事　務　連　絡
令和８年５月 25 日

各{都道府県／市／特別区}水道行政担当課長　殿
国設置専用水道の設置者　殿
（各地方整備局等水道担当経由）

国土交通省水管理・国土保全局
水道事業課企画専門官

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

水道行政の推進につきましては、日頃から格別のご協力をいただき御礼申し上げます。

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、水道事業においても、サイバーセキュリティにおける脅威に直面しています。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す。

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す。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に関する関係省庁会議を開催し、サイバーセキュリティ対策の強化を図っているところです。

つきましては、都道府県、市及び特別区においては、貴管内の専用水道の設置者（国設置専用水道の設置者を除く。）に対して、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いただくよう周知をお願いいたします。

また、国設置専用水道の設置者においては、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いただくようお願いいたします。

なお、各都道府県知事、各国土交通大臣認可水道事業者及び水道用水供給事業者宛には「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）」（令和８年５月 25 日付け国水水第 50 号国土交通省大臣官房上下水道審議官通知）により別紙のとおり通知されているのでお知らせします。

【連絡先】
国土交通省水管理・国土保全局水道事業課
水道計画指導室　池本、下平
E-MAIL　hqt-suidoucyber@ki.mlit.go.jp
TEL　03-5253-8111(内線 34432、34436)

別紙１

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）

2026 年 5 月 18 日

内閣官房国家サイバー統括室、内閣府政策統括官（経済安全保障担当）
警察庁、金融庁、総務省、厚生労働省、経済産業省、国土交通省、防衛省

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等、サイバーセキュリティにおける脅威に直面しています。

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す。

サイバーセキュリティ性能のより高い AI（高性能 AI）は、ベンダ等における脆弱性の発見・修正等や重要インフラ事業者等[1]における検知・対応等のサイバーセキュリティ対策に活用することにより、我が国のサイバー対処能力の更なる強化が期待できます。特に脆弱性に関しては、高性能 AI により、脆弱性の発見・修正等が高速化することが考えられます。一方で、高性能 AI が攻撃者に悪用されることにより、サイバー攻撃がより高速かつ大規模に行われるおそれがあるため、悪用リスクを前提として、高性能 AI を積極的にサイバー防御に活用していくことも含め、対策強化を早急に進めていくことが必要です。

このため、重要インフラ事業者等においては、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します。

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

サイバーセキュリティ対策は、企業活動におけるコストや損失を減らすために必要な投資（将来の事業活動・成長に必須な費用）と位置付けることが重要です。特に重要インフラ・サービスの機能停止が経済社会にもたらす影響の大きさは言うまでもありません。「サイバーセキュリティ経営ガイドライン」[2]（経済産業省・IPA[3]）も参照し、組織のリスクマネジメントの責任を担う経営層のリーダーシップの下で、リスク対策の実施方針の検討、予算や人

---

[1] 本文書では、「重要インフラのサイバーセキュリティに係る行動計画」に基づく重要インフラ事業者等（重要インフラ事業者及びその組織する団体並びに地方公共団体）、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 43 号）第 50 条第 1 項に規定する特定社会基盤事業者及び防衛産業の事業者をいいます。

[2] 経済産業省　サイバーセキュリティ経営ガイドラインと支援ツール
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

[3] 独立行政法人情報処理推進機構

材の確保・割当、実施状況の確認や問題の把握・対応等のサイバーセキュリティ対策の実施をお願いします。

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

英国 AISI による Claude Mythos Preview に関する評価[4]においても、セキュリティアップデートの定期的な適用、堅牢なアクセス制御、構成管理及び包括的なログ監視といったサイバーセキュリティの基本の重要性を改めて示されております。また、米国 CISA による重要インフラのレジリエンス強化のためのガイダンス[5]においても、外部ネットワークとの接続を能動的に遮断し通信が制限された状態でも重要インフラ・サービスの提供を継続する運用の確保（隔離）や隔離状態のまま侵害された重要システムを迅速に復旧させるための計画や手順の策定、訓練等（復旧）の重要性が示されております。

