの国際的な団体 • 2023年にAI Security SIGが発足し、AIを活用したセキュリティ対策やAIを悪用した攻撃と対策の共有等が行われている
	Partnership on AI (PAI)	学術団体、企業等のパートナー (17か国、140組織以上)	2016	• AIが人々や社会にとってよい成果をもたらす解決策を創出する非営利団体 • Safety Critical AIプログラムの活動にて、2021年にAIインシデントのデータベースであるThe AI Incident Database (AIID) を作成。2000件以上のインシデント事例が登録されている
	Cyber Threat Alliance (CTA)	セキュリティ企業がメンバー	2014	• サイバー攻撃の脅威情報を共有し、製品・サービスを改善、セキュリティ向上を目指す組織 • 2025年に報告書「生成AI時代のセキュリティ (Cybersecurity in the Age of Generative AI)」を発表した ➢ Part I, Combating GenAI Assisted Cyber Threats ➢ Part II, Navigating Cyber Threats to GenAI Systems
団体・規格	Coalition for Content Provenance and Authenticity (C2PA)	Steering Committeeメンバー (10社)	2021	• デジタルコンテンツの出所や来歴を認証するための技術標準の団体・規格 • C2PAは、デジタルコンテンツの出所や来歴を追跡することができるため、ディープフェイクの対策となる • 最新バージョン: C2PA Specifications 2.3 (2026年3月時点)
	Really Simple Licensing (RSL)	RSL Collective	2025	• Webパブリッシャーが生成AI利用のために学習データを収集するWebクローラーの条件を設定できる規格 • 従来のrobots.txtでは、クロール許可/拒否の条件指定だったが、RSL 1.0では、“ai-all”、“ai-input”、“ai-index”等のAIクローラーに対する詳細な条件指定が可能となり、Webサイトが無断クロールされ、学習データに利用されるリスクが低減される • 最新バージョン: RSL 1.0 (2026年3月時点)

④ 生成AIによるサイバーセキュリティの攻撃および対策手法の進化に関する政策・規制動向｜AIの活用

- **AIを活用したサイバーセキュリティ対策について各国・地域の動向を調査した結果、すべての対象国・地域が戦略や法令等において対策強化にAIを活用する方針を示しており、国家施策としてのAI活用の重要性が浮き彫りとなった。**

国・地域	政策・規制の動向	関連する政策・規制（一部）
日本	AIを活用したサイバー攻撃を受けたインフラの検知や関連情報の分析の緻密化・迅速化等を、関係主体と連携して推進する	サイバーセキュリティ戦略（2025年12月23日閣議決定）（2025）
カナダ	AIや自動化のようなテクノロジーを活用し、脅威への対処を強化する	国家サイバーセキュリティ戦略（Canada‘s National Cyber Security Strategy）（2025）
米国	重要インフラのサイバーセキュリティ強化として、AI-enabledなサイバー防御ツールを継続的に採用する。AIの活用によって生じる脅威に備え、セキュア・バイ・デザインなシステムを使用する必要性がある	America‘s AI Action Plan（2025）
欧州（EU）	EU内のサイバー対処能力の強化を目指し、European Cybersecurity Alert Systemで高品質な脅威インテリジェンス情報を作成するため、AIやデータ分析などの高度な技術の活用を強化する	• EUサイバーセキュリティ戦略（EU Cybersecurity Strategy）（2020） • サイバー連帯法（EU Cyber Solidarity Act）（2025）
欧州（英国）	AIはサイバー力にとって不可欠な技術のひとつと位置付けられている。ネットワーク監視等の多様なアプリケーションにおいてサイバーセキュリティを強化するためのAIの活用の可能性を言及している	国家サイバー戦略 2022（National Cyber Strategy 2022）（2022）
イスラエル	生成AIの活用は脆弱性検出の迅速化などのサイバーセキュリティの大幅な強化につながる可能性があることを踏まえ、AIベースのサイバーセキュリティメカニズムを開発し、攻撃者やサイバー攻撃を監視、検知、特定する能力、攻撃パターンを分析する能力、サイバーセキュリティの取組を支援する予測能力を向上させる	国家サイバー・セキュリティ戦略 2025（National Cyber Security Strategy 2025）（2025）
中国	AI等の新たな技術を活用し、サイバーセキュリティ保護水準の向上を目指す	中華人民共和国サイバーセキュリティ法（中华人民共和国网络安全法）（2025 改正）
インド	AIを悪用した偽情報に対抗するためのAI-drivenな脅威検出ツール（例: 異常検出、ディープフェイク検出）の開発が必要である	• IndiaAIミッション（IndiaAI Mission）（2024） • AIガバナンス・ガイドライン（India AI Governance Guidelines）（2025）

④ 生成AIによるサイバーセキュリティの攻撃および対策手法の進化に関する政策・規制動向｜AIの悪用

- **AIを悪用したサイバー攻撃への対策における各国・地域の動向を調査し、全ての対象国・地域が戦略や法令等にてAIによるサイバー攻撃の高度化・巧妙化等を踏まえ、脅威の監視・分析等の強化や法規制の整備等で対策を強化する方向性を確認した。**

国・地域	政策・規制の動向	関連する政策・規制（一部）
日本	研究開発等により、AIによって一層脅威が高まると予想されるサイバー攻撃の被害の防止に向けた取組を推進する	サイバーセキュリティ戦略（2025年12月23日閣議決定）（2025）
カナダ	AIやLLMがもたらす脅威や、誤情報、偽情報、悪意ある情報の識別方法といったトピックについて情報を公開し、国民のサイバーセキュリティ意識向上を図る	国家サイバーセキュリティ戦略（Canada ‘s National Cyber Security Strategy）（2025）
米国	重要インフラのサイバーセキュリティ強化として、AIに関連するサイバー脅威を監視するためAI Information Sharing and Analysis Center（AI-ISAC）を設立する	America ‘s AI Action Plan（2025）
欧州（EU）	ENISA（欧州連合サイバーセキュリティ機関/European Union Agency for Cybersecurity）におけるサイバーセキュリティ脅威管理を支援する役割を強化する方針である	Proposal for a Regulation for the EU Cybersecurity Act（2026） 参考: ENISAのAIに関連するレポート • Artificial Intelligence Cybersecurity Challenges（2020） • Artificial Intelligence and Cybersecurity Research（2023） • ENISA Threat Landscape 2025（2025）
欧州（英国）	AIが国家安全保障と犯罪にもたらすリスクに対する防御を強化する	Cyber Growth Action Plan 2025（2025） Laboratory for AI Security Research（LASR）（2024） AI Security Institute（AISI）（2025）
イスラエル	AIを安全に導入するため、敵対的AIからの保護対策の研究開発を推進する	国家サイバー・セキュリティ戦略 2025（National Cyber Security Strategy 2025）（2025）
中国	公共の利益を保護することを目的に、AIが生成するコンテンツのラベル付けを義務化する	人工知能生成合成コンテンツ識別弁法（人工智能生成合成内容标识办法）（2025）
インド	個人や組織への被害報告を収集し、リスクを追跡・分析するためのフィードバックループとして、AIインシデントメカニズムの確立を目指す	• IndiaAIミッション（IndiaAI Mission）（2024） • AIガバナンス・ガイドライン（India AI Governance Guidelines）（2025）

2. 生成AIモデルのセキュリティ確保に関する動向

調査概要

■ 調査目的

生成AIの急速な普及により、生成AIモデルを組み込んだAIシステムの利用が拡大しており、生成AIモデルのセキュリティ確保は喫緊の課題となっている。そこで、生成AIモデルのセキュリティ確保について整理し、現状と課題を把握する。

■ 調査内容

生成AIモデル、および生成AIモデルを組み込んだシステムを調査対象スコープとする。

#	調査項目	調査内容
①	生成AIモデルのセキュリティ確保に関する研究開発動向	セキュリティおよび人工知能に関する主要な学会*での発表論文の調査を行い、調査項目に関わる論文の投稿数や第一著者の所属機関の国・地域、主要な研究機関の研究内容について分析 * 具体的な学会は参考文献を参照
②	生成AIモデルのセキュリティ確保に関する産業動向	生成AIが組み込まれたシステムのセキュリティ確保の管理・運用のプロセス、対策製品・サービスの国・地域別の傾向、対策の動向を調査
③	生成AIモデルのセキュリティ確保に関する政策・規制動向	生成AI含むAI、AIシステムのセキュリティ確保に関する政策・規制を調査
④	生成AIモデルのセキュリティ確保に関する国際連携動向	AIのセキュリティ確保に関連する政府機関の国際連携を調査

■ 調査結果

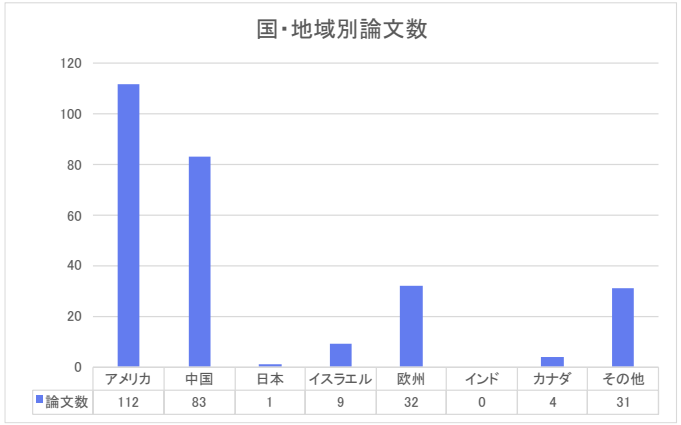
主要な学会における論文の傾向は、2023年以降に発表数が大幅に増加し、第一著者の所属機関が米国と中国であるものが約7割を占めるなど、第1章で述べた動向と一致する。産業動向においては、米国やイスラエルを中心にLLMガードレール等の新たな製品・サービスが登場している。政策・規制では、各国・地域でルール整備が急速に進んでおり、特に英国は国際標準化を主導する動きを見せている。さらに、GPAIや各国・地域のAISI等を通じた国際連携も活発化しており、AIのセキュリティ確保に向けた共通枠組みの形成が進展している。

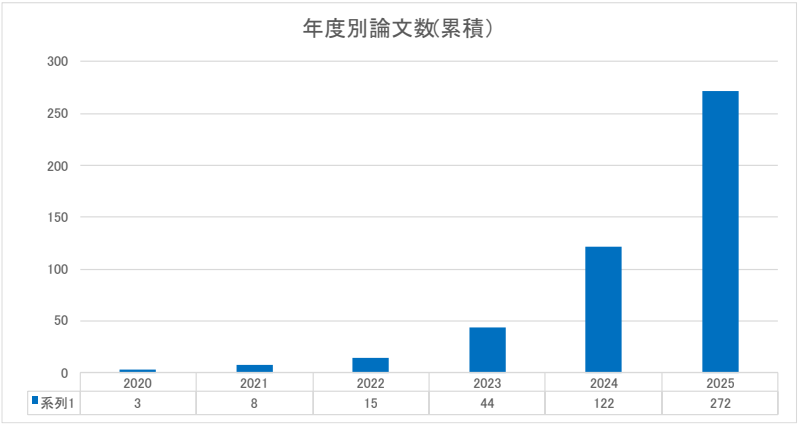
日本においては、2025年9月にAI法が全面施行され、2025年12月23日に人工知能基本計画が閣議決定され、ルール整備が急速に進められており、また、GPAI等を通じた国際的な枠組み作りにも積極的に参加している。しかし、研究開発や製品化の面では、他国・地域が依然として先行しているのが現状であり、今後、国際競争力を一層強化していくことが不可欠である。

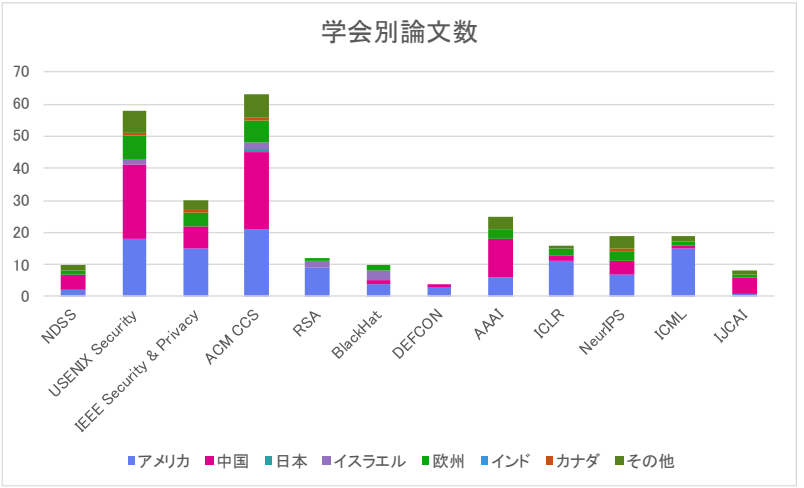
- **“生成AIによるサイバーセキュリティの攻撃および対策手法の進化”と同様に、投稿数は指数関数的に増加しており、特にサイバーセキュリティを主題とする学会を中心に、米国・中国の企業、大学、研究機関の存在感が大きい。**

分析結果

- 年度別の投稿数
  - ➢ 指数関数的に増大（全272件）
- 国・地域別の投稿数
  - ➢ 米国、中国が非常に多数
- 学会別発表数
  - ➢ サイバーセキュリティを主テーマとする学会での発表が多い







- 各国・地域で主要な研究機関、大学、企業
  - ➢ 米国：University of Chicago、Microsoft、Northeastern University、UC Berkeley、Princeton Universityなど
  - ➢ 中国：Zhejiang University、University of Chinese Academy of Sciences、The Hong Kong University of Science and Technology（香港）
  - ➢ 欧州：CISPA Helmholtz Center for Information Security（ドイツ）
  - ➢ その他（シンガポール）：Nanyang Technological University、National University of Singapore

- 米国が「防御」、「攻撃」、「評価」と幅広く研究発表を行っている一方、中国は「防御」、「攻撃」を中心に研究発表が行われている。

・「防御」、「攻撃」、「評価」の観点で研究発表を分類し、各国の傾向を分析

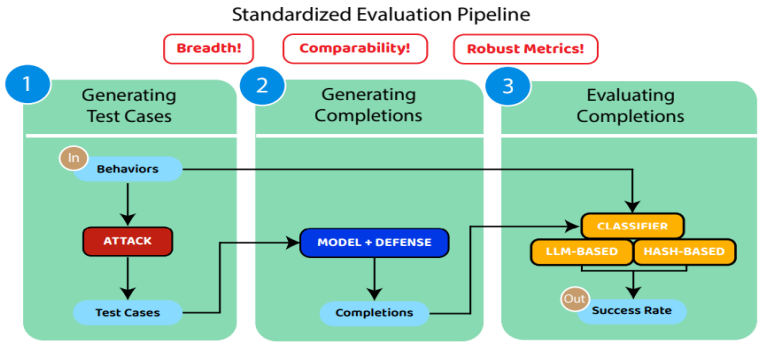
米国の傾向と研究例

傾向：未知の脆弱性の探索/防御、基礎理論の構築や評価基準(ベンチマーク)の作成を推進

HarmBench: A Standardized Evaluation Framework for Automated Red Teaming and Robust Refusal [1]

大規模言語モデル(LLM)に対する自動レッドチーミング(攻撃テスト)と防御策を比較・評価するための標準フレームワーク「HarmBench」を提案し、大規模な実証実験を実施

