別紙様式

意見書

令和8年1月29日

意見提出者

所属（会社名・団体名等）（※１）	一般社団法人新経済連盟
氏名（※２）	代表理事　三木谷 浩史
住所（※２）	〒105-0001　東京都港区虎ノ門1-2-8 虎ノ門琴平タワー5階
連絡先	連絡担当者氏名：大室　陽 電話：050-5835-0770 e-mail：yoh.ohmuro@jane.or.jp

※１ 個人の場合は「個人」と御記入ください。
※２ 法人又は団体の場合は、名称、代表者の氏名及び主たる事務所の所在地を御記入ください。

意見提出フォーマット

「AIのセキュリティ確保に向けた技術的対策に係るガイドライン」本編（案）					
頁	章	項目	図	該当箇所	御意見
1				1. 本ガイドラインの策定の背景等	背景にも記載はされているが、生成AI等の技術発展は著しく、本ガイドラインの内容も定期的なアップデートが必要であると考える。各事業者にとって有益となるような対策や事例等の収集など、引き続き、産業界との連携を密にされることを要望する。
1				1. 本ガイドラインの策定の背景等	広告制作では画像生成AIが既に実用段階にあり、意図しない著作権侵害や不適切画像の生成対策が急務である。また、MCPについてもAIエージェントの実用化にあたり活用を検討している。新たなテクノロジーに対応したセキュリティ指針も可能な限り早期に提示していただきたい（現在の記載では後回しにするように受け取れる）。
7	2	2.1		「これらの攻撃は基本的にプロンプトの入力により実施可能であるため、攻撃の具体的な可能性が比較的高いと考えられる。」	AI システムに特有の攻撃手法が様々存在するなかで、本ガイドライン案では「プロンプトインジェクション攻撃」及び「DoS攻撃」への対策が示されている点について、選択論拠がより明確に示されるとよいのではないか。 なお、AISI, 2025年 3 月「AIシステムに対する既知の攻撃と影響」(https://aisi.go.jp/assets/pdf/Known_Attacks_and_Their_Impacts_on_AI_Systems_JP.pdf)も同様にAIシステムに特有の攻撃と影響を俯瞰し、対策を検討するための参考情報を提供することを目的とした文書であるが、AI システムに特有の攻撃手法が網羅されている。
11	2	2.2		「・細工をしたモデルの導入を通じた攻撃」	AISI にて示されている攻撃手法名との用語の揺れがある （モデルポイゾニング攻撃 (AISI) / 細工をしたモデルの導入を通じた攻撃（本文書））ことから 、用語を統一する、もしくは、異なる意図の攻撃を想定されている場合はマッピングをとるなどの検討をしていただきたい。既存のAI 関連のガイドラインと整合性がとれた文書とすることで、読み手の理解が促進されると考える。
13	3	3.2		注釈10「AI が学習するデータの信頼性の確認は、開発・提供するシステムの目的・用途に応じて重要となる場合があるものである。」	AI学習データの信頼性確認は、AIシステムが社会に与える影響の増大を鑑み、不可欠な要件である。「データポイズニング攻撃」や「細工をしたモデルの導入を通じた攻撃」といったリスクは、AIシステムの公開・非公開にかかわらず発生し、その影響は甚大である。例えば、社会インフラとしての重要性が高いモバイルネットワークサービスの運用・開発において内部利用するLLMでは、データの信頼性が損なわれた際の影響が極めて大きく、この原則の重要性が特に顕著に現れる一例である。 したがって、「重要となる場合があるものである。」という部分は「不可欠な要素である。」と修正するなどにより、AIシステムに関わる全ての主体に対し、学習データの信頼性確保の重要性を明確に喚起すべきである。さらに、量子コンピュータによる暗号解読（PQC）や量子鍵配送（QKD）技術の進展に伴う新たなセキュリティ対策についても、言及いただきたい。
15	3	3.4		3.4 AI 提供者における対策 - ガードレール等による入出力や外部参照データの検証	セキュリティ優先のガードレールにより、広告特有の比喩や多様な表現が一律にブロックされることを懸念する。画一的な制限ではなく、用途に応じて強度や検証項目を柔軟に設定できる運用の実現を要望する。以前ハラスメント検出ツールの検証を行ったところ、事業者自身が取り扱っているコンテンツに関連した正規のやり取りが全てハラスメントとして誤検知されたことがあった。一律なブロックにはこのような懸念があると考えられる。

16	3	3.5		3.5 AI 開発者・提供者に係るその他の基本	セキュリティ確保のためのログ全量保存は、従業員の思考プロセスや未公開アイディア、機微な相談内容を扱う際のプライバシー侵害や監視感に繋がる懸念がある。追跡可能性の確保と利用者の利便性・プライバシー保護のバランスについて、運用上の留意点を追記すべき。ログ保存が利用の阻害要因にならない為の配慮が必要である。
17	3	3.6		3.6 AI サービスの想定事例に応じた分析 - 想定事例１：内部向けチャットボット（RAG 利用	例えば、複数クライアントの機密情報を扱う広告会社では、プロンプトインジェクション等による情報漏洩の防止が重要である。RAG等のデータストア管理において、論理的分離（タグ付け等）で十分か、物理的分離が必要か等、情報の機密性に応じた技術的対策の指針を追記すべき。具体的な分離レベルが明確になれば、安心して導入・運用が可能になる。
その他					対策の対象である「攻撃」について、大まかには①AIのシステム自体に対する攻撃、②AIを使った他のシステムに対する攻撃に大別できると考える。これら2つを分けて議論すべきではないか。特に②については、それを対策することによる弊害も予想されるので対策は慎重に考えるべき。

「AIのセキュリティ確保のための技術的対策に係るガイドライン」別添（付属資料）（案）					
頁	章	項目	図	該当箇所	御意見

※郵送の場合、 用紙の大きさは、日本産業規格Ａ列４番としてください。
※意見フォーマットの行を追加する場合は、行番号を右クリックの上、挿入をクリックしてください。
※全体に対する御意見等がございましたら、頁欄で「その他」を選択の上、「御意見」部分に記載してください。