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

議事次第

令和８年５月 18 日（月）
16 時 15 分～16 時 45 分
赤坂グリーンクロス
４階会議室 ｒｏｏｍＡ

１．開会・挨拶

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強化について

３．閉会・挨拶

＜資料＞

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（案）～Project YATA-Shield～

資料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強化について（案）（重要インフラ事業者等に対する注意喚起）

資料３　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（案）（ソフトウェア・ベンダに対する注意喚起）

資料４　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（案）（政府機関等に対する注意喚起）

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
出席者名簿

松本　尚	サイバー安全保障担当大臣
飯田　陽一	内閣サイバー官
大村　真一	内閣官房国家サイバー統括室統括官
門松　貴	内閣官房国家サイバー統括室統括官
安藤　敦史	内閣官房国家サイバー統括室統括官
関口　祐司	内閣官房国家サイバー統括室審議官
中溝　和孝	内閣官房国家サイバー統括室審議官
斉田　幸雄	内閣官房国家サイバー統括室審議官
飯島　秀俊	内閣官房国家サイバー統括室審議官
佐野　朋毅	内閣官房国家サイバー統括室審議官
田村　亮平	内閣官房国家サイバー統括室内閣参事官
庄司　周平	内閣官房国家サイバー統括室内閣参事官
伊藤　建	内閣官房国家サイバー統括室企画官
柏原　裕	内閣官房内閣審議官（国家安全保障局）
泉　恒有	内閣府政策統括官（経済安全保障担当）
福永　哲郎	内閣府科学技術・イノベーション推進事務局統括官
逢阪　貴士	警察庁サイバー警察局長
柳瀬　護	金融庁総合政策局総括審議官
森田　稔	デジタル庁総括審議官
三田　一博	総務省サイバーセキュリティ統括官
貝原　健太郎	外務省総合外交政策局参事官
藤吉　尚之	文部科学省サイバーセキュリティ・政策立案総括審議官
原口　剛	厚生労働省政策統括官（統計・情報システム管理、労使関係担当）
野原　諭	経済産業省商務情報政策局長
長井　総和	国土交通省政策立案総括審議官
吉野　幸治	防衛省サイバーセキュリティ・情報化審議官

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（案）
～Project YATA-Shield～

2026年5月18日

内閣官房国家安全保障局、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）、内閣府科学技術・イノベーション推進事務局、
警察庁、金融庁、デジタル庁、総務省、外務省、
文部科学省、厚生労働省、経済産業省、国土交通省、防衛省

1．背景・課題認識

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、サイバーセキュリティにおける脅威に直面している状況である。

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て、重要インフラ事業者等[1]への対応と脆弱性の発見・修正等に関する対応の双方に、サイバー安全保障の観点から、危機感を持って迅速に取り組むことが必要不可欠である。

こうした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る。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ある。

このため、重要インフラ事業者等においては、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行うとともに、ベンダ等においては、高性能AIの活用を含め、より早期の脆弱性の発見・修正等の実施が求められる。

---

[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う。

こうした喫緊の課題に対して、関係省庁・関係機関の緊密な連携の下、政府一体となって対応するため、「Project YATA-Shield」と題して、ここに関係省庁・関係機関による施策を取りまとめることとし、関係省庁・関係機関は、これら施策を迅速かつ的確に実施することとする。

2．実施する施策

1）重要インフラ事業者等及び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

［国家サイバー統括室、重要インフラ所管省庁等、内閣府］

重要インフラ事業者等において、経営層のリーダーシップの下、基本的なサイバーセキュリティ対策の確実な実施や、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が速やかに実施されるよう、注意喚起を行う。

また、国家サイバー統括室は、重要インフラ事業者等からのインシデント報告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、被害防止に向けて、必要とする主体に適切な形で情報提供する。そのため、重要インフラ事業者等からのインシデント情報の収集に取り組む。

加えて、重要インフラ所管省庁は、重要インフラ機能の確保の観点から、重要インフラ役務の提供上重大な脆弱性が認められる場合等には、国家サイバー統括室等との連携の下、重要インフラ事業者に対し必要な対応を行う。

②金融分野等での先行的な取組の実施及び他分野への展開

［国家サイバー統括室、重要インフラ所管省庁］

金融分野では、4 月 24 日に、民間企業・政府等が共通理解を持って必要な対応を検討・実施するための官民連携の枠組みが設置された。また、経済産業省の所管分野においても、５月１日に、官民での認識共有を図るための意見交換が行われた。引き続き、各重要インフラ分野において、その分野特性も踏まえて必要な対応を検討・実施できるよう、官民連携を推進する。