評価の流れ



評価

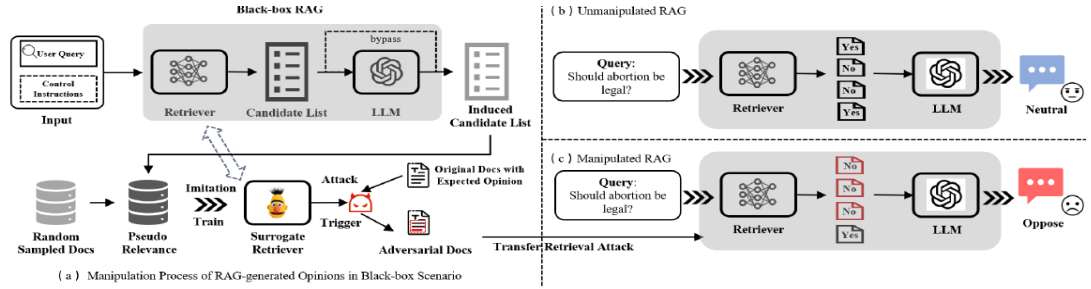
中国の傾向と研究例

傾向：防御、攻撃に分類される研究が多い。

FlippedRAG: Black-Box Opinion Manipulation Adversarial Attacks to Retrieval-Augmented Generation Models [2]

ブラックボックス状態のRAGシステムに対して、数個の文章を改ざんするだけで、検索と生成の双方を操作し、攻撃成功率と意見偏向を大幅に高める攻撃手法(FlippedRAG)を発表

FlippedRAGの概要



攻撃

・「防御」(トレーサビリティ確保、プライバシー保護など)、「攻撃」(プロンプトインジェクション、ジェイルブレイクなど)、「評価」(安全性やベンチマークなど)

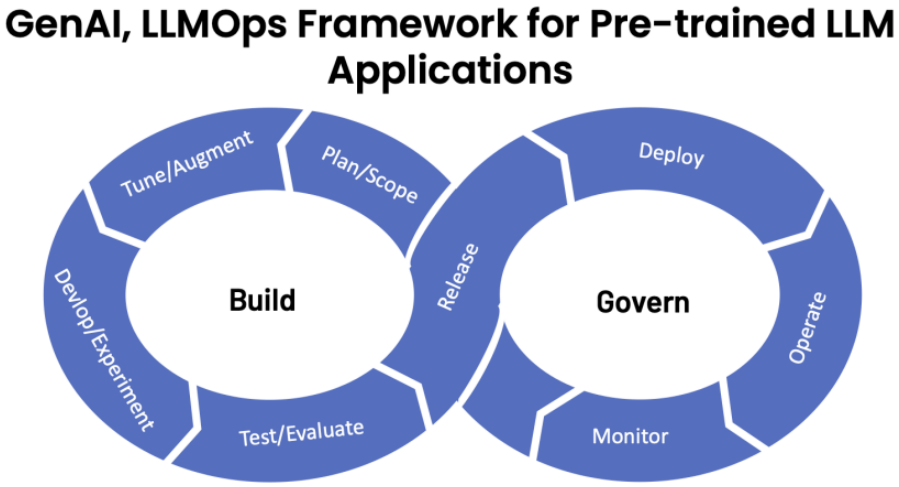
[1]: https://openreview.net/forum?id=f3TUipYU3U&referrer=%5Bthe%20profile%20of%20Bo%20Li%5D(%2Fprofile%3Fid%3D~Bo_Li19)
[2]: https://dl.acm.org/doi/10.1145/3719027.3765023

② 生成AIモデルのセキュリティ確保に関する産業動向｜製品・サービス

- OWASPでは、GenAI、LLMOpsアプリケーションのライフサイクルのフレームワークを公開している。
- OWASPが公開しているLLMおよび生成AIのセキュリティ製品・サービス196製品について、開発企業の国・地域を調査した結果、米国およびイスラエルが中心となって製品・サービスを提供していることが確認された。

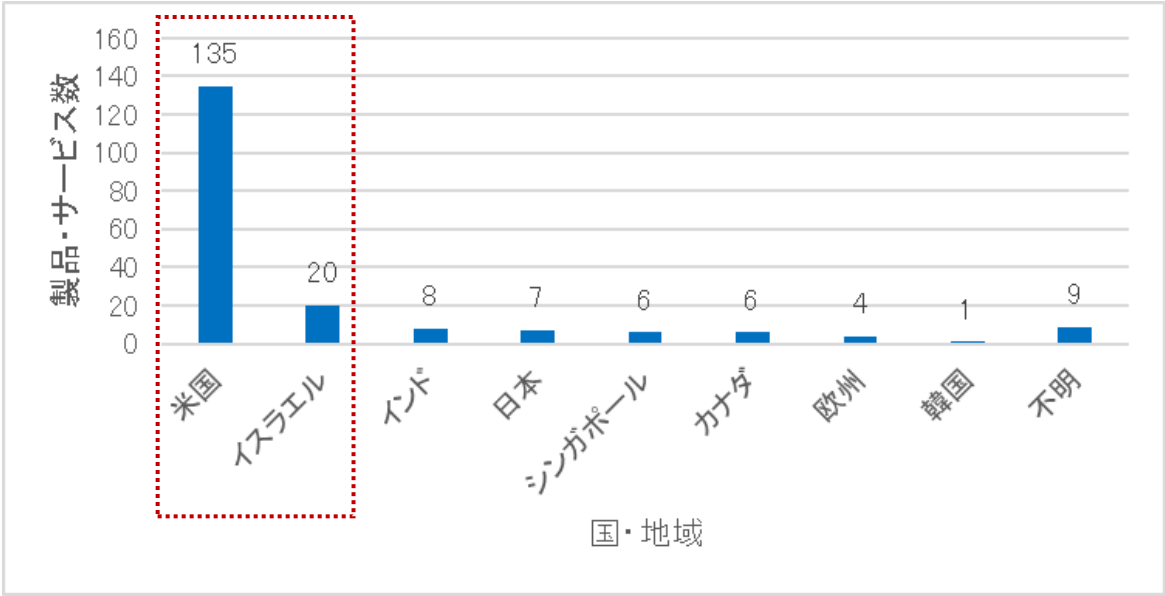
GenAI, LLMOps Framework[1]

OWASPでは、GenAI、LLMOpsアプリケーションのライフサイクルの各段階におけるステージ、開発タスク、セキュリティ手順を定義したフレームワークを公開している。
ステージは、「Plan/Scope」「Tune/Augment」「Develop/Experiment」「Test/Evaluate」「Release」「Deploy」「Operate」「Monitor」「Govern」となる。



全ステージの国・地域別*1の製品・サービス数*2

米国、イスラエルで全体の約8割を占める。



*1 本社機能がある国・地域を開発企業の国・地域とする
*2 1つの製品・サービスが複数ステージをカバーしている場合は、1ステージごとに1製品としてカウント

[1]: OWASP GenAI Security Project – Solutions Reference Guide Q2 Q3' 25 – OWASP Top 10 for LLMs – LLMSecOps Solutions Landscape (CC BY-SA 4.0) より文章、画像引用
OWASP GenAI Security Project – Solutions Reference Guide Q2 Q3' 25 – OWASP Top 10 for LLMs – CyberSecurity Solution and LLMSecOps Landscape Guide (CC BY-SA 4.0) より文章画像引用

② 生成AIモデルのセキュリティ確保に関する産業動向｜製品・サービス

- **LLMや生成AIのアプリケーションは発展途上であり、従来のセキュリティ対策やDevSecOpsのアプローチでは対応できない課題が浮上しており、LLMガードレールをはじめとするLLMや生成AIに特化した製品・サービスが開発・提供され始めている。**

＜LLMや生成AIに対する対策の一例＞

LLMガードレール[1]	• LLMが有害、偏見のある、または不適切なコンテンツを生成することを防ぐための保護メカニズムを提供するものであり、インタラクション中にルール、制約、コンテキストガイドラインを適用することで、定義された倫理的、法的、および機能的な境界内で動作するように設計されている。 • コンテンツフィルタリング、倫理ガイドライン、敵対的入力検出、ユーザーインテント検証を含んでおり、LLMの出力が意図したユースケースと組織のポリシーと一致していることを確認する。
LLM Firewall[1]	• LLMを不正アクセス、悪意のある入力、および潜在的に有害な出力から保護するためのセキュリティレイヤーである。 • LLMとの相互作用を監視およびフィルタリングし、モデルの動作を操作する可能性のある疑わしい入力や敵対的な入力をブロックし、また、事前定義されたルールとポリシーを適用し、LLMが定義された倫理的および機能的な境界内でのみ正当な要求に応答することを保証する。さらに、モデルに出入りするデータの流れを制御することで、データの流出を防ぎ、機密情報を保護する。
Red Teaming[2]	• 攻撃者がどのようにAIシステムを攻撃するかの観点で、AIセーフティへの対応体制および対策の有効性を確認する評価手法である。 • 攻撃者の目線で対象AIシステムにおける弱点や対策の不備（脆弱性）を発見し、それらを修正および堅牢化することで、AIセーフティを維持または向上させる。

[1] 引用: OWASP GenAI Security Project – Solutions Reference Guide Q2 Q3’25 – OWASP Top 10 for LLMs – LLMSecOps Solutions Landscape (CC BY-SA 4.0) より引用
OWASP GenAI Security Project – Solutions Reference Guide Q2 Q3’25 – OWASP Top 10 for LLMs – CyberSecurity Solution and LLMSecOps Landscape Guide (CC BY-SA 4.0) より引用
[2] 引用: AIセーフティに関するレッドチーミング手法ガイド（第1.10版）, https://aisi.go.jp/assets/pdf/J1_ai_safety_RT_v1.10_ja.pdf

② 生成AIモデルのセキュリティ確保に関する産業動向｜団体・規格

- **2020年以降、国際的な団体における新たなプロジェクト活動や規格の策定が進み、協調的な取組が活発化している。こうした動きの一例として、2021年にAIシステムに対する攻撃者の戦術や技術のナレッジベースMITRE ATLASが公開され、AIシステム固有の攻撃手法が体系的に整理されている。**

名称		組織	設立	概要
団体	MITRE	非営利組織	1958	• MITRE ATT&CKをベースとしたAIシステムに対する攻撃者の戦術や技術のナレッジベースMITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) を2021年に公開 • 最新バージョン: Data v5.4.0 (16戦術、97テクニックを公開)
	TrustLLM	TrustLLM Team	2024	• LLMにおける信頼性に関する包括的な研究チーム • 真実性、安全性、公平性、堅牢性、プライバシー、機械倫理の6つの側面でLLMの信頼性を評価する。多数のベンチマーク用のデータセットやLLMの評価結果が公開されている
	Partnership on AI (PAI)	学術団体、企業等のパートナー (17か国、140組織以上)	2016	• AIが人々や社会にとってよい成果をもたらす解決策を創出する非営利団体 • Safety Critical AIプログラムの活動にて、2023年にAIモデルやリリースの種類に応じた推奨ガイダンスSafe Foundation Model Deploymentを公開
	Coalition for Secure AI (CoSAI)	非営利組織 (セキュリティ企業がメンバー)	2024	• イノベーションと標準化を通じて、AIの開発、デプロイの信頼性とセキュリティを強化する組織 • AIシステムのためのソフトウェアサプライチェーンセキュリティ等、4つのワークを実施
	Agentic AI Foundation (AAIF)	Linux Foundation	2024	• エージェント型AIが透明かつ協働的に進化することを確実にするための中立的で開かれた基盤を提供 • 3プロジェクトを推進 (MCP、goose、AGENTS.md)
企業	Meta	–	2004	• 2023年に生成AIの信頼と安全性のツールや評価を提供するオープンエコシステムPurple Llamaプロジェクトを立ち上げ • LLMベースのセーフガードモデルであるLlama Guardや、LLMに対するサイバーセキュリティ評価ツールであるCyberSec Eval等を公開している
団体・規格	Model Context Protocol (MCP)	Agentic AI Foundation (Linux Foundation傘下)	2024	• AIと他のシステムを接続するための技術標準で、Base ProtocolのSecurity Best Practicesにて、攻撃に対する緩和策の実装が記載されている • 最新バージョン: Version 2025-11-25 (2026年3月時点)

③ 生成AIモデルのセキュリティ確保に関する政策・規制動向

- **生成AIを含むAIシステムのセキュリティ確保に関するルール整備が各国・地域で急速に進められている。**
- **英国は、自国で策定した行動規範を国際標準の基礎とすることで、ルール形成における主導権を確保する動きが見られる。**

国・地域	政策・規制の動向	関連する政策・規制（一部）
日本	「AI事業者ガイドライン」等の自主規制が中心だったが、2025年に「AI法」が施行された。AI法に基づいて「人工知能基本計画」が閣議決定され、AIの適正性を確保するガバナンスの構築や、国際的なガバナンス構築を主導する	• AI事業者ガイドライン（2024） • 人工知能関連技術の研究開発及び活用の推進に関する法律（AI法）（2025） • 人工知能基本計画（2025年12月23日閣議決定）（2025）
カナダ	包括的な規制である「AIとデータ法」の草案が2025年に廃案となり、リスクに対し適用すべき措置を特定した「高度な生成AIシステムの責任ある開発と管理に関する自主行動規範」等の自主規範で運用している	• 高度な生成AIシステムの責任ある開発と管理に関する自主行動規範（Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems）（2023） • 【廃案】AI・データ法（AIDA/Artificial Intelligence Data Act）（2025）
米国	米国全体で包括的な規制はないが、2025年にカリフォルニア州でフロンティアAIフレームワークの公表等を規定した「フロンティア人工知能透明性法」が成立する等、州法単位では規制の動きが見られる	フロンティア人工知能透明性法（Transparency in Frontier Artificial Intelligence Act）（2025）
欧州（EU）	生成AIを含む包括的な規制である「AI規制法」が2024年に施行。リスクに応じた規制が適用され、システミックリスクを伴う汎用目的AIモデルに関しては、適切なレベルのサイバーセキュリティ保護が義務付けされている	AI規制法（EU Artificial Intelligence Act）（2024）
欧州（英国）	2025年に提出した「人工知能（規制）法案」が審議の最中、AIシステム、およびそれを開発・導入する組織の安全を確保するための原則を定めた「AIサイバーセキュリティ行動規範」が公表され、本規範は、国際標準 ETSI TS 104 223の基礎として使用されている	• 人工知能（規制）法案（Artificial Intelligence (Regulation) Bill [HL]）（2025） • AIサイバーセキュリティ行動規範（Code of Practice for the Cyber Security of AI）（2025） • ETSI TS 104 223「Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems」（2025）
イスラエル	包括的な規制はないが、「人工知能規制と倫理に関する政策」において、AIシステムのライフサイクル全体にわたり、サイバー関連のリスクを低減するために適切な措置を講じるべきであると述べている	イスラエルの人工知能規制と倫理に関する政策（Israel's Policy on Artificial Intelligence Regulation and Ethics）（2023）
中国	AIに関し細かな規制が策定されており、2023年に生成AIに特化した「生成人工知能サービス管理暫行弁法」が施行され、セキュリティ評価の届出等が義務付けされている	生成人工知能サービス管理暫行弁法（生成式人工智能服务管理暫行办法）（2023）
インド	包括的な規制はないが、2025年に包括的な規制となる倫理と説明責任の枠組みを確立ための「人工知能（倫理と説明責任）法案 2025」が公表された	人工知能（倫理と説明責任）法案 2025（The Artificial Intelligence (Ethics and Accountability) Bill, 2025）（2025）