今後策定される「重要インフラのサイバーセキュリティ対策のための統一基準」（重要インフラ統一基準）[6]や各分野の安全基準等も参照しつつ、資産管理、リスクアセスメント、脆弱性管理、アカウント管理・認証・アクセス制御、バックアップの確保、監視・分析、事業継続計画の策定、インシデントへの対応及び復旧、組織の壁を越えたサプライチェーン・リスクへの対応等、基本的な対策の確実な実施をお願いします。これらの実施状況については、実効的な対策を継続的に行うべく、今後、関係省庁・関係機関を通じて機動的に確認しますのでご協力をお願いします。

加えて、更なるサイバーセキュリティ対策水準の向上のため、内部・外部を問わず全てのアクセスを信頼せず継続的に検証する「ゼロトラスト」の考え方に基づくシステム設計・運用への移行、侵害を前提として組織内の不審な活動や攻撃痕跡等を能動的に検知・分析する取組（脅威ハンティング等）の強化、高性能 AI を活用したサイバーセキュリティ対策の強化[7]（例：脅威検知・インシデント対応・脆弱性発見等）等、更なる取組の検討・実施を推奨します。また、各分野におけるセキュリティ対策を実践する人材の育成の観点から、NICT[8]による実践的サイバー防御演習「CYDER」[9]や、IPA 産業サイバーセキュリティセンターに

---

[4] 英国 AISI　Our evaluation of Claude Mythos Preview's cyber capabilities
https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities

[5] 米国 CISA　CI Fortify: Strengthening Resilience Across Critical Infrastructure
https://www.cisa.gov/topics/industrial-control-systems/ci-fortify

[6] 2026 年 4 月「重要インフラ統一基準（案）」に関する意見の募集について
https://www.cyber.go.jp/policy/group/infra/report.html

[7] 高性能 AI の活用にあたっては、情報漏えいや意図しない学習への流用等のリスクを適切に管理する必要があることに留意。

[8] 国立研究開発法人情報通信研究機構

[9] NICT 実践的サイバー防御演習「CYDER」　https://cyder.nict.go.jp/

よる「中核人材育成プログラム」[10]等の活用も検討ください。

また、国家サイバー統括室は、インシデント情報等のサイバーセキュリティ関連情報を分野横断的に集約・分析し、被害防止に向け、必要とする主体に適切な形での情報提供に取り組みます。そのため、重要インフラ事業者等においては、インシデントやその予兆等を確認した場合には、所管省庁等を通じて国家サイバー統括室まで連絡[11]をお願いします[12]。

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

ベンダ等による高性能 AI の活用により、脆弱性の発見・修正等が高速化することが考えられます。また、高性能 AI が攻撃者に悪用されることにより、脆弱性の発見から悪用までの時間が極めて短くなるとともに、多数の脆弱性への対応が必要となります。こうした蓋然性が高まっていることを前提に、既知の未処理脆弱性のリスクを改めて検証し対応を行うとともに、資産管理を徹底した上で、脆弱性情報を積極的に収集し、発見された脆弱性のリスク評価及びリスクに応じた対応（修正プログラムの適用やリスク緩和措置等）を速やかに行うことをお願いします。また、多数の脆弱性への対応を同時並行で求められる可能性が高まることから、脆弱性の影響度、悪用リスク、事業継続への影響等を踏まえた優先順位付けを行うことも重要です。

その際、迅速に行われるべきリスク評価及びリスクに応じた対応は、事業継続等の観点も踏まえた総合的な判断となり得ることから、あらかじめそのプロセス・体制等を構築し、業界団体や事業所管省庁とも情報交換を図ることが推奨されます。

---

[10] IPA　中核人材育成プログラム 事業内容
https://www.ipa.go.jp/jinzai/ics/core_human_resource/about.html

[11] 「重要インフラのサイバーセキュリティに係る行動計画」では、重要インフラ事業者等は重要インフラ所管省庁及びセプターを経由して内閣官房へ情報連絡を行い、内閣官房は重要インフラ所管省庁及びセプターを経由して重要インフラ事業者等へ情報提供を行うことを基本としています。