③人材育成支援［総務省、経済産業省、文部科学省、関係省庁］

重要インフラ事業者等のサイバーセキュリティ人材を育成し、サイバー対処能力強化に繋

げるため、NICT[2]による実践的サイバー防御演習「CYDER」や、IPA[3]産業サイバーセキュリティセンター等による人材育成支援、リ・スキリング等を含む大学・専修学校等におけるサイバーセキュリティ人材育成機能の強化を推進する。

④政府機関等[4]の情報システムにおける対応

［国家サイバー統括室、デジタル庁、関係省庁］

民間事業者のみならず、政府機関等に対しても基本的なサイバーセキュリティ対策の確実な実施や、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応強化が速やかに実施されるよう、注意喚起を行う。また、政府機関等の情報システムにおいても、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を進める。

２）脆弱性の発見・修正等の対応

①外国政府機関や AI 開発者等との更なる連携［国家サイバー統括室、外務省、関係省庁］

これまでにも外国政府機関や AI 開発者等との情報交換等を積み重ねているところ。我が国のサイバー対処能力強化を図る観点から、重要インフラ事業者等やベンダ等のニーズも踏まえつつ、外国政府機関や AI 開発者等との更なる連携を図り、高性能 AI へのアプローチも含め、必要な情報収集・対応を行う。

②ソフトウェア・ベンダへの注意喚起［経済産業省、国家サイバー統括室］

ソフトウェア・ベンダ[5]が、セキュア・バイ・デザインの原則に基づき、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う。これを通じて、脆弱性を低減させた上でのソフトウェアのリリースや、残存する脆弱性の修正プログラムの作成・提供等を促す。

③AISI[6]による技術支援等［内閣府、国家サイバー統括室］

AISI により、フロンティア AI モデルのサイバーセキュリティ性能や悪用等を迅速かつ的確に把握するための情報収集・評価の実施及びこれを踏まえた情報提供、ガイドラインの策定等、これらを実施するための評価方法・環境等の構築、英国 AISI を始めとする諸外国 AISI

---

[2] 国立研究開発法人情報通信研究機構

[3] 独立行政法人情報処理推進機構

[4] 国の行政機関、独立行政法人及びサイバーセキュリティ基本法（平成 26 年法律第 104 号）第 13 条に規定される指定法人をいう。

[5] ソフトウェアを開発・提供・運用する主体

[6] AI セーフティ・インスティテュート

との連携を行う。

④技術開発の推進［内閣府、経済産業省、総務省、文部科学省］

経済安全保障重要技術育成プログラムや NICT によるビッグテック等との共同研究、研究機関等による技術開発を通じて、我が国の脆弱性の発見・修正等の AI 技術の高度化を図る。

⑤高性能 AI を活用したサイバー対処能力の強化［国家サイバー統括室、警察庁、防衛省］

高性能 AI を悪用したサイバー攻撃の増加を念頭に、サイバー関連データの国家サイバー統括室への集約の推進や、機密性の高いデータの取扱い、これらを踏まえた迅速な意思決定を行う上での AI 活用の考え方等の検討・具体化、AI を活用した資機材の導入等、AI を活用したサイバー対処能力の向上・強化に努める。その上で、サイバー対処能力強化法[7]に基づく協議会の枠組みの下、IPA・AISI と連携し情報共有等の取組を強化する等、AI セキュリティに関する官民連携の強化を図る。

3．フォローアップ

AI を巡る動向が急速に変化する中においても、より実効的な対応を継続的に行うべく、関係省庁・関係機関はこれら施策の実施状況を機動的に確認し、追加的な対応を不断に検証・実施する。

[7] 重要電子計算機に対する不正な行為による被害の防止に関する法律（令和 7 年法律第 42 号）

資料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強化について（案）
（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。

資料３

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（案）
（ソフトウェア・ベンダに対する注意喚起）

令和８年５月 18 日
内閣官房国家サイバー統括室、経済産業省

足下で、ソフトウェア※の脆弱性発見について高い能力を有する AI（高性能 AI）の開発が進んでいる。こうした高性能 AI は、未知の脆弱性の早期発見や是正によりセキュリティ向上に役立つ一方で、仮に悪意ある者に使われた場合には、サイバーセキュリティ上のリスクが一気に高まるおそれがある。

このため、政府全体としては、内閣官房国家サイバー統括室を中心に AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化に関する対策パッケージ「Project YATA-Shield」をとりまとめたところである。経済産業省としても、高性能 AI を活用したサイバーセキュリティ産業の育成も重要との観点の下、引き続き、国内のサイバーセキュリティ対策の実装を支える高度な人材育成や、研究開発などサイバーセキュリティ産業の育成・振興等の各種施策の企画・実行を推進していく予定である。

