

令和8年3月27日

「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」 (案) に対する意見募集の結果及びガイドラインの公表

総務省は、「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」(案)について、令和7年12月26日(金)から令和8年1月29日(木)までの間、意見募集を実施し、同意見募集の結果を踏まえて、「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」を策定しましたので、公表します。

1 概要

総務省では、令和7年9月からサイバーセキュリティタスクフォースの下でAIセキュリティ分科会を開催し、AIに不正な出力を行わせたり、AIを搭載するシステムの停止を生じさせたりするといったAIへの脅威に対して、AIのセキュリティを確保するための技術的対策の検討を行ってきました。同分科会の検討結果を踏まえて作成した「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」(案)について、令和7年12月26日(金)から令和8年1月29日(木)までの間、意見募集を行ったところ、52件の意見の提出がありました。

今般、提出された意見を踏まえ、「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」を策定しましたので、提出された意見及びその意見に対する総務省の考え方と併せて公表します。

2 提出された意見

「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」(案)の意見公募に提出された意見及びその意見に対する総務省の考え方は、[別紙1](#)のとおりです。

3 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

「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」本編は[別紙2](#)、「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)」は[別紙3](#)のとおりです。

4 資料の入手方法

[別紙1](#)、[別紙2](#)及び[別紙3](#)の資料については、e-Gov (<https://www.e-gov.go.jp>)の「パブリック・コメント」欄に掲載します。

【関係報道資料等】

- ・「AI セキュリティ分科会」の開催（令和7年9月10日公表）
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00249.html
- ・「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」（案）に対する意見募集（令和7年12月25日公表）
https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00337.html

【連絡先】

総務省 サイバーセキュリティ統括官室

担 当 ： 中村参事官補佐、中川主査、河村官

電 話 ： 03-5253-5749（直通）

メー ル ： security-AI<@>soumu.go.jp

※迷惑メール防止のため、@を「<@>」と表示しています。

メールをお送りになる際には、「<@>」を@に直してください。