資料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

2026年5月28日

国土交通省

高性能AIの出現に対するサイバーセキュリティ対策強化の必要性

国土交通省

●高性能AI、とりわけ、本年４月７日に米国アンソロピック社が公表した「Claude Mythos Preview」（ミュトス）を始めとするフロンティアAIモデルの出現により、**システムの脆弱性を発見・修正等する能力が急速に向上。**

●高性能 AIの活用による、脆弱性の発見・修正の高速化、攻撃の早期検知・対処等により、重要インフラ事業者のサイバー対処能力の更なる強化が期待できる。

●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。**

●こうしたサイバーセキュリティ上の脅威に直面していることを踏まえ、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、**官民が連携し、対策強化を早急に進めていくことが必要。**

重要インフラ事業者等の皆様へのお願い

国土交通省

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を、攻撃被害によるコストや損失を減らし、サービス停止を回避するために必要な投資と位置付けて対策を行う。

・サイバー攻撃による被害リスクに応じた対応方針の検討
・予算や人材の手当て
・継続的な取組の進捗状況の確認や問題の把握・対応　等

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

●基本的な対策を確実に実施する。

・システム構成等の把握や監視、バックアップデータの確保、事業継続計画の策定、攻撃発生時の対応体制の整備、委託先等のサイバーセキュリティ対策状況の把握　等

●加えて、更なる取組の検討・実施を推進する。

・「ゼロトラスト」に基づくシステム設計・運用への移行

※ゼロトラスト：システム内のあらゆる挙動を常に確認・検証する考え方。

・高性能AIのサイバーセキュリティ対策への活用
・政府の人材育成プログラムも活用した専門性の高い人材の育成

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

・脆弱性情報を積極的に収集し、発見された脆弱性に対し、事業継続への影響等を踏まえ必要に応じ優先順位付けを行った上で、迅速かつ的確に修正プログラムの適用等を行う。

基本的なサイバーセキュリティ対策の主要項目例

国土交通省

項目	主な目的	具体の対策内容（例）
資産管理	守るべき情報システム、情報等の特定・明確化	・情報資産目録の作成・更新 ・ネットワーク構成図、データの流れ図等の作成・更新 ・未承認の機器の接続有無の監視
リスクアセスメント	事業活動等に対する影響評価に基づく、対応すべきリスクの特定・優先順位付け（対応方針の作成）	・保有する情報資産で想定されるリスクの特定・分析・影響度の評価 ・対応すべきリスクの決定・優先順位付け ・定期的な評価の実施
脆弱性管理	システム等の弱点・欠陥の解消による攻撃可能箇所の最小化	・脆弱性情報の収集、その解消を実施するための管理体制の構築 ・定期的な脆弱性診断の実施 ・脆弱性情報に基づく、迅速な修正プログラムの適用や機器の更新等
アカウント管理・認証・アクセス制御	システム、情報等の接続・利用の限定による不正利用・アクセスの防止	・システム、情報等の利用者とその利用権限を最小限に限定 ・本人確認等に対する強固な認証手続の実施（多要素認証など）
監視・分析	不正利用・アクセスやシステム異常の早期検知	・システム、情報等の不正利用や不正アクセス、システム異常の監視 ・ログ（通信・操作記録）分析やアラート対応による早期検知 ・常時監視体制の整備
バックアップの確保	サイバー攻撃によるシステム停止リスクの最小化、システムの早期復旧	・バックアップの定期的な取得、データの分離保管 ・復旧テストの平時からの実施
事業継続計画の策定	サービス停止の回避、早期の復旧	・災害だけでなく、サイバー攻撃も想定したBCP策定 ・代替手段、復旧優先順位の明確化
インシデントへの対応及び復旧	被害の最小化と早期の復旧、再発の防止や将来のインシデント抑止	・対応体制の構築、対応手順（経営層への報告を含む）の確立 ・通信遮断やシステム停止等、攻撃発生時の被害拡大防止策の実施 ・原因分析と再発防止策の検討、実施
サプライチェーン・リスクへの対応	外部起因による事業継続リスクの低減、外部経由のサイバー攻撃の抑止	・委託先、取引先のセキュリティ対策状況の把握 ・サプライチェーンにおけるリスク評価及びリスク軽減策の実施 ・委託先、取引先へのセキュリティ要求事項の整理、契約・監査による統制