④ 生成AIモデルのセキュリティ確保に関する国際連携動向

- 2020年に「責任あるAI」の開発・利用の実現を目的とする国際的なイニシアティブGPAI*1が発足し、2024～2025年にかけて生成AIの商用化時の安全性を保証する実践的なアプローチの展開を支援するSAFE*2プロジェクトが実施され、成果のひとつとしてSAFEマッピングデータベースを公開した。
- 2023年以降、各国・地域でAIの安全性に関する機関の設立が進み、2024年にAISI国際ネットワーク*3（2025年12月にInternational Network for Advanced AI Measurement, Evaluation and Scienceへ改名）が発足し、国際的な共通体制の枠組み形成が進んでいる一方、中国はCnAISDAを設立し、独自の取組を進めている。

*1 GPAI: Global Partnership on Artificial Intelligence
*2 SAFE: Safety and Assurance of Generative AI
*3 AISI国際ネットワーク: The International Network of AI Safety Institutes

【GPAI*の発足】（2020年）
＊44か国が参加（2026年2月時点）

【AISI国際ネットワーク*の発足】（2024年）
＊10か国が参加（2026年2月時点）

カナダ
- Canadian AI Safety Institute（CAISI）の設立（2024年）
- GPAIモントリオール専門家支援センターの設立（2020年）

米国
- U.S. AI Safety Institute（USAISI）の設立（2024年）
  2025年にCenter for AI Standards and Innovation（CAISI）に改名

欧州（英国）
- AI Safety Institute（AISI）の設立（2023年）
  ＊2025年にAI Security Institute（AISI）に改名

欧州（フランス）
- INESIA（Institut national pour l'évaluation et la sécurité de l'IA）の設立（2025年）
- GPAIパリ専門家支援センターの設立（2020年）

欧州（EU）
- European AI Officeの設立（2024年）

日本
- AI Safety Institute（AISI）の設立（2024年）
- GPAI東京専門家支援センターの設立（2024年）

中国
- China AI Safety and Development Association（CnAISDA）の設立（2025年）

イスラエル
- AIの安全性に関する独立した政府機関は確認できていない

インド
- IndiaAI Safety Institute の設立（2025年）

ケニア

オーストラリア

シンガポール

韓国

Partnership on Science of AI Safetyの公表（2024年）

「研究協力の強化に向けた新規ファンディングと、世界的なAIの安全性をさらに高める新たなパートナーシップ」の公表（2024年）

3. アクティブ・サイバー・ディフェンスに関する動向

調査概要

■ 調査目的

国の基幹システムや重要インフラ等の機能を停止させることを狙う、高度な侵入・潜伏能力を備えたサイバー攻撃に対する懸念が急速に高まっていることから、アクティブ・サイバー・ディフェンスの導入が各国で進んでいる。一方で、国内でアクティブ・サイバー・ディフェンス（能動的サイバー防御）を進めるには、その実現に必要な技術だけでなく、政策・規制の動向、社会で実現するにあたっての課題、国際連携の取組、および研究開発動向について理解することが重要と考えられる。そこで、アクティブ・サイバー・ディフェンスに関する動向を調査することで、現状の問題点を把握する。

■ 調査内容

#	調査項目	調査内容
①	アクティブ・サイバー・ディフェンスの定義	各種文献等に関連する用語（例：能動的サイバー防御）も含め、アクティブ・サイバー・ディフェンスの用語の定義、アクティブ・サイバー・ディフェンスを実現するためのプロセス等を調査、整理を実施
②	アクティブ・サイバー・ディフェンスの政策面での方向性	各種文献等をもとに調査対象国の政策・制度の整理を実施
③	アクティブ・サイバー・ディフェンスを各国・地域の社会で実装するための課題	各種文献等をもとに各国・地域の社会での実装状況や課題の整理を実施
④	アクティブ・サイバー・ディフェンスを国際連携で進めるための課題	各種文献等をもとに各国・地域の連携動向や課題の整理を実施
⑤	アクティブ・サイバー・ディフェンスの研究開発動向	セキュリティ関連の8つの学会を対象に、2020～2025年のアクティブ・サイバー・ディフェンスの研究開発動向について調査し、傾向・カテゴリ分析を実施

■ 調査結果

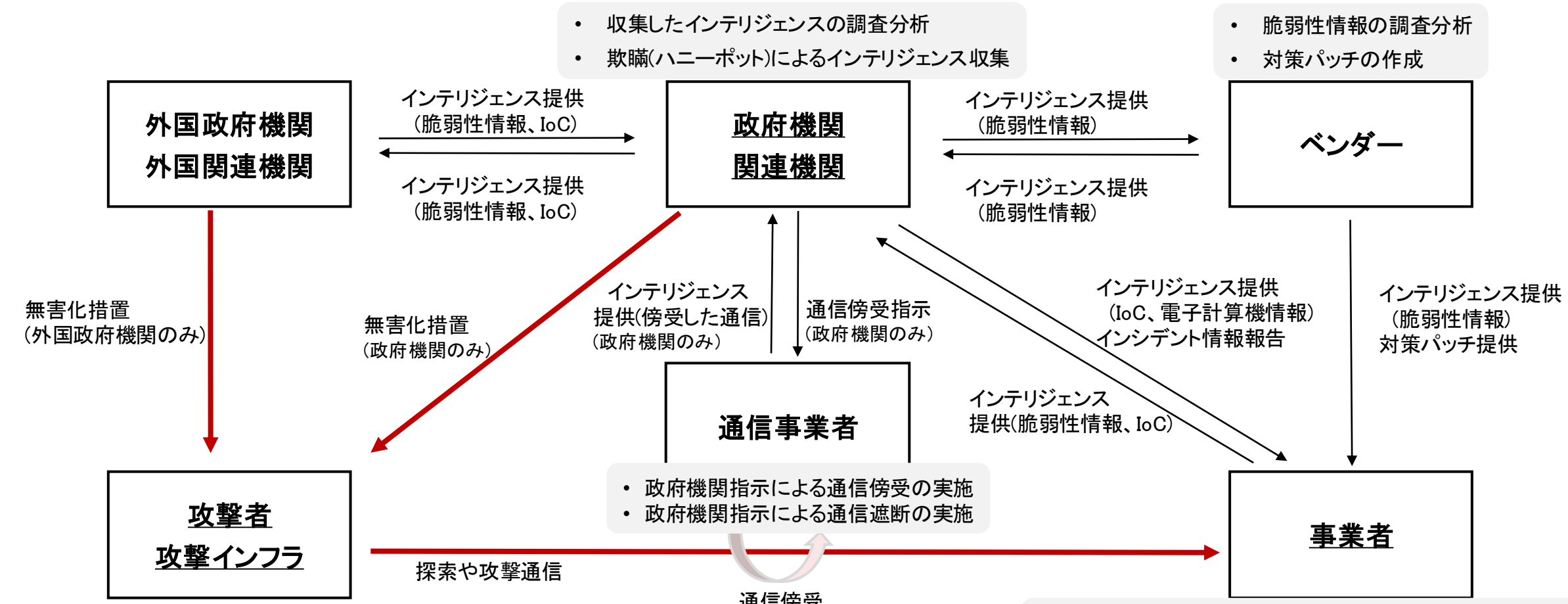
アクティブ・サイバー・ディフェンスの定義や法制度は各国・地域で異なるものの、「事前防御・堅牢化・監査」「情報共有や即時通報」「インテリジェンス収集」「無害化措置」は共通して整備されていることを確認した。その実装においては、通信傍受の透明性確保や人材の育成等が、各国・地域に共通する課題として明らかにした。また、QuadやUKUSA協定といった多国間連携の枠組みは存在するが、各国、地域間での認識の違いや情報共有の枠組み整備が、多国間で連携を深化させる上での課題となっている。関連する主要な学会では、第一著者の所属機関の国・地域が米国、中国、欧州である論文が約9割を占め、特にインテリジェンス分析に関する研究発表が多い傾向が見られる。

日本においては、2025年にサイバー対処能力強化法および同整備法が成立し、全面施行へ向け準備が進められている。他国・地域と比較した日本固有の課題としては、法律上、通信傍受が制限されているため、実効性の確保と他国連携への影響を意識することが必要である。

① アクティブ・サイバー・ディフェンスの定義

- **アクティブ・サイバー・ディフェンスにおいて、政府機関が中心的な役割を果たしている。**

アクティブ・サイバー・ディフェンスに関する一般的な主な実施主体と主な実施内容を以下にまとめた。



IoC(Indicator of Compromise):マルウェアのファイル名、攻撃や探索時に通信先となったIPアドレスなどの痕跡のこと

→ :インテリジェンス情報の提供(脆弱性情報、IoCなど)

➡ :攻撃者による探索や攻撃通信、政府機関/外国政府機関による無害化措置など

① アクティブ・サイバー・ディフェンスの定義

- **アクティブ・サイバー・ディフェンスの用語は各国や地域によっては異なるが、用語の概念としては存在している。**

政策・規制に関する文献等により、アクティブ・サイバー・ディフェンスや能動的サイバー防御等に関する調査を実施し、各国における言葉としての定義や位置づけをまとめた。

国・地域	定義
日本	• 令和4年(2022年)12月に**国家安全保障会議において国家安全保障戦略が決定**され、**能動的サイバー防御(ACD)の考え方や目的、構成要素を明示** • 令和7年(2025年)5月公布の**サイバー対処能力強化法*1及び同整備法*2において、能動的サイバー防御の実現のための法整備を実施** *1 重要電子計算機に対する不正な行為による被害の防止に関する法律 *2 重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律
米国	• 2011年に**DoD(米国国防総省/Department of Defense)においてActive Cyber Defense(ACD)の概念が提唱**され、2015年にはCNSSI(米国国家安全保障システム委員会/Committee of National Security Systems)の用語集で定義されて、それを引用する形で**NIST CSRC GlossaryにActive Cyber Defenseを記述** • 2012年に**DARPA(米国国防高等研究計画局/Defense Advanced Research Projects Agency)においてActive Cyber Defenseに関する研究を実施**
欧州（EU）	• アクティブ・サイバー・ディフェンスという用語は確認できていない。 • 類似した概念としては、2022年に**NIS2指令(Network and Information Systems 2 Directive)において予防や検知、脆弱性管理等のリスク管理措置の義務化され**、2025年に**サイバー連帯法(Cyber Solidarity Act)においてEU全体として即応・相互支援などの枠組みが制度化**された。 • 2025年にENISA(欧州連合サイバーセキュリティ機関/European Union Agency for Cybersecurity)にて、NIS2指令に関しての技術的実装に関してのガイダンスとしてのNIS2 Technical Implementation Guidanceを公表
欧州（英国）	• 2016年に**UK National Cyber Security CentreにおいてActive Cyber Defenceプログラムを開始** • 2022年に**National Cyber StrategyにおいてActive Cyber Defenceを位置づけ**た
イスラエル	• アクティブ・サイバー・ディフェンスという用語は確認できていない。 • 類似した概念としては、**INCD(イスラエル国家サイバー局/Israel National Cyber Directorate)においてActive securityを記述** • INCDが主導する「サイバー・ドーム」においてACDにおける攻撃の検知を行い通信遮断の自動化の推進
中国	• アクティブ・サイバー・ディフェンスという用語は確認できていない。 • 類似した概念としては、**主动防御（Active Defense）があり、GB/T(国家標準推奨) 39204-2022 重要情報インフラの情報セキュリティ技術およびセキュリティ保護要件に記述があるとのこと**。
カナダ	• アクティブ・サイバー・ディフェンスという用語は確認できていない。 • 類似した概念としては、2019年に**CSE法(通信保安局法/Communications Security Establishment Act) が成立し、その中にActive Cyber Operationsに関して記述**
インド	• アクティブ・サイバー・ディフェンスという用語は確認できていない。 • 類似した概念としては、2025年に公開された**Doctrine for Cyberspace OperationsにおいてProactive and adaptive cyber defenceの記述があるとのこと**

② アクティブ・サイバー・ディフェンスの政策面の方向性

- **アクティブ・サイバー・ディフェンスの関わる法律は、どの国や地域も法整備がされているが、カバーする範囲は法律により異なっている。**

アクティブ・サイバー・ディフェンスや能動的サイバー防御等について対象国の法制度を調査し、整理比較した。以下に分析結果を示す。
主な罰則規定は次スライドにまとめた。

国・地域	(1)事前防御・堅牢化・監査	(2)情報共有や即時通報	(3)インテリジェンス収集 (ハニーポットや通信傍受)	(4)無害化措置 (テイクダウン・通信遮断)
日本	サイバー対処能力強化法および同整備法(25年)【罰則】 重要経済安保情報保護・活用法(24年)【罰則】	サイバーセキュリティ基本法(14年) 重要経済安保情報保護・活用法(24年)【罰則】	サイバー対処能力強化法および同整備法(25年)【罰則】	
米国	Executive Order 14028 – Improving the Nation's Cybersecurity(21年) CISA Binding Operational Directives/BODs (15年)	Cybersecurity Information Sharing Act of 2015 Cyber Incident Reporting for Critical Infrastructure Act/CIRCIA(22年)【罰則】	Foreign Intelligence Surveillance Act Section 702/FISA(78年)【罰則】	Federal Rules of Criminal Procedure Rule 41(16年) Computer Fraud and Abuse Act(86年)【罰則】
欧州(EU)	Directive (EU) 2022/2555/NIS2指令(22年)【罰則】 Cyber Resilience Act/CRA(24年)【罰則】		Cyber Solidarity Act(25年)	
欧州(英国)	The Network and Information Systems Regulations 2018(NIS規則)【罰則】 Cyber Security and Resilience Bill(25年)【罰則】		Investigatory Powers Act 2016(16年)【罰則】	Investigatory Powers (Amendment) Act 2024(24年)【罰則】
イスラエル	Protection of Privacy Regulations (Data Security), 5777-2017(18年)【罰則】	Amendment No. 13 to the Privacy Protection Law(25年)【罰則】	Security Service Law(02年)	National Cyber Protection Law(26年)【罰則】
中国	サイバーセキュリティ法 (25年)【罰則】	国家サイバーセキュリティ事件報告管理方法(25年)	データ安全法 (2021年) 国家情報法 (17年)【罰則】	サイバーセキュリティ法(26年)【罰則】
カナダ	Critical Cyber Systems Protection Act/CCSPA(25年) 法案(25年)【罰則案】		CSE Act 2019(19年)	
インド	Information Technology Act(8年)【罰則】	CERT-In Directions(22年)【罰則】	Telecommunications Act(23年)【罰則】	Information Technology Act(9年)【罰則】