[12] 警察では、各都道府県警察や重要インフラ事業者等で構成される「サイバーテロ対策協議会」等の枠組みを通じて情報提供・注意喚起等を実施しているところ、実空間における対応もあり得ることから、重要インフラ事業者等においては、警察にも相談等をお願いします。

別紙２

「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実施について（重要インフラ事業者等に対する注意喚起）」に係る補足説明

令和８年５月 25 日
国土交通省水管理・国土保全局水道事業課水道計画指導室

本資料は、令和８年５月 18 日に AI 性能の高度化を踏まえたサイバーセキュリティ対策に関する関係省庁会議においてとりまとめられた「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実施について（重要インフラ事業者等に対する注意喚起）」に記載の対策内容について補足説明するものです。

以下の補足説明のほか、「水道分野における情報セキュリティ確保に係る安全ガイドライン（第二版）」（令和８年５月 13 日改定）（以下「安全ガイドライン」という。）及びその概要版等を参考にサイバーセキュリティ対策の強化をお願いします。

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

安全ガイドラインの「1 「安全ガイドライン」策定の背景」において、以下のとおり経営層に係る説明があります。経営層のリーダーシップの下で、リスク対策の実施方針の検討、予算や人材の確保・割当、実施状況の確認や問題の把握・対応等のサイバーセキュリティ対策の実施をお願いします。

1.1.1 「安全ガイドライン」の目的

サイバーセキュリティに係るリスクへの必要な備えや、有事の際の適切な対処等を実現すること等であり、特に、経営層（【1.1.6 責任者・組織等の役割(1)】参照）が積極的に関与し、サイバーセキュリティに係るリスクへの備えを経営戦略として位置付け、サイバーセキュリティに係るリスクマネジメントを実施することなどにより、重要インフラ事業者等自らが自己検証を行いつつ、対策を進めていくことが必要となっている。

1.1.6 責任者・組織等の役割

各重要インフラ事業者等内における責任者・組織等の役割を以下のとおり定義する。

なお、該当する責任者・組織等そのものが存在しない場合、同様の役割を担っている役割・組織等に読み替えること。

(1) 経営層

経営層は、重要インフラ事業者等の社会的責任として、サイバーセキュリティを確保するよう取り組むこと。また、自らがリーダーシップを発揮し、任務保証

の考え方を踏まえて対応すること。

なお、「重要インフラのサイバーセキュリティに係る行動計画」（2025 年６月 27 日）に示されたように、組織の意思決定機関が決定したサイバーセキュリティ体制が、当該組織の規模や業務内容に鑑みて適切でなかったため、組織が保有する情報が漏えい、改ざんまたは滅失（消失）もしくは毀損（破壊）されたことにより会社に損害が生じた場合、体制の決定に関与した経営層は、組織に対して、任務懈怠（けたい）に基づく損害賠償責任を問われ得る。

また、決定されたサイバーセキュリティ体制自体は適切なものであったとしても、その体制が実際には定められたとおりに運用されておらず、経営層や監査役がそれを知り、または注意すれば知ることができたにも関わらず、長期間放置しているような場合も同様である。

個人情報の漏えい等によって第三者が損害を被ったような場合、経営層・監査役に任務懈怠につき悪意・重過失があるときは、第三者に対しても損害賠償責任を負う点についても留意する必要がある。

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

○基本的な対策の確実な実施

別紙１の２．で挙げられている、各分野の安全基準、リスクアセスメント、脆弱性管理、事業継続計画の策定について、以下のとおり補足説明します。

・各分野の安全基準

「水道施設の技術的基準を定める省令」においては、水道施設の運転管理をする電子計算機に関して、サイバーセキュリティを確保するための必要な措置が講じられていることが具備しなければならない要件として規定されており、これが水道分野の安全基準（強制基準）に該当します。詳しくは、安全ガイドラインのコラム２を参照ください。

