別　紙

国水水第50号
令和8年5月25日

各都道府県知事　殿

各国土交通大臣認可 {水道事業者／水道用水供給事業者} 殿

（各地方整備局等経由）

国土交通省大臣官房上下水道審議官
（公印省略）

AI性能の高度化を踏まえた
サイバーセキュリティ対策の強化について（通知）

AI技術は急速に進展・普及しており、サイバー攻撃にAIが悪用されることで、攻撃のスピード・規模が劇的に増加するなど、我が国の重要インフラ事業においても、サイバーセキュリティにおける脅威に直面している。特に、本年４月７日に米国Anthropic社が公表した「Claude Mythos Preview」を始めとするフロンティアAIモデルによる、脆弱性の発見・修正等のサイバーセキュリティ性能の急速な向上に備えた対応が必要不可欠である。

サイバーセキュリティ性能のより高いAIは、サイバーセキュリティ対策の向上に資する一方、攻撃者により悪用される懸念もあり、早急な対応が必要である。こうした状況を踏まえ、５月18日に内閣官房国家サイバー統括室を始めとする関係府省等において「AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について（重要インフラ事業者等に対する注意喚起）」（別紙１）を取りまとめたところである。

ついては、国土交通大臣認可の水道事業者及び水道用水供給事業者においては、引き続き水道法に基づくサイバーセキュリティ対策に係る水道施設の技術的基準の遵守を徹底の上、別紙１を踏まえ、下記のとおり経営層のリーダーシップの下、高性能AIの悪用リスクに備えたサイバーセキュリティ対策の実施や、より高速かつ大量に脆弱性が発見・修正されることを前提とした対策強化をお願いする。

また、都道府県においては、貴管内の都道府県知事認可の水道事業者及び水道用水供給事業者に対してこの旨周知をお願いする。

記

【対策内容】
１．経営層のリーダーシップの下でのサイバーセキュリティ対策
２．基本的なサイバーセキュリティ対策の確実な実施及び更なる対策の強化
３．高性能AIにより高速化する脆弱性の発見・修正等への対応

※これらの対策内容については、別紙１の記載内容に加え、別紙２の補足説明を参考のこと。