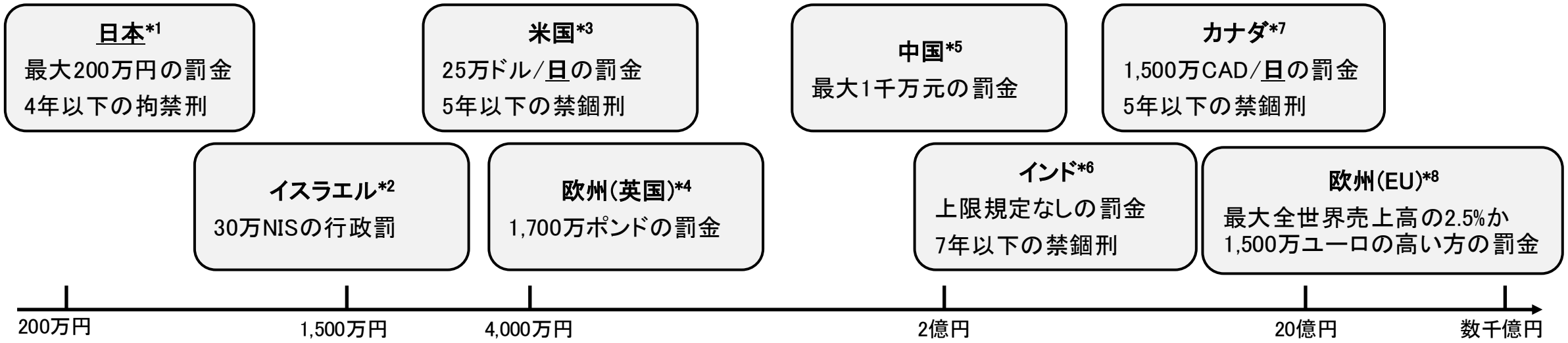
西暦:法律や法案、規則が公布/提出/公開された一番新しい年　【罰則】:罰則規定がある法律や法案

② アクティブ・サイバー・ディフェンスの政策面の方向性

- **罰則に関しては、個人に対しては拘禁刑/禁錮刑や罰金、企業に対しては罰金が科せられている。**
- **直接的な罰則以外に政府契約の解除や将来の入札禁止、予算制限などの制裁措置、経営陣の職務停止といった罰則もあった。**

アクティブ・サイバー・ディフェンスや能動的サイバー防御等について対象国の法制度を調査し、罰則規定の観点で整理比較した。

◎報告義務違反や措置命令違反に関しての各国や組織における罰則の比較(米国とカナダは一日当たりの罰金)



◎その他の罰則

- 日本*1　インシデント報告義務違反や是正命令違反の場合、民間企業の従業員や法人に対して、200万円以下の罰金(両罰規定あり)。
- 米国*9　要件未達の場合、政府契約の解除や将来の入札禁止(Debarment)の対象
- 欧州(EU)*10　経営者の関与義務違反の場合、一時的な職務停止や経営職務からの排除
- 中国*5　域外の主体に対しての制裁:資産凍結、取引停止、入国禁止(ネット安全法にて処罰)

*1:サイバー対処能力強化法および同整備法 *2:National Cyber Protection Law(法案) *3:Foreign Intelligence Surveillance Act Section 702/FISA、法廷侮辱罪
*4:The Network and Information Systems Regulations 2018 *5:サイバーセキュリティ法 *6:Information Technology Act *7:Critical Cyber Systems Protection Act
*8:Cyber Resilience Act/CRA *9:Executive Order 14028 – Improving the Nation's Cybersecurity *10:Directive (EU) 2022/2555/NIS2指令

④ アクティブ・サイバー・ディフェンスを国際連携で進めるための課題

- **慎重かつ機敏な対応が求められるアクティブ・サイバー・ディフェンスを国際的な連携で進めるうえで、各国や組織で共通の認識や事前準備、信頼の構築を実施する必要があり、法制度や外交的立場の違いにより足並みを揃えるためには課題が残っている。**

アクティブ・サイバー・ディフェンスや能動的サイバー防御等について複数の国や地域間の国際連携の内容を調査し、課題を整理した。以下に分析結果をまとめた。

1. アクティブ・サイバー・ディフェンスに対する各国や地域の認識の違い
   - **他国に対してアクティブ・サイバー・ディフェンスにおける無害化措置を実施した際、相手国から主権侵害や武力行使とみなされないように外交的正当化や国際法上の紛争に発展するリスクの軽減が課題**である。一方で**各国から無害化措置を実施されないようにデュー・ディリジェンス責任を果たすことが重要**である。
   - EUにおいては、攻撃対象の端末がEU以外の国にある場合、EUとして「どのような対応や制裁を行うか」についての加盟国27カ国の意見集約の迅速化が課題である。Cyber Solidarity Actにおいて、サイバー対応メカニズムやEU-CyCLONe（サイバー危機連絡組織ネットワーク）などが制定されているため、迅速な意見集約や対応をするための仕組みは整備されつつあるが、加盟国の対応に依存する面も残っている。
   - **国により法的な解釈や制限が異なるため、複数の国々で共同作戦を実施する際、足並みを揃えることが課題**である。

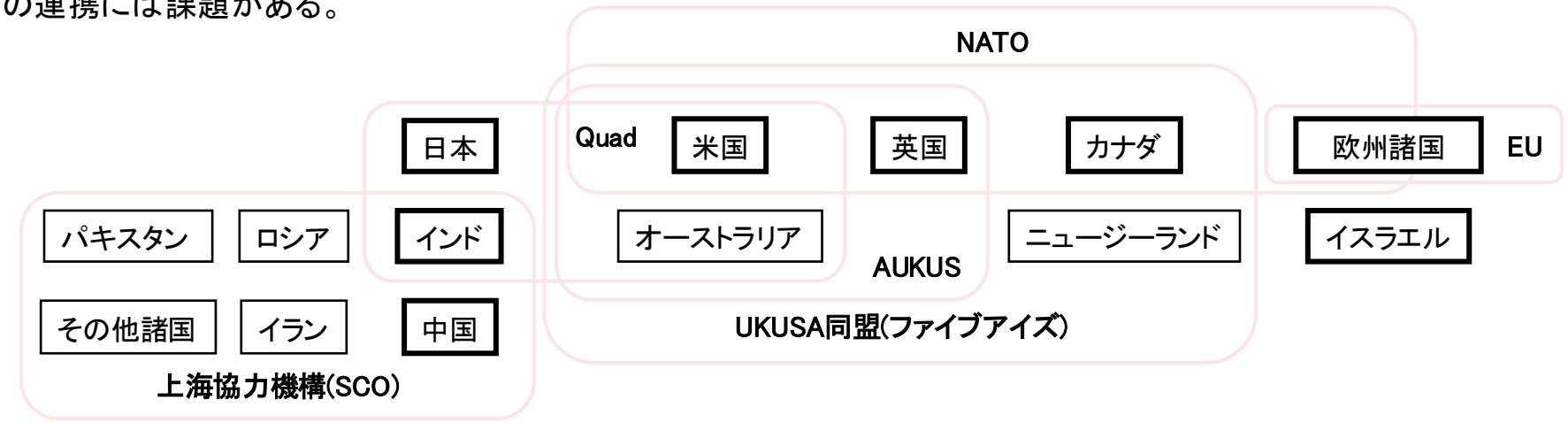
2. 情報共有の仕組み
   - アクティブ・サイバー・ディフェンスを実施するにあたり、一つの国や地域で得られる情報のみではなく、複数の国や地域が相互に情報を共有することが重要である。そのために信頼構築や情報共有の仕組みの整備が課題であり、特に**機密情報を共有するためにセキュリティクリアランスの徹底による相互の信頼構築や、技術的なセキュリティレベルの平準化や法律の整備、運用ルールの策定などを推進する必要**がある。また、タイムリーな情報共有を行うため、これらの整備は事前に実施しておく必要がある。
   - インドにおいては、多くの欧米諸国のグローバル企業のIT運用やSOC（Security Operation Center）の委託先として機能し、民間企業における運用・監視レベルの国際化が進んでいる。一方で、国家レベルの機密情報の国際化は別途必要である。

④ アクティブ・サイバー・ディフェンスを国際連携で進めるための課題

- **アクティブ・サイバー・ディフェンスを実施するための国際連携における複数国間の連携は重要であり、米国を中心に進んでいる。**
- **米国を含まない他国間連携や二国間連携も進んでおり、各国や組織によっての戦略の違いが出ている。**

3. 複数国間連携の枠組み

- アクティブ・サイバー・ディフェンスのための情報共有を含んだ複数国間連携の枠組みとしては、米国を中心とした**Quad(日米豪印戦略対話/Quadrilateral Security Dialogue)**や**UKUSA協定(United Kingdom-United States of America Agreement。別称ファイブアイズ)**、**AUKUS(Australia, United Kingdom, United States)**等の枠組みがあり、**NATO(北大西洋条約機構/North Atlantic Treaty Organization)**においても同様の役割を果たしている。**それぞれの構成国や位置づけ、各国の技術水準や法制度が異なるため、円滑な連携に向けての課題**がある。
- イスラエルにおいては、二国間連携として米国との特別な関係（Special Relationship）にありACDにおいても緊密に連携している。また、インドやドイツともそれぞれ2国間連携を進めており、ACD関連技術の共有をベースにした国際連携を進めている。
- 中国においては、欧米諸国の国際連携の枠組みには入っていない。一方で、**SCO(上海協力機構/Shanghai Cooperation Organization)**として複数の国と連携をしているが、連携の目的や加盟国間の関係性より一貫した方針を取るのは難しく、欧米諸国の国際連携のような欧米諸国の国際連携のように機密情報のやり取りや技術協力の推進は課題である。また、中国の国家観やガバナンスモデルの違いから、欧米諸国との連携には課題がある。

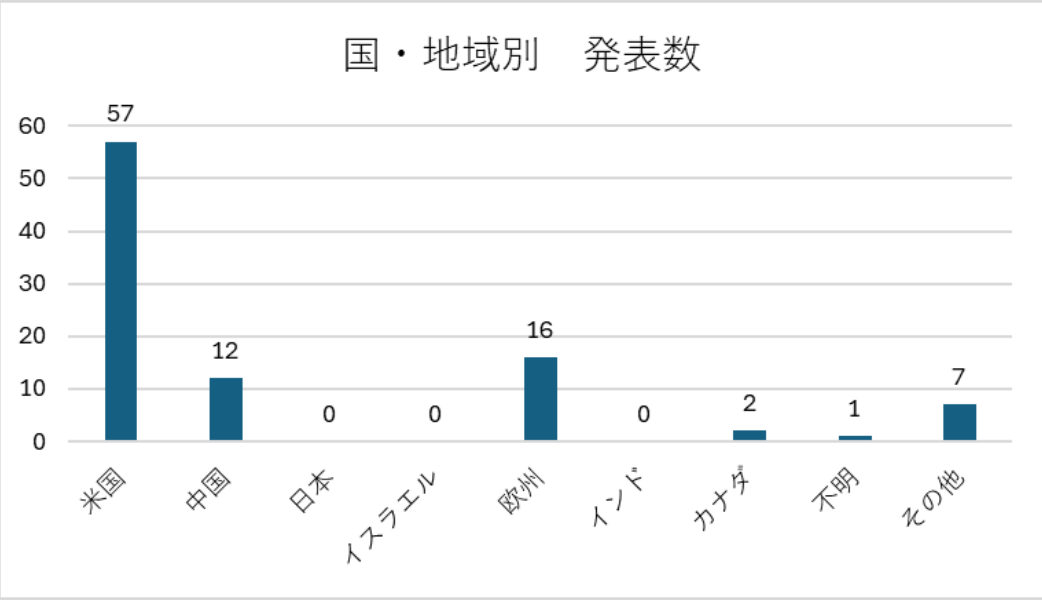


調査対象国を中心とした多国籍間の連携の枠組み

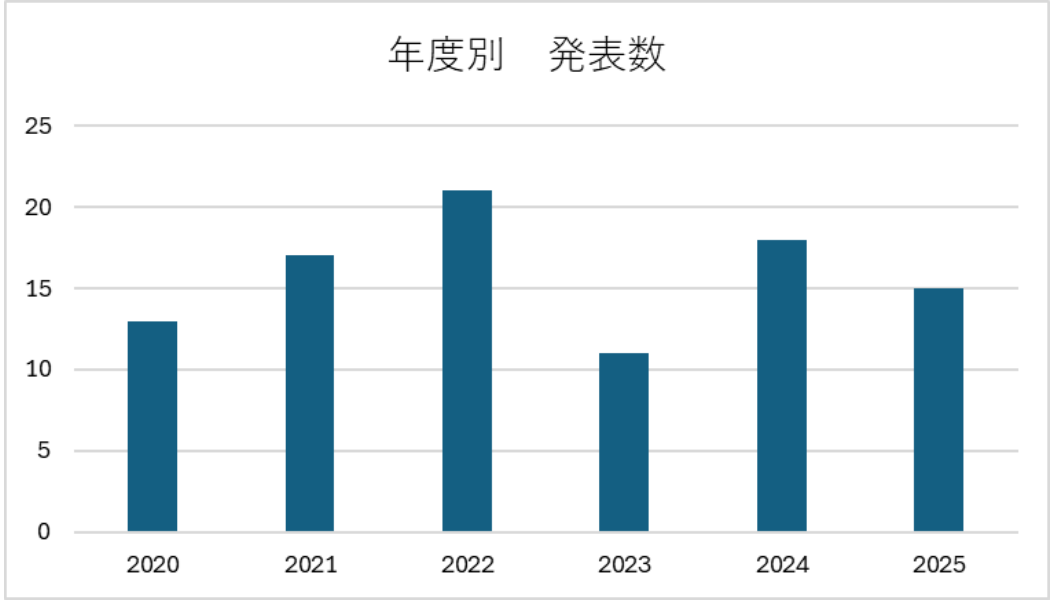
⑤ アクティブ・サイバー・ディフェンスの研究開発動向｜分析結果

- **アクティブ・サイバー・ディフェンスは国防に関する点もあるため、投稿／発表数自体は少ない。**
- **2023年については、生成AIに関する投稿／発表の増加により、アクティブ・サイバー・ディフェンスの採択率が若干低下した可能性がある。**

- 調査範囲において、アクティブ・サイバー・ディフェンスに関連する発表は計95件と比較的少ない。



国・地域別に見ると、投稿／発表数において米国が圧倒的首位。次いで欧州、中国の投稿／発表が見受けられた。



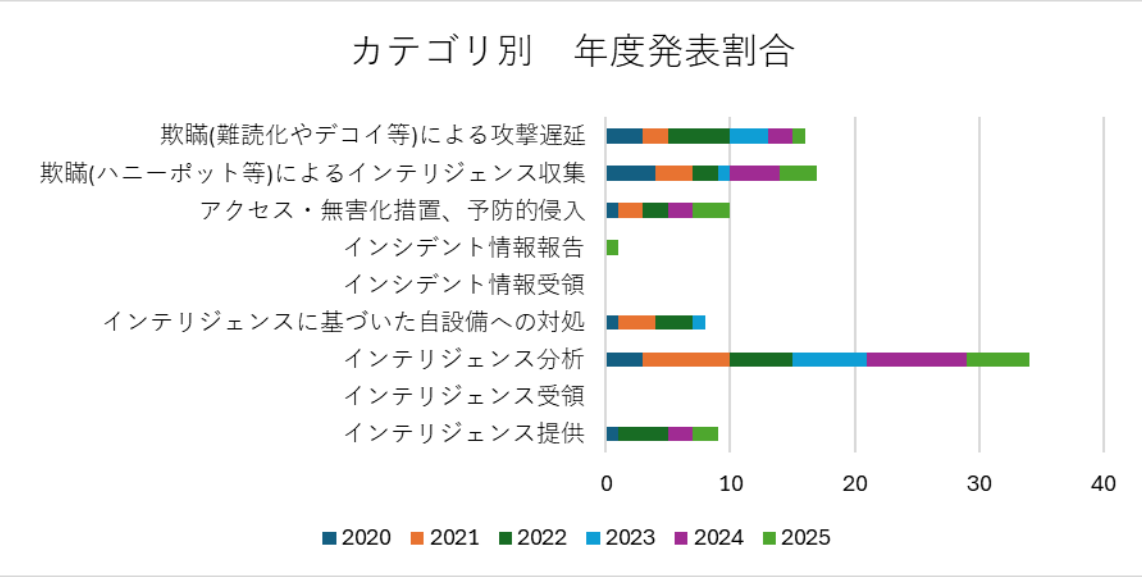
投稿／発表数について、2023年に急落していることが判明。同年に生成AIに関する投稿／発表が増加したことが一因の可能性がある。