・リスクアセスメント

安全ガイドラインの「4.2 リスクアセスメント」において、以下のとおりリスクアセスメントに係る説明が実施方法等とともにあります。セキュリティ対策の運用において、リスクアセスメントを実施し、その結果を踏まえて目標とする将来像の設定をお願いします。

4.2 リスクアセスメント

【趣旨・目的】

サイバーセキュリティ確保のための仕組みは、セキュリティリスクに関する環境変化や日々のセキュリティ対策の運用状況に応じて適宜見直さなければ、新たな脅威に対応できない。そのため、セキュリティ対策の運用においてリスクアセスメントを行う必要がある。

システム運用中も、サイバー攻撃に関する新たな脅威の発生等の環境変化に応じて適宜リスクアセスメントを実施し、本来あるべき状況や要件を検討・目標とする将来像を決定することが重要である。

また、サイバーセキュリティ戦略本部・重要インフラ専門調査会「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第１版）」別紙３を参照ください。

<https://www.mlit.go.jp/sogoseisaku/jouhouka/content/001310078.pdf>

表．リスクアセスメントプロセス（安全ガイドライン概要版からの抜粋）

リスクアセスメントプロセス	
①リスクアセスメントの対象の特定	絶えず変化する自組織を取り巻く状況及び関係主体等のニーズを踏まえ、重要インフラサービスの提供に必要な業務の範囲・水準等を明らかにするとともに、当該業務の遂行に必要な情報システム等の経営資源を特定する。また、その過程で自組織のリスクに対する態度・リスク許容度を分析する
②リスク特定	情報システム等の経営資源に対する「サイバーセキュリティリスク」を特定する
③リスク分析	リスクに対する態度・リスク許容度等を考慮しつつ、「事象の結果によるサービス・業務への影響度合い」や「事象の発生可能性」等を評価軸として策定されるリスク基準を活用して、特定されたリスクの大きさを確認する。重要インフラサービスの継続提供を不確かなものとするシナリオを作成し、リスク分析を実施することが望ましい。重要インフラサービスの継続的提供を不確かなものとするリスクとしては、自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化、感染症やテロ・戦争、システム障害、労災・事故、内部不正等があり、リスクの特性に応じたリスク分析手法を選択する
④リスク評価	基準値以上の大きさのリスクを抽出するとともに、個別事情も考慮してリスク対応の対象とするリスクを抽出する

・脆弱性管理

資産管理を行って脆弱性を把握し、適切な脆弱性管理を行うことが重要です。脆弱性診断を外部のベンダ等の事業者に依頼する場合には、実施主体や実施内容等が適切であることを確認・判断することが重要ですが、その際に、例えば、以下のガイドラインが参考になります。最新のものを参照するようにしてください。この他、情報セキュリティや脆弱性等の管理に関する各種の国際規格（ISO）もあり、適宜参照ください。

・政府情報システムにおける脆弱性診断導入ガイドライン（デジタル庁）
　最適な脆弱性診断を選定、調達できるようにするための、脆弱性診断導入に係る基準とその指針について説明したもの。政府機関向けのものですが、脆弱性診断の分類、要件、診断ベンダーの選定基準、実施基準等を規定しており、水道事業者等においても活用可能なものです。
　〈https://www.digital.go.jp/resources/standard_guidelines〉

また、ベンダ等の事業者が提供する脆弱性診断サービスをリスト化したものとして、「情報セキュリティサービス基準適合サービスリスト」の「脆弱性診断サービス」や「ペネトレーションテスト（侵入試験）サービス」があります。当該リストには、経済産業省の定める情報セキュリティサービス基準（情報セキュリティサービスに関する一定の技術要件及び品質管理要件等）への適合が審査登録機関により認められたサービスが掲載されており、適宜参照ください。

・情報セキュリティサービス基準適合サービスリスト（独立行政法人情報処理推進機構）
　〈https://www.ipa.go.jp/security/service_list.html〉
・情報セキュリティサービス基準（経済産業省）
　〈https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html〉