※記載されている内容はあくまでも一例です。各種ガイドライン等を参照した上で、各組織の実情に応じた対策をお願いします。

対応に当たっての留意点

国土交通省

- 「閉域網（インターネット等と接続されていないネットワーク）であっても安全とは限らない。」との意識をもってセキュリティ対策を講じていくことが重要。

- 誰しもがサイバー攻撃を受ける可能性があることを前提に、障害等による影響をいかに低減し、事業継続させるか等の対策（レジリエンス対策）を講じていくことが重要。

- サイバー攻撃の巧妙化・高度化、技術革新等の動向のほか、自らの事業運営におけるデジタル化の進展等を踏まえ、セキュリティ対策を継続的に検証し見直すことが重要。

- 国家を背景とした攻撃キャンペーン等、深刻化するサイバー脅威に対しては、官民双方向のコミュニケーションの強化が重要。

  （サイバー事案やその予兆等を認識した場合には、速やかに連絡をお願いします。）

（参考）

政府の対策パッケージ「Project YATA-Shield」及び関係機関への注意喚起の概要

Project YATA-Shield※

- フロンティアAIモデルによるサイバーセキュリティ性能が向上する中においても、我が国のサイバーセキュリティが確保されるよう、**政府全体としての対策パッケージを取りまとめ**。

基本的な認識・考え方

重要インフラ事業者等・政府機関等が取るべき対応

- **発見された脆弱性のパッチ適用やリスク緩和措置**を速やかに実施（リスクベース）
- **基本的な対策**、**多層防御の実施**、**インシデント発生時の備え**　等

※英国・米国政府の注意喚起も参考に

脆弱性を発見するAIの進化

- **Anthropic（Project Glasswing）**：Mythosへのアクセスを、**ビッグテックや重要インフラ等**に限定。
- **OpenAI**：GPT-5.5-Cyberへのアクセスを、**一部の認証者**に限定して付与。

実施する施策

重要インフラ事業者等・政府機関等への対応

① 重要インフラ事業者等への注意喚起等
② 金融分野での先行的な取組及び 他分野への展開
③ 人材育成支援
④ 政府機関等の情報システムにおける対応

脆弱性の発見・修正等への対応

① 外国政府機関やビッグテック等との更なる連携
② ソフトウェア・ベンダへの注意喚起
③ AISIによる技術支援等
④ 技術開発の推進
⑤ 高性能AIを活用したサイバー対処能力強化

※YATA：Yielding Advanced Threat Awareness with AI（脅威の可視化）の頭文字。
「正確に写す」という八咫鏡(やたのかがみ)もあるように、「ＡＩ性能の高度化に伴うサイバー脅威を正しく認識し、防御する／対応する」という趣旨。

関係機関への注意喚起

● 対策パッケージ「Project YATA-Shield」の取りまとめ・公表を行い、**重要インフラ事業者等、政府機関等、ソフトウェア・ベンダへの注意喚起**を公表・実施。

重要インフラ事業者等

●経営層のリーダーシップの下での対策の実施

→ 必要な投資と捉えて、組織のリスクマネジメントとして実施

●基本的な対策の確実な実施等

英：基本的な対策
米：隔離・復旧
} が重要

→ 資産管理、脆弱性対策、インシデント対応・復旧など（重要インフラ統一基準）

→ 実施状況の機動的な確認

●高速化する脆弱性の発見・修正等への対応

→ 脆弱性のリスク評価、パッチ適用・リスク緩和措置の速やかな実施

政府機関等

●組織トップのリーダーシップの下、対応の徹底を要請

●基本的な対策の徹底

英：基本的な対策
米：隔離・復旧
} が重要

→ 資産管理、脆弱性対策、インシデント対応・復旧など（政府統一基準）

→ 実施状況の機動的な確認（各機関・NCOによる監査）

●脆弱性対策の強化

→ パッチ管理・適用の運用設計の見直し、パッチ適用・リスク緩和措置の速やかな実施

ソフトウェア・ベンダ

●高性能AIも活用しながら、**脆弱性の早期発見・対応**

① リリース前のソフトウェア

→ 脆弱性を低減させた上でリリース

② リリース後のソフトウェア

→ 脆弱性の把握、パッチの早期作成、顧客への早期提供