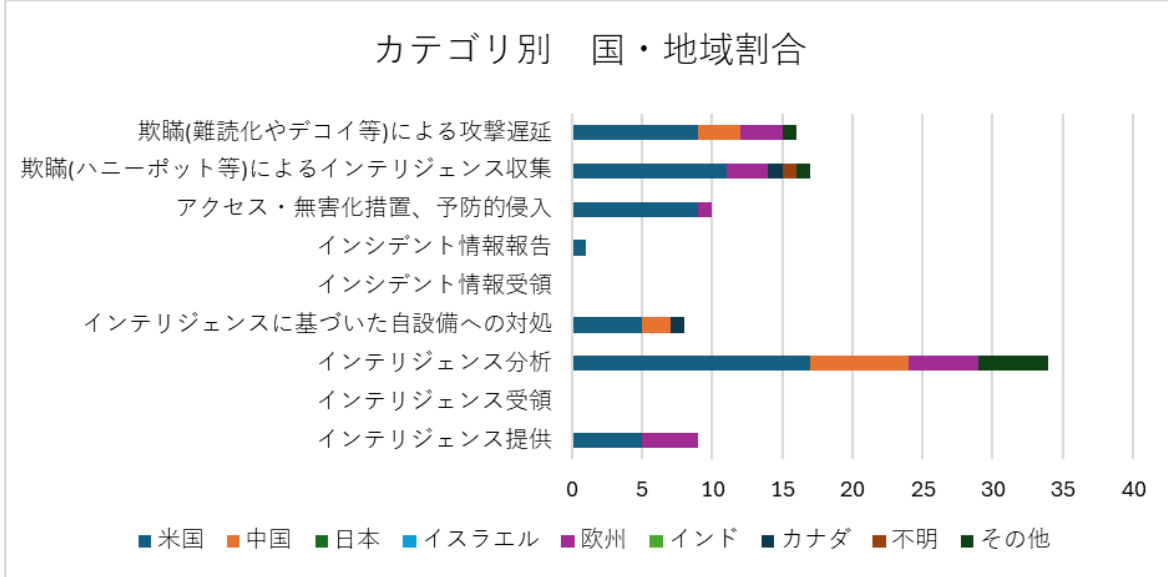
※ 調査期間：2020～2025，調査学会：[A][B][C][D][E][F][G][M]（「参考文献」参照）

⑤ アクティブ・サイバー・ディフェンスの研究開発動向｜分析結果

- **投稿／発表カテゴリとして、「インテリジェンス分析」に関する発表が多い傾向が見受けられた。**
- **母数自体が少ないこともあり、国・地域に起因したカテゴリ傾向については特に見受けられなかった。**

- 以下カテゴリの観点で傾向分析を実施
  - 欺瞞(難読化やデコイ等)による攻撃遅延
  - 欺瞞(ハニーポット等)によるインテリジェンス収集
  - アクセス・無害化措置、予防的侵入
  - インシデント情報報告
  - インテリジェンスに基づいた自設備への対処
  - インテリジェンス分析
  - インテリジェンス提供





⑤ アクティブ・サイバー・ディフェンスの研究開発動向｜研究内容紹介

- **学会によって投稿／発表内容の踏み込み度合が異なる。特にDEF CONでは、犯罪組織への潜入などの発表も確認した。**
- **また、生成AIを用いた発表は少ない印象があった。**

年	学会	タイトル	著者	概要
2025	DEF CON	Kill List: Hacking an Assassination Site on the Dark Web [1]	Carl Miller他	ダークウェブ上の暗殺請負サイトで脆弱性が見つかり、暗殺依頼（氏名・住所・行動情報・写真等）を傍受可能になったことを端緒に、注文の収集・精査、当局連携、標的への直接警告へと発展した調査記録。結果として175件超の依頼開示、34逮捕、28有罪、180年超の実刑につながった旨が説明されている
2025	NDSS	Hitchhiking Vaccine: Enhancing Botnet Remediation With Remote Code Deployment Reuse [2]	Runze Zhang他	マルウェアの更新機構を逆利用して、駆除用ペイロードを配布する構想を提示。自動解析パイプライン ECHO を実装し、Androidマルウェア702件の調査で523件が当該アプローチにより駆除/無効化/警告可能と報告
2024	DEF CON	Behind Enemy Lines: Going undercover to breach the LockBit Ransomware Operation [3]	Jon DiMaggio (Analyst1)	LockBitランサムウェア集団に対し、講演者が長期の潜入（undercover）で信頼獲得・内部コミュニケーションの観察を行い、集団の実態理解やリーダー（LockBitSupp）の実体特定に関与した、という発表。犯罪組織の運用や意思決定に迫る旨が説明されている
2020	NDSS	Into the Deep Web: Understanding E-commerce Fraud from Autonomous Chat with Cybercriminals [4]	Peng Wang他	自律チャットボットAubreyで実在の詐欺関係者と会話し情報収集。会話を有限状態機械（FSM）的に設計して自動対話を成立させ、470人の詐欺関係者とチャットし、未知のSIMゲートウェイやアカウント売買サイト、攻撃ツール等のアーティファクトを収集。詐欺のサプライチェーンや役割間関係（共謀・転売等）も明らかにしたと報告

[1]: https://defcon.org/html/defcon-33/dc-33-speakers.html#content_60382
[2]: https://www.ndss-symposium.org/ndss-paper/hitchhiking-vaccine-enhancing-botnet-remediation-with-remote-code-deployment-reuse/
[3]: https://defcon.org/html/defcon-32/dc-32-speakers.html#54433
[4]: https://www.ndss-symposium.org/ndss-paper/into-the-deep-web-understanding-e-commerce-fraud-from-autonomous-chat-with-cybercriminals/

4. サイバーセキュリティ人材の育成に関する動向

調査概要

■ 調査目的

サイバー攻撃の高度化・巧妙化を背景に、サイバーセキュリティ人材の育成・確保は世界的な喫緊の課題となっている。生成AIの普及は、人材育成・確保のあり方にも影響を与えつつある。そこで、各国・地域および産業等における現状と、生成AI等による変化を調査し、課題整理を行う。

■ 調査内容

#	調査項目	調査内容
①	サイバーセキュリティ人材の充足状況	調査対象国・地域のサイバーセキュリティ人材の充足状況を調査
②	サイバーセキュリティ人材の育成に関する政策・規制動向	教育課程の年齢を対象とした各国・地域の育成に関する政府機関等の取組、サイバーセキュリティに関する学科の比較、人材育成フレームワーク、セキュリティ・クリアランスを調査
③	サイバーセキュリティ人材の育成に関する国際連携動向	各国・地域間やパートナーシップ等の協力関係や、国際機関における人材育成に関する取組を調査
④	サイバーセキュリティ人材の育成に関する研究開発動向	セキュリティに関する主要な学会*での発表論文の調査を行い、調査項目に関わる論文の投稿数や第一著者の所属機関の国・地域、主要な研究機関の研究内容について分析 * 具体的な学会は参考文献を参照
⑤	サイバーセキュリティ人材の育成に関する産業動向	セキュリティトレーニングや教育コンテンツの製品・サービスの開発企業の国・地域別の比較、生成AIを活用した製品について調査。また、AI×セキュリティに関する国際資格の動向を調査

■ 調査結果

政策・規制および国際連携では、生成AIと人材育成を明確に関連付けた取組は確認できなかったが、大学において、AI×セキュリティの学科を設置している国は確認できた。サイバーセキュリティやAI分野における自国・地域内の人材育成・確保を強化する取組や、国際連携を推進する動きが見られた。また、重要な機密を取り扱う個人に対するセキュリティ・クリアランスが国際的に重要視されており、各国・地域ともに制度化が進んでいる。研究開発・産業面においては、AIの普及に伴う職域の再定義やスキルセットの再構築の必要性が指摘されており、AIとサイバーセキュリティの双方に関する知識を求める国際資格も登場しつつある。

日本においては、2025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」で、「AIとサイバーセキュリティの両方の専門性を兼ね備えた人材の発掘・育成に向けた取組も推進する」と明記されている。今後は、AIとサイバーセキュリティの双方の知識を有した人材の育成・確保の重要性が一層高まると考えられる。

① サイバーセキュリティ人材の充足状況

- **不足人数等に差はあるが、各国・地域それぞれサイバーセキュリティ人材は不足している状況となる。**

国・地域	充足状況	サイバーセキュリティ人材の労働力ギャップの概要	引用元
日本	不足	2023年の調査結果において、現状が48万人で、11万人不足している	• 経済産業省「サイバーセキュリティ人材の育成促進に向けた検討会最終取りまとめ」 • ISC2 CYBERSECURITY WORKFORCE STUDY 2023 (2023)
カナダ	不足	「Cybersecurity Specialists」は3万1,800人雇用されており、2021～2023年の労働市場の状況としては不足の兆候は中程度（moderate signs of shortage）である	• Government of Canada「Cybersecurity specialists (2024-2033) | Canadian Occupational Projection System (COPS)」(2025)
米国	不足	サイバーセキュリティ関連の業務に従事する労働者の推定数は133万7,400人（2026）で、需給比率（Supply vs Demand Ratio）は74%（2025）で労働力が不足している	• CyberSeek「Cybersecurity Supply/Demand Heat Map」(2026)
欧州（EU）	不足	2022年、EUにおけるサイバーセキュリティ専門家の不足は26万人から50万人であったが、ニーズは88万3,000人と推定されており、労働力のギャップが発生している	• European Commission「Communication on the Cybersecurity Skills Academy」(2023)
欧州（英国）	不足	約14万3,000人がサイバーセキュリティの職務に従事しており、労働力のギャップは約3,800人で、2023年のレポートの1万1,100人から大幅に減少している	• Department for Science, Innovation & Technology「Cyber security skills in the UK labour market 2025」(2025)
イスラエル	－(*)	2023年のハイテク分野（フィンテック等サイバーセキュリティ以外の分野を含む）での雇用者数は約39万6,000人で、前年比で1万人増加	• Israel Innovation Authority「2024 Annual Report The State of High-Tech」(2024)
中国	不足	2019年のサイバーセキュリティ人材ギャップは70万から140万人で、サイバーセキュリティ専門家は約10万人だったため、人材ギャップ率は93%に達していた。必要とされる専門家の数は、2020年には155万人、2027年には327万人になるとされており、トレーニングを受けている人材数（3万人/年）とは乖離がある	• Center for Security and Emerging Technology「2022 White Paper on the Live-Fire Capabilities of Cybersecurity Talents: Attack and Defense Live-Fire Capability Edition」(2023) (2022网络安全人才实战能力白皮书 攻防实战能力篇の英訳)
インド	不足	2025年までに推定150万人のサイバーセキュリティの人材の職員が埋まらない	• Data Security Council of India (DSCI)「Indian Cybersecurity Product Landscape Report 3.0」(2025)

＊イスラエルに関しては、フィンテック等サイバーセキュリティ以外の分野を含む「ハイテク分野」の区分で人材数が記載されているため、サイバーセキュリティに関する人材の過不足は判断できないため「－」とした

② サイバーセキュリティ人材の育成に関する政策・規制動向｜人材育成

- **中等教育以前の人材育成は、各国・地域の教育制度等の違いにより、カリキュラム重視や放課後教育重視等、取組に差が見られる。**
- **高等教育におけるサイバーセキュリティ教育の品質向上や、関連する学部・学科の拡充を目的として、米国や中国等では、政府が教育機関の認証を行っている。また、高度なサイバーセキュリティ人材の育成を支援するため、修士・博士課程の学生に対する給与の支給、奨学金の提供、企業での実習機会の付与等の取組を行っている国も見られる。**

日本	米国	欧州（EU、ドイツ）	欧州（英国）
【中等教育以前における育成の取組】 • サイバーセキュリティに関する包括的なカリキュラムや大規模な学習プラットフォームはないが、中学校の「技術・家庭科」、高等学校の「情報Ⅰ・Ⅱ」において、情報セキュリティに関する基礎的な事項を履修している。情報セキュリティや生成AI等の教育を拡充するため、中学校で「新・技術分野（仮称）」が創設される方針となる **【高等教育における育成の取組】** • 2023年に「KOSENサイバーセキュリティ教育推進センター」を国立高等専門学校機構に設置し、サイバーセキュリティ人材育成のためのエコシステム構築等の取組を推進し、プラス・セキュリティ人材、トップ人材の輩出を目指す （2024年3月で政府支援が終了） • 「数理・データサイエンス・AI教育プログラム認定制度」を設け、大学、高等専門学校のサイバーセキュリティを含む数理・データサイエンス・AIに関する正規課程の教育プログラムのうち、一定の要件を満たした優れた教育プログラムを政府が認定する	**【中等教育以前における育成の取組】** • CISAより助成金を受けて運営しているCYBER.ORGより、2021年にK-12全体（5～18歳）を対象とした統一的なカリキュラムであるK-12 Cybersecurity Learning Standardsが公開された。「コンピューティングシステム」、「デジタルシチズンシップ」、「セキュリティ」の3つをコアコンセプトとしたサイバーセキュリティの包括的なカリキュラムを提供している **【高等教育における育成の取組】** • NSAが主導する「NCAE-C（National Centers of Academic Excellence in Cybersecurity）」プログラムにて、国内のサイバーセキュリティに関する教育機関（College、University）を「Cyber Defense」、「Cyber Research」、「Cyber Operations」の3区分にて認証を行っている。約500校（2026年2月時点）が認定を受けており、認定機関の学生に対し、卒業後一定期間米国政府への勤務を義務とした奨学金制度を設けている	**【高等教育における育成の取組（EU）】** • 2023年にEUのサイバーセキュリティ人材不足に対応することを目的とした「サイバーセキュリティ・スキル・アカデミー（Cyber Skills Academy）」が立ち上げられ、その取組のひとつとして、産学ネットワークの強化を図っている **【高等教育における育成の取組（ドイツ）】** • ドイツの博士課程の学生は一般的に大学のリサーチ・アシスタントとして働いており、雇用契約に基づき給与を得ながら研究に従事している。 ➢ 参考: 公共部門研究者の典型的な給与（TV-L E13） 48,000～60,000ユーロ/年間[1] （2024年におけるフルタイム雇用労働者の平均年収は62235ユーロ）[2]	AIの普及に伴う雇用の変化に対応するため、2015年より開始された「CyberFirst」プログラムを基盤とし、2025年にDSIT（科学・イノベーション・技術省/Department for Science, Innovation and Technology）が「TechFirst」プログラムを開始した **【中等教育以前における育成の取組】** • 11～18歳を対象とする「TechYouth」の取組のひとつとして、11～14歳を対象とし、カリキュラムを補完する課外活動の位置付けで、インタラクティブな無料のサイバーセキュリティ学習プラットフォーム「Cyber Explorers」を展開している **【高等教育における育成の取組】** • テックキャリアを目指す学部生900名、修士課程学生100名/年を支援する「TechGrad奨学金」、AIを研究分野とする修士課程学生を支援する「Spärck AI Scholarship」等が設けられており、奨学金の給付の他、企業への実習支援等も実施している • サイバーセキュリティ、機械学習等のフロンティア技術を研究分野とする博士課程の学生500名を支援する「TechExpert」がある

