資料１－１

「AIセキュリティ分科会」開催要綱

１　目的

生成AIを始めとするAI技術は加速度的に発展しており、あらゆる領域で社会実装が急速に進んでいる。

このような中、AIの安全安心な活用促進のために「AI事業者ガイドライン」が策定され、各主体が連携して取り組むべき共通の指針の一つとして「セキュリティ確保」が位置付けられている。また、AIの安全性に対する国際的な関心の高まりを踏まえ、我が国においても関係省庁・関係機関から構成される「AIセーフティ・インスティテュート（AISI）」が設立され、AIに対する脅威の特定等が行われてきている。

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ことを目的とする。

２　名称

本会合は、「AIセキュリティ分科会」と称する。

３　検討事項

（１）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
（２）上記の対策の普及啓発の在り方

４　構成及び運営

（１）本分科会の主査は、サイバーセキュリティタスクフォースの座長が指名する。
（２）本分科会の構成員は、別添のとおりとする。
（３）主査は、本分科会を招集し、主宰する。
（４）主査は、必要があると認めるときは、主査代理を指名することができる。
（５）主査代理は、主査を補佐し、主査不在のときは主査に代わって本分科会を招集し、主宰する。
（６）本分科会の構成員は、やむを得ない事情により出席できない場合において、代理の者を指名し、出席させることができる。
（７）主査は、必要と認める者をオブザーバとして招聘することができる。
（８）主査は、必要があると認めるときは、外部の関係者の出席を求め、意見を聴くことができる。
（９）その他、本分科会の運営に必要な事項は、主査が定めるところによる。

５　議事・資料等の扱い

（１）本分科会は、原則として公開とする。ただし、主査が必要と認める場合は非公開とする。
（２）本分科会で使用した資料については、原則として、総務省のウェブサイトに掲載し、

公開する。ただし、公開することにより、当事者若しくは第三者の利益を害するおそれがある場合又は主査が必要と認める場合は非公開とする。

（３）本分科会の議事要旨は、原則として公開とする。ただし、主査が必要と認める場合は非公開とする。

６　スケジュール

本分科会は、令和７年９月から開催する。

７　その他

本分科会の事務局は、総務省サイバーセキュリティ統括官室が行う。

別添

「AIセキュリティ分科会」
構成員名簿

（敬称略、五十音順）

秋山　満昭　NTT株式会社　社会情報研究所　上席特別研究員

新井　悠　株式会社NTTデータグループ　技術革新統括本部
品質保証部情報セキュリティ推進室　NTTデータCERT担当
エグゼクティブ・セキュリティ・アナリスト

石川　朝久　東京海上ホールディングスIT企画部　サイバーセキュリティグループ
Distinguished Cyber Security Architect

篠田　佳奈　株式会社BLUE　代表取締役

高橋　健志　国立研究開発法人情報通信研究機構（NICT）サイバーセキュリティ研究所
AIセキュリティ研究センター　研究センター長

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

福田　昌昭　株式会社Preferred Networks　VPoE 兼 技術企画本部長

北條　孝佳　西村あさひ法律事務所・外国法共同事業　パートナー弁護士

森　達哉　早稲田大学　理工学術院　教授

綿岡　晃輝　SB Intuitions 株式会社 R&D本部 Data&Safety 部
Responsible AI チームチームリーダー/Chief Research Engineer