

AIセキュリティ分科会について

令和7年9月

AIセキュリティ分科会事務局

背景・目的

- 生成AIの社会実装が急速に進む中、AIのセキュリティ確保が重要な課題となっており、「デジタル社会の実現に向けた重点計画」（令和7年6月13日閣議決定）では、総務省が、今年度末までに、生成AIとセキュリティのガイドラインを策定・公表することとされている。
- また、AIの安全安心な活用促進については、「AI事業者ガイドライン」（総務省・経済産業省）において「セキュリティ確保」が共通指針の一つに位置付けられ、これを踏まえ、関係省庁・関係機関により構成される「AIセーフティインスティテュート(AISI)」※が、AIに対する脅威の特定等を行っている。
- 本分科会は、このような状況を踏まえ、「サイバーセキュリティタスクフォース」の下に開催される会合として、AIに対する脅威への技術的対策について検討を行う。

※ AIの安全安心な活用が促進されるよう 官民の取組を支援する機関。統合イノベーション戦略2024に基づきIPAに設置。

主な検討事項

- AI開発者及び提供者における、AIに対する脅威への技術的対策の在り方
- 上記対策の普及啓発の在り方

構成員（敬称略・50音順）

秋山 満昭	NTT株式会社 社会情報研究所 上席特別研究員	高橋 健志	国立研究開発法人情報通信研究機構（NICT）
新井 悠	株式会社NTTデータグループ 技術革新統括本部		サイバーセキュリティ研究所
	品質保証部情報セキュリティ推進室		AIセキュリティ研究センター 研究センター長
	NTTデータCERT担当	披田野 清良	株式会社KDDI総合研究所 セキュリティ部門 エキスパート
	エグゼクティブ・セキュリティ・アナリスト	福田 昌昭	株式会社Preferred Networks VPoE 兼 技術企画本部長
石川 朝久	東京海上ホールディングス株式会社	北條 孝佳	西村あさひ法律事務所・外国法共同事業
	IT企画部サイバーセキュリティグループ		パートナー弁護士
	Distinguished Cyber Security Architect	森 達哉	早稲田大学 理工学術院 教授（主査）
篠田 佳奈	株式会社BLUE 代表取締役	綿岡 晃輝	SB Intuitions 株式会社 R&D本部 Data&Safety 部
オブザーバ：国家サイバー統括室、内閣府、デジタル庁、文部科学省、経済産業省、AISI			Responsible AI チームチームリーダー/Chief Research Engineer

スケジュール

- 令和7年9月 第1回分科会（以降、月1回程度の開催を想定）
- 令和7年12月頃 分科会とりまとめ
- 令和7年度内 総務省ガイドラインの公表

「デジタル社会の実現に向けた重点計画」(令和7年6月13日 閣議決定)

本文 4. 取組の方向性と重点的な取組

(4) 安全・安心なデジタル社会の形成に向けた取組

⑤ サイバーセキュリティの確保

・AI を積極的に活用したセキュリティ対策(AI for Security)を推進するとともに、セキュリティ分野における AI の安全な利用(Security for AI)に向けた環境整備の取組などを進めていく。

重点政策一覧 4. 取組の方向性と重点的な取組

○[No.4-25] 生成 AI 等を活用したサイバーセキュリティ対策強化

具体的な目標: 【「Security for AI」の取組】

・2025年度末までに、生成AIとセキュリティのガイドラインの策定・公表を 実施。2026年度には、2025年度に公表したガイドラインの更新等を実施。
主担当府省庁: 総務省 関係府省庁: ー

「サイバーセキュリティ2025」(令和7年6月27日 サイバーセキュリティ戦略本部決定)

第4部 2024年度のサイバーセキュリティ関連施策の取組実績、評価及び今年度の取組

4 横断的施策

4.1 研究開発の推進

(3) 中長期的な技術トレンドを視野に入れた対応

<2025年度年次計画>

・生成AI等の技術は日に日に進歩を続けており、生成AI等を悪用したサイバー攻撃が国内外で発生している。そのため、令和6年度に調査・分析を行ったAIを悪用したサイバー攻撃の脅威への対策等の、開発者・提供者が留意すべきセキュリティリスクを取りまとめ、AIの安心・安全な開発・提供に向けたセキュリティガイドラインを策定する。

・引き続き、総務省において、生成AIをはじめとするAI技術がサイバーセキュリティに与える影響について、正の側面と負の側面の双方から、調査を実施し、必要な対策について検討を進める。

— AISIの関係府省庁・機関

AISIは、12府省庁・5関係機関が横断的に参画する**政府関係機関**
事務局は経済産業省とデジタル庁を所管官庁としている**IPA内に設置**

* 2025年4月時点