[1]: A quick guide to research funding in Germany, https://www.research-in-germany.org/en/funding-jobs.html
[2]: フルタイム労働者の中央値年収は5万2159ユーロ―連邦統計局, https://www.jil.go.jp/foreign/jihou/2025/07/germany_03.html

4. サイバーセキュリティ人材の育成に関する動向
② サイバーセキュリティ人材の育成に関する政策・規制動向｜人材育成

イスラエル	中国	カナダ	インド
【中等教育以前における育成の取組】 • 2011年に開始されたCyber Education Centerの「Magshimimプログラム」は、選抜された生徒に対し、10～12年生の3年間、サイバーセキュリティに関する学習を放課後に行う。コース終了時のスキルは、米国のコンピュータサイエンスを専攻する学部生相当となる **【高等教育における育成の取組】** • 多くの大学でサイバーセキュリティの学部専攻を設けている。また、アカデミアをサイバーセキュリティエコシステムの重要な柱と位置付け、INCD（国家サイバー総局/Israel National Cyber Directorate）は「The National Cyber Security Research Center Program」として6つの研究センターを設立しており、産学官軍が連携するハブである「CyberSpark」には、研究センターの1つであるBen-gurion universityが参加している ➢ Haifa university – The Center for Cyber Law & Policy（CCLP） ➢ Technion – Hiroshi Fujiwara Cyber Security Research Center ➢ Tel-aviv university –The Blavatnik Interdisciplinary Cyber Research Center（ICRC） ➢ Bar-ilan university – BIU Research Center in Applied Cryptography and Cyber Security ➢ Hebrew university – HUJI Cyber security Research Center（H-CSRC） ➢ Ben-gurion university – Cyber@BGU	**【中等教育以前における育成の取組】** • 2021年に中等職業教育、高等職業教育（専科教育、本科教育）の専攻リストが「職業教育専門分野リスト」として再編され、サイバーセキュリティが追加されている **【高等教育における育成の取組】** • 2017年、教育省とCAC（Cyberspace Administration of China/サイバースペース管理局）は、世界水準のサイバーセキュリティ大学を認定するWCCS（一流网络安全学院/World-Class Cybersecurity Schools）と呼ばれるプログラムを開始。5年ごとに認定の選抜が行われ、2024年1月の新フェーズでは16校が認定され、これまでに国内90以上の大学がサイバーセキュリティ関連の学部を設置、200以上の大学が専攻を設置している。 2024年6月時点では、サイバースペースセキュリティ学科を設置している高等教育機関は626校となる。	**【中等教育以前における育成の取組】** • ニューブランズウィック州では、Career Connected Learningとして12年生を対象とした「Cybersecurity 120」コースを開講している。Computational Thinking（計算論的思考）を用いて、サイバーセキュリティの課題を分析し、リスク低減を目指すことを目的としている。サイバーセキュリティの基礎的な知識の習得だけでなく、ケーススタディなどの実践的な内容も含まれている **【高等教育における育成の取組】** • カナダ・サイバーセキュリティ・センター（CCCS/Canadian Centre for Cyber Security）では、カナダの学術機関で新たなサイバーセキュリティに関するプログラムやコースが立ち上がっている中、国内の教育の質を向上させることを目的に、高等教育機関のサイバーセキュリティのカリキュラムの見直し支援（Cyber security curriculum review）を行っている	**【中等教育以前における育成の取組】** • 5年間で22万5,000人のサイバーセキュリティの訓練を受けた個人の育成を目指す「Information Security Education and Awareness（ISEA）プロジェクト」の第3フェーズ」が2023年推進されており、ハッカソン等のイベントを開催している **【高等教育における育成の取組】** • Electronics System Design and Manufacturing（ESDM）とIT/IT Enabled Services（IT/ITES）セクターにおける博士号取得者数を増やすため、2014年から「Visvesvaraya PhD Scheme」を開始。2021年より第2フェーズが開始され9年間でフルタイム学生を1000人、パートタイム学生を150人等を支援することを目標としており、国際会議への参加費用や、選抜者には海外の研究室への訪問費用等も支援に含まれる[1] 第2フェーズにおいては、現時点でサイバーセキュリティに関する研究領域（Cyber Security, Cryptography、Digital Forensics、Hardware Security、Cyber-physical system, Biometric Security）で20名程度の学生が支援を受けている

[1]: PhD Scheme, https://phd.dic.gov.in/

② サイバーセキュリティ人材の育成に関する政策・規制動向｜“セキュリティ”表記のある学科数の比較

- **韓国、中国がサイバーセキュリティを専門とする学科を新設し設置数を増やしているのに対し、日本は学科として設置されている大学が二校に留まる。**

＜“セキュリティ”表記のある学科数の日本、韓国、中国の比較＞

日本	• “セキュリティ”表記のある学科を設置しているのは、二校（長崎県立大学 情報セキュリティ学科、情報セキュリティ大学院大学 情報セキュリティ研究科）となる • 【参考】大学数: 813校、大学院数: 665校（2024年5月時点）[1]
韓国	• “セキュリティ”表記のある学科を設置しているのは、149校 203学科あり、うち14学科が学科名にAIとセキュリティを含んでいる[2] 例: Korea University College of Science and Technology Department of AI Cyber Security • 【参考】4年制大学: 223校、専門大学: 144校、大学院大学: 44校（2022年時点）[3]
中国	• サイバースペースセキュリティ学科を設置している高等教育機関は626校（2024年6月時点） • 世界水準のサイバーセキュリティ大学を認定するWCCSプログラムの国家政策等の影響で、学部・学科の再編等を行い、学科の設置が増加しているとみられる • 【参考】香港、マカオ、台湾を除く中国本土の高等教育機関: 3072校（2023年6月時点）[4]

[1]: 文部科学省 令和6年度全国大学一覧 08大学に関する統計等, https://www.mext.go.jp/a_menu/koutou/ichiran/mext_00038.html
[2]: Higher Education in Korea > Department information by keyword よりデータを抽出して集計, https://www.academyinfo.go.kr/mjrinfo/mjrinfo0450/doInit.do
[3]: 引用: JST/APRCレポート「韓国における主要大学と企業の協力動向」, https://spap.jst.go.jp/investigation/downloads/2024_tp_02.pdf
[4]: 引用: 中国教育部 全国高等学校名単, http://www.moe.gov.cn/jyb_xxgk/s5743/s5744/A03/202306/t20230619_1064976.html

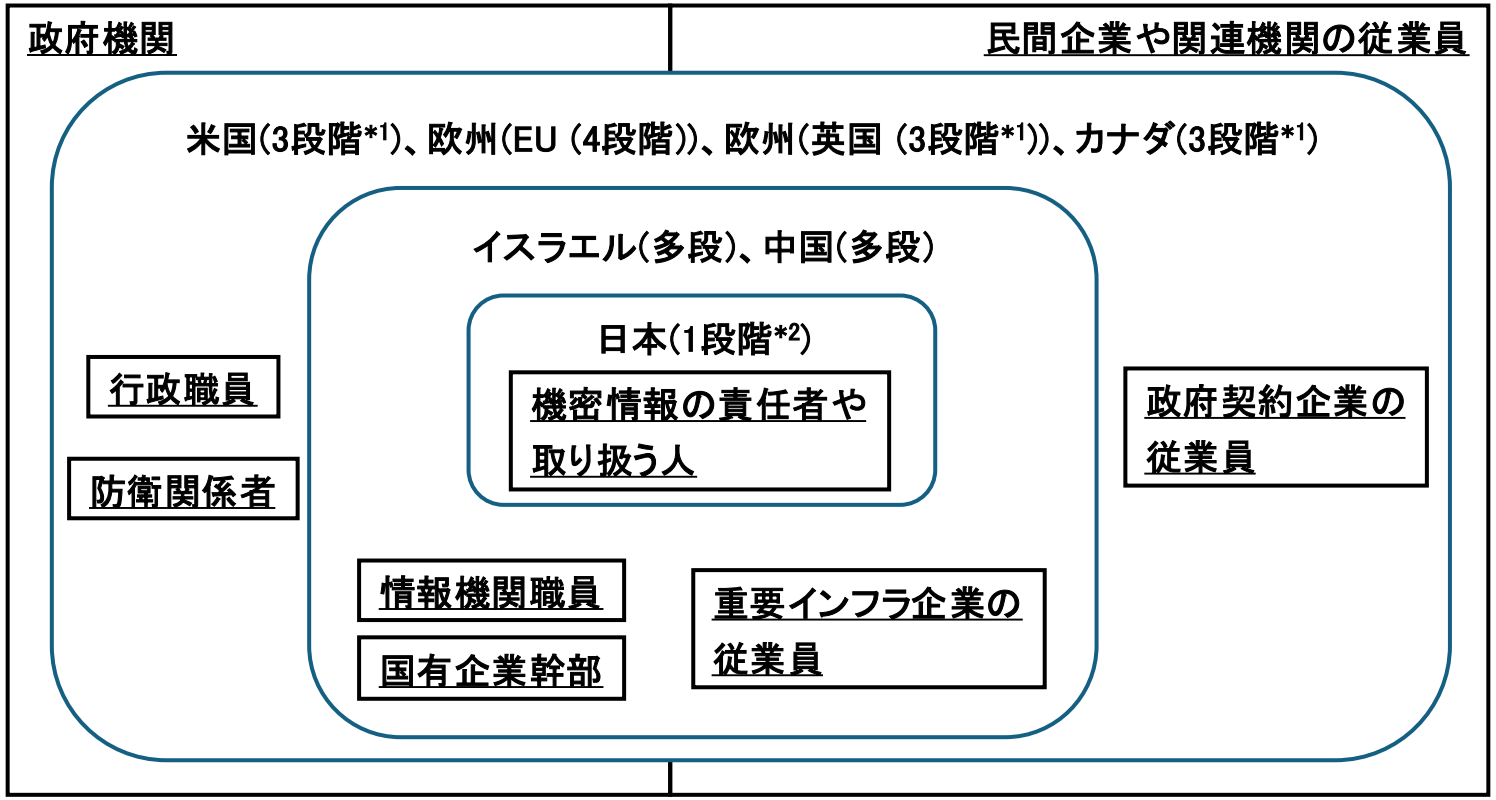
② サイバーセキュリティ人材の育成に関する政策・規制動向｜人材育成フレームワーク

- **米国NISTのNICE Frameworkが国際的に広く参照され、各国の人材育成フレームワークに多くの影響を与えている。**
- **一方で、中国は国家標準として能力要件を規定し、インドは国家資格の枠組みにより職種横断で学習成果ベースのレベル整理を行うなど、各国で違いが見受けられる。**

国・地域	フレームワーク名	公開年 改定年	説明
日本	セキュリティ知識分野（SecBoK） 人材スキルマップ	2003年 2025年	JNSA(日本ネットワークセキュリティ協会)が策定。15役割(ロール)とNICE Frameworkの スキル項目(スキル項目約1200弱)とのマッピングを実施 ITSS+ セキュリティ領域との連携も意識
	ITSS+ セキュリティ領域	2020年 2022年	IPAが公開。日本の実務に即し、橋渡し人材から専門家までを網羅する実務型基準 17分野のサイバーセキュリティの関連領域を定義
米国	NICE Framework （NIST SP 800-181）	2017年 2025年	NISTが策定。世界のデファクトスタンダードのフレームワーク。7つのカテゴリーを33の専門分野と 52種類の職務に分類し、職務ごとのタスクや知識、能力、スキルを定義(v2.1.0)
欧州(EU)	European Cybersecurity Skills Framework（ECSF）	2022年 –	ENISAが策定。EU域内での人材流動を目的に、EUの共通の枠組み 12の標準プロファイルごとのミッション、タスク、スキル、知識を定義
欧州(英国)	Cyber Career Framework	2021年 2026年	英国サイバーセキュリティ評議会(UKCSC)が策定 15の専門分野ごとに主な責任やタスク、必要なスキルや知識、キャリアパスを定義
イスラエル	Israel National Cybersecurity Strategy 2025-2028	2025年 –	INCDが策定。人材育成のフレームワークは確認できなかったが、人材育成に関しての必要性や教育/訓練に関しての記載があり
中国	GB/T 42446-2023 信息安全技术 网络安全从业人员能力基本要求	2023年 –	サイバーセキュリティ従事者の能力を定義する国家標準規格 5つのカテゴリーを定義とのことだが原本を確認できず
カナダ	The Canadian Cyber Security Skills Framework	2023年 2023年	CSEが策定。NICE Frameworkを自国内向けに簡素化 4つのカテゴリーと3つの職種(役割)に分類
インド	NSQF（National Skills Qualification Framework）	2013年 2023年	スキル開発・起業促進省が策定。サイバーセキュリティも含めた全職種の「知識」「技能」「適性」に 基づきレベルを8段階で格付け

② サイバーセキュリティ人材の育成に関する政策・規制動向｜セキュリティ・クリアランス

- 重要な機密を取り扱う個人に対するセキュリティ・クリアランスが重要視されており、各国・地域ともに制度化が進んでいる。一方で、対象範囲が各国や組織ごとに異なるため、連携強化のためには対象範囲の統一が重要となっている。
- 人的適格性評価の段階数は、日本は1段階に過ぎないがそれ以外の国や組織は3段階以上であり、国際連携上の課題が残る。
- インドのセキュリティクリアランス制度は確認できてないが、情報漏えいに高額な罰金を科して事後的な抑止力を強化している。



各国や組織の法令が想定するセキュリティクリアランスの対象者の概念図
()内はセキュリティクリアランスにおける人的適性評価レベルの段階数
3段階の例を*に示し、多段は分野によって基準が異なることを示している

*1 Top Secret/DV (Developed Vetting)
Secret/SC (Security Check)
Confidential/CTC (Counter-Terrorist Check)
*2 特定秘密の保護に関する法律

③ サイバーセキュリティ人材の育成に関する国際連携動向

- 各国・地域間や国際機関等でサイバーセキュリティ人材の育成の様々な国際協力が行われており、2025年に英国が国際的な人材の枠組や基準の相互認証性を高めることを目的に「サイバーセキュリティ人材に関する国際的な連合」を公表し、2026年2月現在、日本を含め6か国が参画している。
- 中国は、アフリカ諸国に対し強力なデジタル・インフラ開発を継続支援をしており、その一環としてAIやサイバーセキュリティ等の分野における人材の育成や技術革新の協力を拡大している。