・事業継続計画の策定

安全ガイドラインの「4.5 事業継続計画等」において、以下のとおり事業継続計画に係る説明があります。経営層のリーダーシップの下で、リスク対策の実施方針の検討、予算や人材の確保・割当、実施状況の確認や問題の把握・対応等のサイバーセキュリティ対策の実施をお願いします。

4.5 事業継続計画等

【趣旨・目的】

重要インフラサービス障害が発生した場合、安全を確保するとともに、許容可能な時間内に許容可能な水準まで復旧させることが要求されるため、重要インフラサービス障害の発生に備えた対処態勢をあらかじめ整備することが重要となる。

そこで、初動対応（緊急時対応）の方針等を定めた「コンティンジェンシープラン」、事業継続を目的とした復旧対応の方針等を定めた「事業継続計画（BCP：Business Continuity Plan）」及び平時のサービス水準までの復旧対応の方針等を定めた「事業復旧計画」に、サイバー空間からの脅威にも備えられるよう、サイバーセキュリティを組み入れる。策定に当たり、「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書【別紙】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」を参照とすることが望ましい。

なお、重要インフラ事業者等としてのBCP等とは別のものとして、重要インフラサービスの継続に特化したIT-BCP等を策定している場合はBCP等との整合的な運用の確保が必要である。

○更なる対策の強化

別紙１の２．で挙げられている、「ゼロトラスト」の考え方、所管省庁等を通じた国家サイバー統括室への連絡について、以下のとおり補足説明します。

・「ゼロトラスト」の考え方

安全ガイドラインの「7 専門用語集　7.3 その他」において、以下のとおり用語の説明があります。

(9) ゼロトラストセキュリティ

ゼロトラストセキュリティとは、外部ネットワーク（インターネット）と、内部ネットワーク（LAN）との境界による防御（境界型セキュリティ）には限界があり、内部ネットワーク内にも脅威が存在し得るという考えのもと、データや機器等の単位でのセキュリティ強化をうたった考え方を指す。

・所管省庁等を通じた国家サイバー統括室への連絡

インシデントやその予兆等を確認した場合には、「健康危機管理の適正な実施並

びに水道施設への被害情報及び水質事故等に関する情報の提供について」（令和８年４月３日付け国水水第 18 号国土交通省水管理・国土保全局水道事業課長通知）の「水道における情報システム障害等が発生した場合」に基づいて、情報の提供をお願いします。国家サイバー統括室に対しては国土交通本省より連絡します。

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

・脆弱性の発見・修正等、脆弱性への対応

既知の未処理脆弱性のリスクを改めて検証し対応を行うとともに、前述のとおり、資産管理を行って脆弱性を把握し、適切な脆弱性管理を行うことが重要です。脆弱性診断を外部のベンダ等の事業者に依頼する場合には、適宜、上記のデジタル庁のガイドライン等（今後の更新を含め）を参考にして適切な診断手法であるかどうかを確認するようにしてください。

また、国家サイバー統括室及び経済産業省では、ソフトウェア・ベンダに対して、高性能 AI も活用しながら、ソフトウェア開発ライフサイクル全体において脆弱性の早期発見・対応に率先して取り組むよう注意喚起を行っているところです。高性能 AI を活用するソフトウェア・ベンダを活用することも、脆弱性への対応に有効です。

・リスク評価

リスク評価は、上記の２．の「リスクアセスメント」の実施プロセス（リスクアセスメントの対象の特定→リスク特定→リスク分析→リスク評価）の最後の段階に位置し、前段階のリスク分析において策定されるリスク基準の基準値以上の大きさのリスクを抽出した上で、個別事情も考慮してリスク対応の対象とするリスクを抽出することになります。そして、抽出したサイバーセキュリティリスクに対し、「サービス・業務への影響度」や「事象の発生頻度」等を踏まえて、「低減」、「回避」、「移転（共有）」、「保有（受容）」の４つのリスク対応のうち、いずれかの具体的な対応を決定します。リスクアセスメントの詳細は、安全ガイドライン等を参照ください。

以上