こうした政府の取組も念頭に置きつつ、広く産業界で用いられているソフトウェアを開発・提供・運用する主体（ソフトウェア・ベンダ）の皆様におかれては、セキュア・バイ・デザインの原則に基づき、以下のとおりソフトウェア開発ライフサイクル（SDLC）全体において高性能 AI も活用しながら脆弱性の早期発見・対応に率先して取り組むことをお願いしたい。なお、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されたい。

１．リリース前のソフトウェアについては、高性能 AI を積極的に活用し、リリース後の脆弱性発見の可能性を低減させた上で、リリースをする。

２．リリース後のソフトウェアについては、自ら高性能 AI を積極的に活用して自らがリリースしたソフトウェアの脆弱性の把握に努めるとともに、脆弱性関連情報の収集・早期把握に努めつつ、脆弱性が発見された場合には（必要に応じ高性能 AI も活用して）パッチを早急に作成し、顧客に速やかに提供する。

※　ソフトウェアには、製品として顧客に提供されるソフトウェアのほか、クラウドサービスなど顧客が直接利用する IT サービスであるソフトウェアサービス、システム・サービスの構成要素として提供されるソフトウェアも含まれる。

＜参考資料＞

- 国家サイバー統括室「国際共同ガイダンス「セキュアバイデザイン・セキュアバイデフォルト原則」に署名（令和５年 10 月）
- 経済産業省／国家サイバー統括室「サイバーインフラ事業者に求められる役割等に関するガイドライン」（令和８年３月）
- 経済産業省「産業界へのメッセージ」（令和８年４月）
- 独立行政法人情報処理推進機構「情報セキュリティ早期警戒パートナーシップガイドライン」（最終更新：令和８年４月）

資料4

事務連絡
令和8年5月18日

各府省庁情報セキュリティ担当者 各位

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（案）

内閣官房国家サイバー統括室

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（高性能AI）は、開発・利用するプログラム等における脆弱性の発見・修正等や各政府機関等[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る。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ため、悪用リスクを前提として、対策強化を早急に進めていくことが必要である。

このため、各政府機関等においては、以下のとおり、高性能AIの悪用リスクに備え、政府統一基準に基づく基本的な対策を徹底するとともに、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の強化を図られたい。

1．高性能AIの悪用リスクに備え、政府統一基準に基づき、資産管理、リスクアセスメント、脆弱性対策、アカウント管理・認証・アクセス制御、バックアップの確保、ログの取得・管理、監視・分析、インシデントへの対応及び復旧等、基本的な対策を徹底すること[2,3]。

2．特に、情報システムを構成する機器等へのセキュリティパッチの速やかな適用は非常に重要であり、高性能AIの悪用などのサイバー攻撃の高度化、自動化等を踏まえ、必要に応じて、セキュリティパッチ等の対策用ファイルの適時の適用を前提とした運用設計（パッチマネジメント（管理））を見直すこととするほか、機器等で利用するソフトウェアに関する脆弱性情報を入手し脆弱性対策計画を策定し実施する場合においても、こう

した技術や脅威の動向を踏まえて、迅速な対策が必要であるかどうかを見極めた上で[4]、実施の要否、実施時期等を判断することとするなど、脆弱性対策の強化を図ること。

3．これらの実施状況については、実効的な対応を継続的に行うべく、各政府機関等で実施する情報セキュリティ監査において機動的に確認すること。なお、国家サイバー統括室による監査においても当該実施状況について確認を行う。

なお、国家サイバー統括室においては、巧妙化・高度化を遂げる組織的なサイバー攻撃につき、初期段階から把握し、被害の防止につなげるため、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、各政府機関等に対する適切な形での情報提供やサイバー対処能力強化法等に基づく措置を含む能動的な防御・抑止に取り組むこととしている。そのため、各政府機関等においては、インシデントやその予兆等を確認した場合には、国家サイバー統括室まで速やかに報告願いたい。

---

[1] 国の行政機関（26 機関）、独立行政法人（86 法人）及び指定法人（10 法人）をいう。

[2] 英国 AISI による Claude Mythos Preview に関する評価においても、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、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が改めて示されている。（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）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いる。（米国 CISA　CI Fortify: Strengthening Resilience Across Critical Infrastructure https://www.cisa.gov/topics/industrial-control-systems/ci-fortify）

[3] 特に、攻撃の端緒となりやすいインターネットへの露出領域を最小限にするとともに、閉域網について過信することなく管理の徹底をはかること。

[4] 横断的アタックサーフェスマネジメント事業等をとおして GSOC から情報提供している脆弱性については、リスクベースを評価した上で通知しており、参考とされたい。