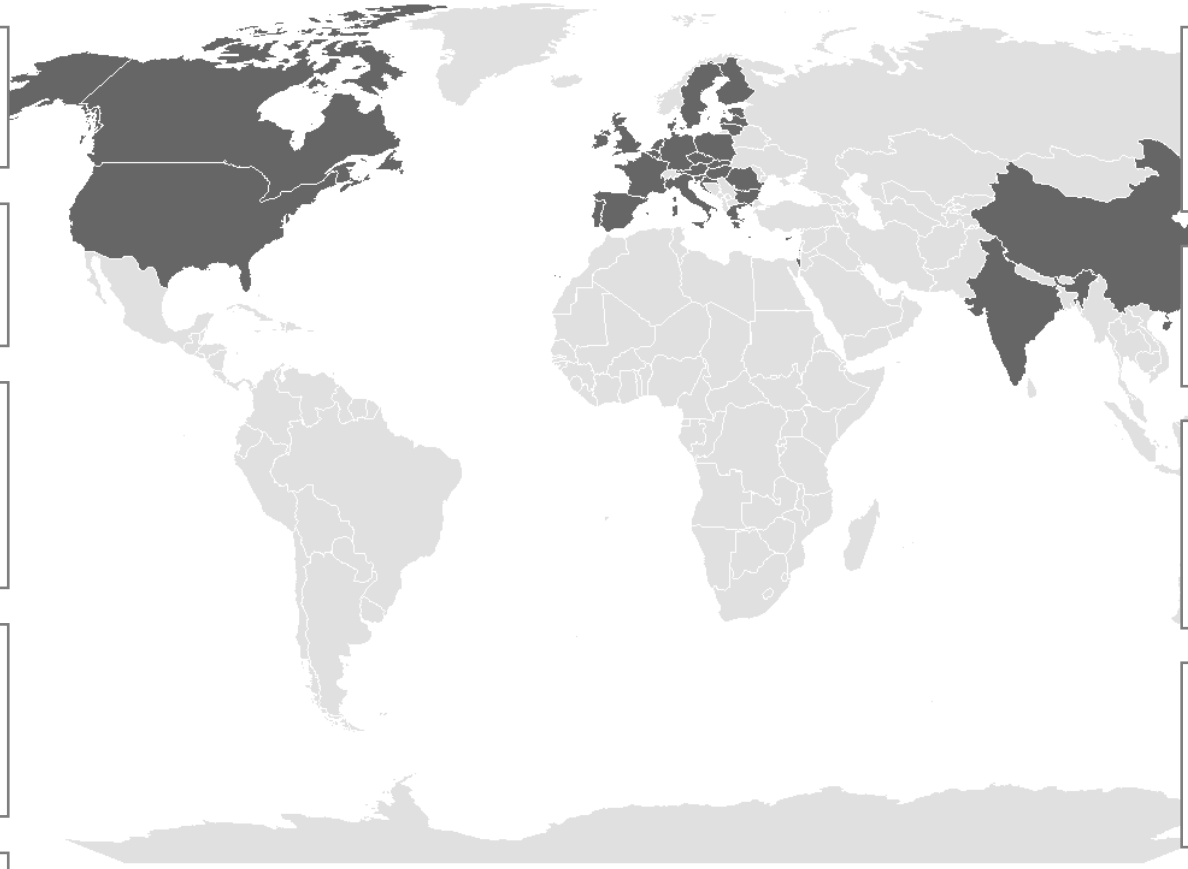
日本、欧州（英国）
「日英戦略的サイバー・パートナーシップ」の公表（2026年）

欧州（ドイツ）、イスラエル
「Security and Cybersecurity Pact」の公表（2026年）

インド、イスラエル
「MOU BETWEEN INDIA AND ISRAEL CONCERNING OPERATIONAL COLLABORATION ON CYBER SECURITY」の公表（2020年）

中国、アフリカ諸国
「Initiative on China-Africa Jointly Building a Community with a Shared Future in Cyberspace」の公表（2021年）

GFCE（Global Forum on Cyber Expertise）
ワーキンググループD「Cybersecurity Culture and Skills」の立ち上げ（2018年）



日本、欧州（英国）、カナダ、シンガポール、ガーナ、ドバイ
「サイバーセキュリティ人材に関する国際的な連合」共同声明の公表（2025年）

日本、米国、インド、オーストラリア
「日米豪印サイバーセキュリティ・パートナーシップ」共同原則の公表（2022年）

日本、ASEAN
「日ASEANサイバーセキュリティ能力構築センター（AJCCBC/ASEAN-Japan Cybersecurity Capacity Building Centre）」の設立（2018年）

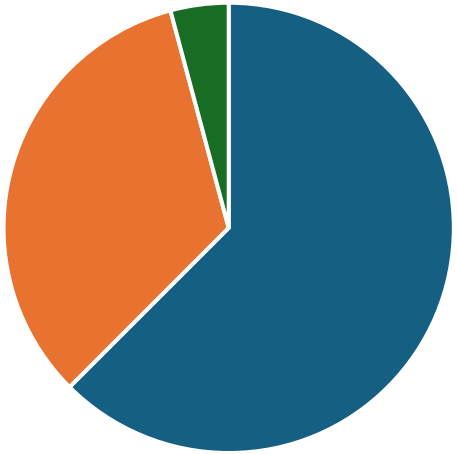
世界経済フォーラム（World Economic Forum: WEF）
「Strategic Cybersecurity Talent Framework」の公表（2024年）

④ サイバーセキュリティ人材の育成に関する研究開発動向｜統計分析

- **研究発表の件数としては、米国と欧州で9割以上を占める。**

(1) サイバーセキュリティ人材の職域・業務内容に関する研究開発

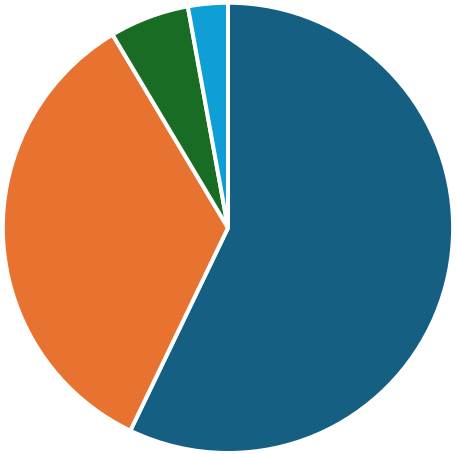
全24件



[(1)の傾向]
SOCや脅威ハンティング等の“実務”の体系化/標準化や**AI技術の進展に伴う業務内容や人材像の再定義**など実施

(2) サイバーセキュリティ人材教育に関する研究開発

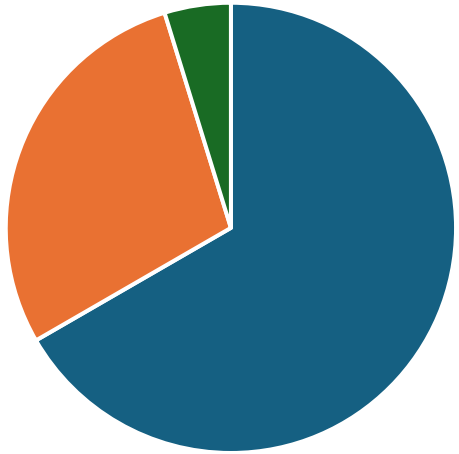
全35件



[(2)の傾向]
一般ユーザーだけでなく**専門人材(SOC等)も対象に実践的なトレーニング方法**や教育効果の定量/定性的な評価方法を研究

(3) サイバーセキュリティ人材確保に関する研究開発

全21件



[(3)の傾向]
人材不足の問題点、現状などの分析やチーム作り、技能の可視化、人材獲得戦略について研究

(1) ピックアップ発表： AI and the Cybersecurity Workforce of the Future (RSA 2025基調講演)、Todd Thibodeaux (Comp TIA) [1]

概要：AI技術の進展がサイバーセキュリティ分野に与える影響、特に人材の役割やスキル要件の変化について言及。AIの導入がセキュリティ業務の自動化を進める一方で、人間の役割をより戦略的・分析的な領域へとシフトしている。従来の定型業務から脱却し、AIを活用しながら判断力・創造力・倫理的判断を発揮できる人材が求められるようになっており、職域の再定義とスキルセットの再構築が必要と提言。

(2) ピックアップ発表： Tools Make Me Snore: A Next-Gen Framework for Training SOC Analysts Non-Perishable Skills (NDSS 2025)、Francis Hahn (USF) [2]

概要：SOC分析官の訓練手法を再設計。現役SOC従事者へのヒアリングから、サイバー防御の現場で重要なのはクリティカルシンキング(批判的思考)と技術スキルの両方だが、技術スキルはツールや攻撃手法の変化で「陳腐化しやすい」ことを特定。そこで実際のセキュリティインシデントを題材にした模擬SOCシナリオによる教育プログラムを開発し、あえて特定ツールへの依存を排除した演習とすることで、変化に左右されにくい分析・判断力の養成が可能に。

(3) ピックアップ発表： Human Performance in Security Operations: A Survey on Burnout, Well-Being and Flow State Among Practitioners (NDSS 2025)、Kashyap Thimmaraju (TU Berlin) [3]

概要：SOC従事者のバーンアウト(燃え尽き症候群)や幸福度に関する包括的調査を実施。19名のSOC担当者を対象に、コペンハーゲン・バーンアウト指数(CBI)等の心理尺度でストレス状態を定量評価し、バーンアウト率が約3割超に達すると判明。SOC要員の多くが使命感を持ちながらも深刻な疲弊リスクを抱えている状況から、負荷分散や職場環境の改善といった組織的な対策の必要性を提言。

[1]: https://www.rsaconference.com/library/presentation/usa/2025/ai%20and%20the%20cybersecurity%20workforce%20of%20the%20future
[2]: https://www.ndss-symposium.org/ndss-paper/auto-draft-545/
[3]: https://www.ndss-symposium.org/ndss-paper/auto-draft-548/

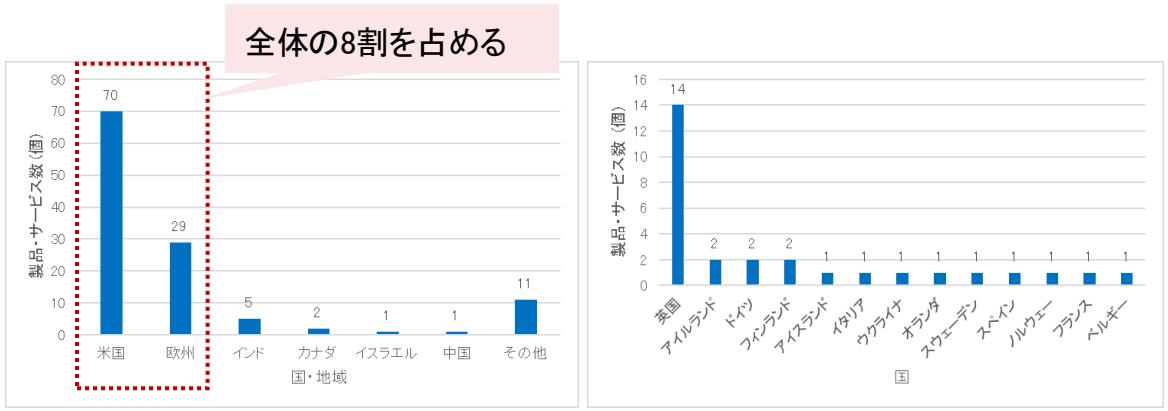
⑤ サイバーセキュリティ人材の育成に関する産業動向｜製品・サービス

- Gartner Peer InsightsのEnterprise Software Categories「Security Awareness Computer-Based Training」[1]に掲載の製品・サービス119製品*1の開発企業の国・地域*2は、米国、欧州が全体の8割を占める一方、日本は製品数が0という結果となった。
- 生成AIを悪用したサイバー攻撃を模したトレーニングや、生成AIを利用しトレーニングをカスタマイズする等、生成AIが組み込まれた製品が登場しつつある。

Security Awareness Computer-Based製品の国・地域別の数

Security Awareness Computer-Based製品

以下の1つ以上の機能を有する製品・サービス
- すぐに使えるトレーニングと教育コンテンツ
- 従業員のテストと知識チェック
- 複数言語で利用可能
  （ネイティブまたは字幕または部分的な翻訳を通じて利用可能）



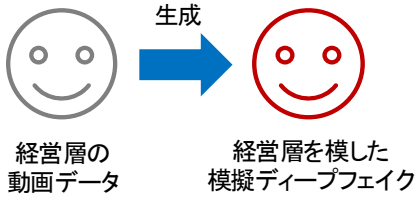
国・地域全体　　欧州

*1 2026年2月9日時点掲載の122製品から開発企業の国・地域が不明な3製品を除いた119製品を対象とする
*2 本社機能がある国・地域を開発企業の国・地域とする

生成AIの製品・サービスへの組み込み動向

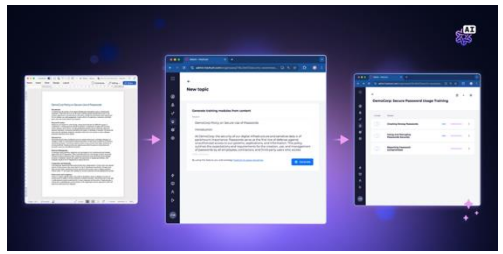
AIを悪用した攻撃に対するトレーニング: 模擬ディープフェイクビデオの作成

- 【概要】自社の経営層をデータから作成した模擬ディープフェイクビデオをトレーニングで利用
- 【製品・サービス名】KnowBe4 Security AwarenessのAIDA (AI Defense Agents) アドイン
- 【企業名】KnowBe4社
- 【国・地域】米国



生成AIのトレーニングへの活用: カスタマイズしたトレーニングの作成

- 【概要】セキュリティポリシーやガイドライン等をアップロードし、レッスンや理解度確認クイズを自動生成。組織特化したトレーニングの作成が可能
- 【製品・サービス名】Hoxhunt
- 【企業名】Hoxhunt社
- 【国・地域】欧州（フィンランド）



画像引用: Turn security policies into awareness training with GenAI Content Generation, https://hoxhunt.com/blog/turn-security-policies-into-awareness-training-with-genai-content-generation

[1]: Gartner Peer Insights Security Awareness Computer-Based Training, https://www.gartner.com/reviews/market/security-awareness-computer-based-training

⑤ サイバーセキュリティ人材の育成に関する産業動向｜国際資格

- **情報システム監査の国際資格CISAを認定しているISACAによるAI監査のAAIA、およびマネジメントのAAISMの新設、ホワイトハッカー認定の既存の国際資格CEHへのAI領域の追加など、AI×セキュリティに関する資格整備が進んでいる。これにより、産業界においてAIに関連するセキュリティ知識の習得や専門家認定の重要性が高まりつつあることがうかがえる。**

AI×セキュリティに関する新たな国際資格

AAIA (Advanced in AI Audit) (2025年) *1

AAIA ISACA Advanced in AI Audit

【概要】

世界初のAI監査に関する資格。
有効なCISA、CIA (IIA) 、またはCPA (AICPA) 認定の保有が前提となる。
出題領域は以下の3ドメイン

- ドメイン1 – AIガバナンスとリスク (AI Governance and Risk)
- ドメイン2 – AIオペレーション (AI Operations)
- ドメイン3 – AI技術とコントロール (AI Auditing Tools and Techniques)

【サイトURL】

ISACA東京支部/公認情報システム監査人 (CISA: Certified Information Systems Auditor)

AAISM (Advanced in AI Security Management) (2025年) *1

AAISM ISACA Advanced in AI Security Management

【概要】

世界初のAI-centricなセキュリティマネジメントの資格。
有効なCISM、またはCISSP (ISC2) 認定の保有が前提となる。
出題領域は以下の3ドメイン

- ドメイン1 – AIガバナンスとプログラム管理 (AI Governance and Program Management)
- ドメイン2 – AIリスクと機会の管理 (AI Risk and Opportunity Management)
- ドメイン3 – AI技術とコントロール (AI Technologies and Controls)

【サイトURL 】

ISACA東京支部/公認情報セキュリティマネージャー (CISM: Certified Information Security Manager)

AI領域が追加された既存の国際資格

CEH (Certified Ethical Hacker: 認定ホワイトハッカー) v13のリリース (2024) *2

CEH AI Elite

【概要】

ホワイトハッキングスキルの習得を目的としたCEHがv13に更新され、世界初のエシカルハッキングプログラムとなった。

＊エシカルハッキング: システムやネットワークのセキュリティを強化するために、ハッキング技術を使って脆弱性を見つけるトレーニング

AIに関する主な追加事項

- AI駆動のエシカルハッキング
- サイバーセキュリティにおけるAIと機械学習
- ディープフェイクの脅威

【サイトURL 】

CEH Certification | Certified Ethical Hacker Course | EC-Council

*1 画像引用: ISACA東京支部, https://www.isaca.gr.jp/index.html
*2 画像引用: CEH（認定ホワイトハッカー）の資格獲得コース | EC-Council公式トレーニング, https://www.gsx.co.jp/services/securitylearning/eccouncil/ceh.html

5. 生成AI時代のサイバーセキュリティについての各国・企業等の動向

調査概要

■ 調査目的

2025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」では、サイバーセキュリティに関する施策の立案および実施にあたって従うべき基本原則として「5つの原則」が示されており、その一つに「自律性」が掲げられ、様々な施策が推進されている。サイバーセキュリティ人材の不足や、関連技術を海外に依存している現状が課題となっており、国内を基盤とした人材・技術の育成を一層強化する必要がある。

また、1～4章で見てきたように、生成AIの普及や地政学リスクの変化によりサイバー攻撃は高度化・巧妙化しており、一国のみでの対応には限界があることから、国際連携の重要性は増している。

以上を踏まえ、日本のサイバーセキュリティの自律性確保に資する観点から、各国・地域および国際的な取組を整理・比較する。

■ 調査内容

#	調査項目	調査内容
①	サイバーセキュリティの自律性確保の観点から見た、日本と他国・地域等の取組の比較	1～4章の調査結果より、日本のサイバーセキュリティの自律性確保に必要な観点として、以下の2つの観点に着目し、取り上げるべき国・地域等の取組を整理し、日本と比較する • 研究開発、人材育成の観点で「人材・技術の育成」を整理 • 政策・規制、社会実装（産業化）の観点で「社会システム（社会の枠組み）」を整理

■ 調査結果

「人材・技術の育成」、「社会システム（社会の枠組み）」の観点で日本と他国・地域等の取組を比較した結果、他国・地域では、両方の観点において政府主導による戦略的取組が展開されており、日本においてもAIやサイバーセキュリティに関するルール整備や産業振興施策等の充実・強化が進められているものの、他国・地域が先行している状況にあり、国際連携の観点からも一層の強化が必要である。

サイバーセキュリティの自律性を確保するためには、国内を基盤とした人材・技術の強化が不可欠である。

そのため、「人材・技術の育成」と「社会システム」の両輪を回しつつ、ルール整備や国際連携を強化しながら産官学が一体となり取り組みを進めていくことが重要となる。

① サイバーセキュリティの自律性確保の観点から見た、日本と他国・地域等の取組の比較｜取組の現状比較

- **「人材・技術の育成」、「社会システム（社会の枠組み）」の観点で日本と他国・地域等の取組を比較した結果、他国・地域では、両方の観点において政府主導による戦略的取組が展開されており、日本においてもAIやサイバーセキュリティに関するルール整備や産業振興施策[1]等の充実・強化が進められているものの、他国・地域が先行している状況にあり、国際連携の観点からも一層の強化が必要である。**

人材・技術の育成

	他国・地域		日本
人材	米国では18歳以下を対象とした統一的なカリキュラムが提供されている	↔	中等教育以前における体系的なカリキュラムの整備が進んでいない
	イスラエルでは人材を選抜し、10～12年生の3年間で大学レベルに相当する高度な専門教育が実施されている	↔	人材を選抜し、中長期的に育成するような取組は実施されていない
	韓国や中国をはじめとする多くの国・地域で、サイバーセキュリティを専門とする学部・学科の設置が進んでおりAIとセキュリティの学科も新設されている	↔	サイバーセキュリティを学べる大学・大学院は増加しているが、学科にセキュリティが含まれる大学・大学院は二校のみであり、専門性の育成の観点で課題がある
技術	AIやセキュリティ分野のトップカンファレンスでは、米国や中国の発表が大半を占める	↔	AIやセキュリティ分野のトップカンファレンスにおける日本の発表はごくわずかとなる
	欧米の博士課程の学生は、給与、あるいは給付型の奨学金が支給されており、経済的に安定した状況で研究に従事している	↔	日本の博士課程の学生は、給与、あるいは給付型の奨学金を受給できる人はわずかで、経済的に安定した状況で研究に従事している学生は限定的である

社会システム（社会の枠組み）

他国・地域		日本
グローバルなセキュリティ製品・サービスの開発企業は、米国、イスラエル、欧州に集中している。新たな製品・サービスを創出する人材を適切な処遇で受け入れ、成長を後押しする産業的な受け皿が形成されていると考えられる	↔	グローバルなセキュリティ製品・サービスの開発企業は、ごくわずかである。産業的な受け皿としての新たな製品・サービスを創出する人材を受け入れるポジションや適切な処遇の確保が不十分と考えられる
各国・地域においてセキュリティ・クリアランス制度の整備が進んでおり、欧米では人的適格性評価を複数の段階数で実施されている	↔	2025年に「重要経済安保情報保護法」が施行され、セキュリティ・クリアランス制度の本格運用に向けた準備が進められている
英国では、国際標準化を見据えたAIサイバーセキュリティの原則が策定されており、AIセキュリティに関する国際標準への積極的な関与が見られる	↔	AIセキュリティに関する国際標準を見据えた法令やガイドラインの策定は見受けられないが、AISIやGPAI等で積極的なルールメイキングを推進している
AIのセキュリティ活用やAIモデルの安全性確保に関する団体・規格がでグローバルで設立される中、米国企業等が主導的な役割を果たしている	↔	日本企業が主導してルール形成や標準化を推進している事例は限定的である

[1]: 経済産業省 サイバーセキュリティ産業振興戦略, https://www.meti.go.jp/press/2024/03/20250305001/20250305001-2.pdf

① サイバーセキュリティの自律性確保の観点から見た、日本と他国・地域等の取組の比較｜必要な取組

- **サイバーセキュリティの自律性を確保するためには、国内を基盤とした人材・技術の強化が不可欠である。**
  そのため、「人材・技術の育成」と「社会システム」の両輪を回しつつ、ルール整備や国際連携を強化しながら産官学が一体となり取り組みを進めていくことが重要となる。

人材・技術の育成

＜国際競争力を持つ人材の育成＞

- 中等教育以前の体系的なカリキュラムの整備や選抜人材への高度な専門教育の実施
- AI×サイバーセキュリティのスキルを有する人材の育成
- 研究・製品開発等において国際競争力を発揮し得るイノベーター人材の育成

＜製品化の種となるような新たな技術の育成＞

- 産学官連携や国際連携による共同研究プロジェクトの強化
- 社会実装を視野に入れた中長期的な研究プロジェクトの推進
- 研究開発支援に係る助成制度の拡充

サイバーセキュリティの自律性確保

社会システム（社会の枠組み）

＜人材の受け皿・情報取扱者の信頼性確保＞

- 博士号取得者等のイノベーター人材を含む多様なセキュリティ人材の受け皿を、適切な処遇の下で確保
- セキュリティ・クリアランス制度の適切な運用による各国・地域との円滑なサイバー情報の共有の促進

＜国産の製品・サービスの市場拡大＞

- 政府機関による国産製品・サービスの積極的な調達等による国内市場の安定確保
- 国際市場への展開を見据えた、業界規格等に準拠した競争力のある製品・サービスの創出

＜AIの安全な利用のための国際協調＞

- 国際標準を見据えた国内法令やガイドラインの策定を推進し、日本がグローバルなルール形成や標準化において主体的な関与の実施

6. 今後の展望

6. 今後の展望
① 1～5章の調査結果まとめ

1～5章の調査結果まとめを示す。

生成AIによるサイバーセキュリティの攻撃対策手法の進化	• 2023年以降に大幅に論文数が増加しており、第一著者の所属機関の国・地域は米国と中国で約8割を占める • 生成AIを活用したセキュリティ製品が登場しつつあるが、社会実装はまだ初期段階にある • 各国・地域では、サイバーセキュリティ分野におけるAIの活用を促進する一方で、その悪用に対する規制や対策の強化が進められている
生成AIモデルのセキュリティ確保に関する動向	• 2023年以降に大幅に論文数が増加しており、第一著者の所属機関の国・地域は米国と中国で約7割を占める • 米国やイスラエルを中心にLLMガードレール等の新たな製品・サービスが登場している • 各国・地域でルール整備が急速に進んでいる。また、GPAIや各国・地域のAISI等を通じた国際連携も活発化しており、AIのセキュリティ確保に向けた共通枠組みの形成が進展している
アクティブ・サイバー・ディフェンスに関する動向	• 各国・地域で「事前防御・堅牢化・監査」「情報共有や即時通報」「インテリジェンス収集」「無害化措置」の対応が整備されており、各国・地域に共通する実装上の課題として、通信傍受の透明性確保や人材の育成等が挙げられる • QuadやUKUSA協定といった多国間連携の枠組みは存在するが、各国・地域間での認識の違いや情報共有の枠組み整備が、多国間で連携を深化させる上での課題となっている • 主要な学会*では、第一著者の所属機関の国・地域が米国、中国、欧州である論文が約9割を占め、特にインテリジェンス分析に関する研究発表が多い傾向が見られる
サイバーセキュリティ人材の育成に関する動向	• 人材不足を背景に、各国・地域で人材育成・確保を強化する取組や、国際連携を推進する動きが見られる • セキュリティ・クリアランスが国際的に重要視されており、各国・地域ともに制度化が進んでいる • AIの普及に伴う職域の再定義やスキルセットの再構築の必要性を指摘する論文発表もあり、また、AI×サイバーセキュリティの国際資格も登場しており、AIの知識を有するセキュリティ人材の重要性の高まりが見られる
生成AI時代のサイバーセキュリティについての各国・企業等の動向	• 「人材・技術の育成」、「社会システム（社会の枠組み）」の観点で日本と他国・地域等の取組を比較した結果、他国・地域では、両方の観点において政府主導による戦略的取組が展開されており、日本においても法令整備や産業振興施策等の充実・強化が進められているものの、他国・地域が先行している状況となる • サイバーセキュリティの自律性を確保するためには、国内を基盤とした人材・技術の強化が不可欠である。そのため、「人材・技術の育成」と「社会システム」の両輪を回しつつ、ルール整備や国際連携を強化しながら産官学が一体となり取り組みを進めていくことが重要となる

② 生成AI時代に求められる研究開発・政策・規制・人材育成における今後の変化

1、2、4章における研究開発・産業、政策・規制・国際連携、人材育成に関しての調査結果より、現在の状況と生成AI時代に求められる今後の展望を以下のとおり整理した。

	現在	今後
研究開発・産業	• 生成AIを利用および悪用したセキュリティ技術や生成AIモデルのセキュリティ確保に関する様々な技術の研究開発が加速度的に進められている • 一方で実用的なAIを利用したセキュリティ製品はまだ導入段階であり、リスクも残っている	• 目標設定から計画、実行までを人間の介在を最小限に抑えて自律的に行うエージェントAIの開発など、新たなAI技術等を悪用したサイバー攻撃への対策が一層重要となる • 防御側においてもAIを積極的に活用し、防御基盤の高度化・強化を図ることが不可欠である
政策・規制・国際連携	• AIおよびサイバーセキュリティに関する法整備や連携の枠組みが世界的に急速に進展している • AIの安全性に関しての国際連携の枠組みが整備されているが、統一的な枠組みには至っていない	• 今後、AIが社会インフラとしての位置付けを一層強めることが予想される • AIの活用促進とリスク管理のバランスを図りつつ、国際協調の下で、安心してAIを利用できる共通的なルール形成を進めていくことが重要である
人材育成	• 人材不足を背景に、各国・地域で人材育成の強化を図っており、AIの普及によりセキュリティ業務の効率化が進んでいる • 重要機密を取り扱う個人に対するセキュリティ・クリアランスが国際的に重要視され、各国・地域で制度化が進められている	• AIとサイバーセキュリティの双方に精通した専門人材の需要が急速に拡大すると見込まれ、AIの活用を前提とし、今後は想像力や判断力を発揮できる人材が求められる • サイバー対処を国際協力しながら実施するにあたって、国家間のセキュリティクリアランスの相互認証の重要性が増すと考えられる

③ サイバーセキュリティの自律性確保へ向けた産学官の取組の方向性

今後、ICTインフラやIoT機器の増加、新たなAI技術の登場等により、サイバー攻撃の高度化・巧妙化が進むことが想定される。これに伴い、サイバーセキュリティの重要性は一層高まり、市場規模の拡大が見込まれている。

こうした状況を踏まえ、国産製品・サービスを核とした持続的な産官学のエコシステムを構築し、AIの進展を踏まえてこれを発展させていくことで、サイバーセキュリティ自給率の向上、さらにはサイバーセキュリティの自律性確保を図ることが重要である。その実現に向けた産学官の取組の方向性を整理した。

人材・技術の育成

産
- AI を核とする新たなセキュリティ製品・サービスの源泉となる研究開発の推進

学
- グローバルなAI×サイバーセキュリティ人材・技術の輩出

官
- AI×サイバーセキュリティ人材育成の教育や支援の強化
- 研究開発における助成制度の拡充や産学官連携の強化

サイバーセキュリティの自律性確保

社会システム（社会の枠組み）

産
- イノベーター人材を含む多様なセキュリティ人材の受け皿の確保
- 国産製品・サービスの販路拡大
- AI、セキュリティの業界団体・規格におけるルール形成の先導

学
- 製品・サービスの技術中立的な評価
- 実証実験等の社会実装を見据えた産学官連携の推進

官
- 国産製品・サービスの積極的な調達
- スタートアップ等の新たな製品・サービスを生み出す企業の周知・支援
- セキュリティ・クリアランス制度の運用
- AI等の活用や国際連携によるサイバー対処能力の強化、国際的なルール形成の主導

参考文献

参考文献

■ 研究開発動向調査で参照

[A] ACM CCS (ACM Conference on Computer and Communications Security) https://www.sigsac.org/ccs.html

[B] IEEE Security & Privacy (IEEE Symposium on Security and Privacy) https://www.ieee-security.org/TC/SP-Index.html

[C] NDSS (Network and Distributed System Security) https://www.ndss-symposium.org/

[D] USENIX Security https://www.usenix.org/

[E] RSA Conference https://www.rsaconference.com/

[F] BlackHat https://blackhat.com/

[G] DEF CON https://defcon.org/

[H] AAAI (The Association for the Advancement of Artificial Intelligence) https://aaai.org/

[I] ICLR (Internation Conference on Learning Representations) https://iclr.cc/

[J] ICML (Internation Conference on Machine Learning) https://icml.cc/

[K] NeurIPS (Conference on Neural Information Processing Systems) https://nips.cc/

[L] IJCAI (International Join Conference on Artificial Intelligence) https://www.ijcai.org

[M] USENIX WOOT (The Workshop on Offensive Technologies) https://www.usenix.org/conferences

■ 産業動向調査で参照

[N] Gartner Peer Insights https://www.gartner.com/peer-insights/home