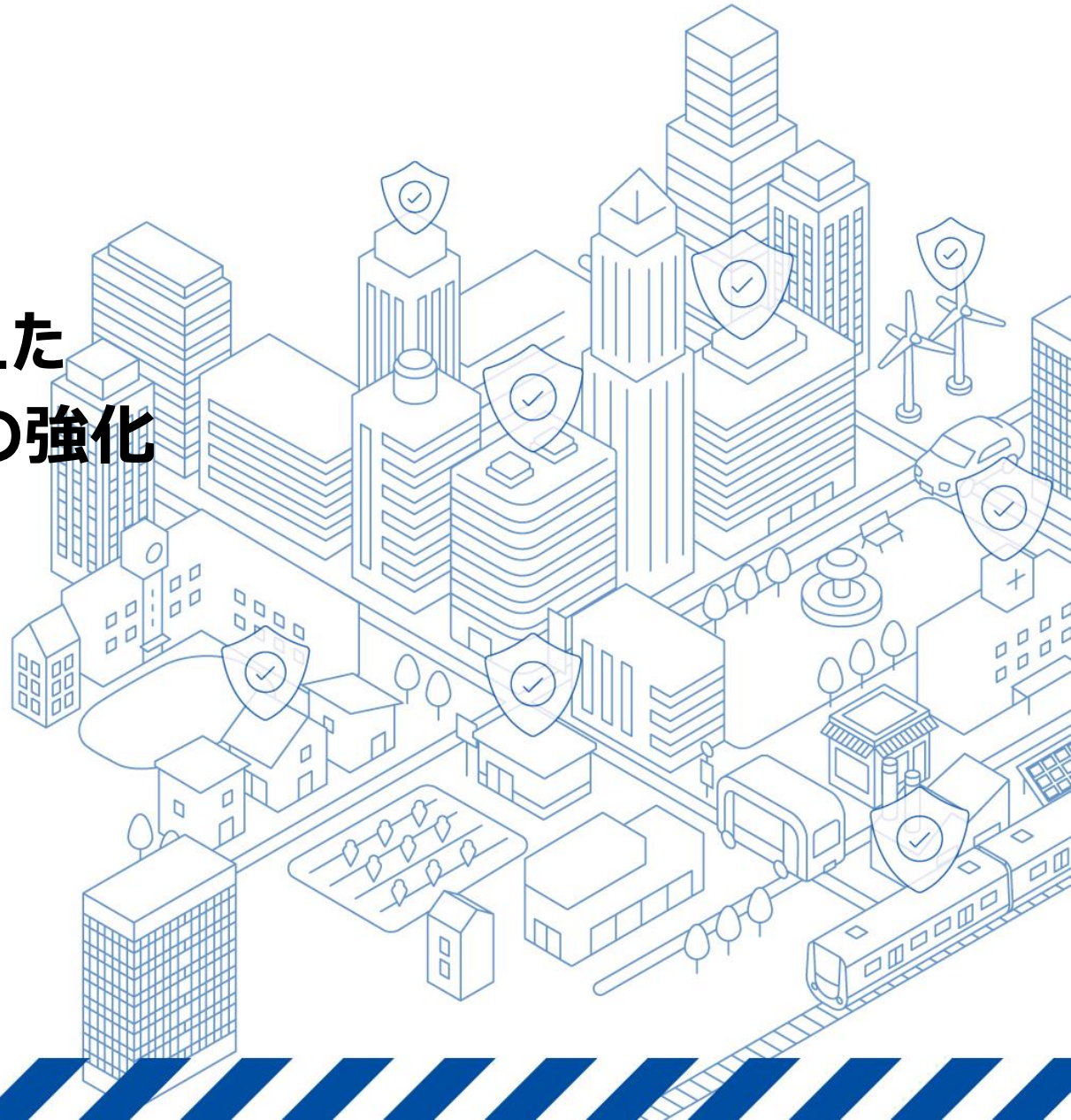
資料６

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



2026年６月15日

内閣官房国家サイバー統括室（NCO）

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、**総理指示を踏まえて、政府全体としての対策パッケージを取りまとめ。**（5月18日）

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

これまでの取組及び今後の取組方針①

- **AI性能の高度化を踏まえた、政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」**に基づき、関係省庁において、**対策を迅速に進めていく**。

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：

- ◆ **分野共通事項**として、**重要インフラ事業者等への注意喚起**（関係省庁連名）を実施（5/18付）。
- ◆ 加えて、重要インフラ所管省庁においては、これまでに**大臣出席の下、各業界団体トップ等との意見交換を実施**し、**脅威認識や対策の方向性を共有**。特に金融分野では、官民連携会議の作業部会での議論も踏まえて、**金融機関等に対し、短期的な対応を要請**（5/22付：金融庁・日本銀行連名）。また、**情報通信分野では**、ICT-ISACにおいて、レジリエンス強化に向けて、**フロンティアAIに対する考え方や対応策を検討中**。
- ◆ 引き続き、各重要インフラ分野において、先行的な取組も参考にしつつ、**分野特性や事情も踏まえて必要な対応・確認進めていく**。

② 政府機関等：

- ◆ **政府機関等への注意喚起**を国家サイバー統括室（NCO）から全府省庁に対し発出（5/18付）。
- ◆ 今後、**高性能AIを活用した、政府の重要システムにおける脆弱性の確認・対応等**を、**国家サイバー統括室（NCO）を中心に、デジタル庁を始めとする各府省庁とも連携して進めていく**。

③ 各種基準・ガイドライン等への反映

- ◆ 「Project YATA-Shield」や今般の注意喚起等を踏まえて、**重要インフラ統一基準や政府統一基準、関連するガイドライン**等も必要に応じ策定・改定を進めていくとともに、**サイバーセキュリティ戦略に基づく年次計画（サイバーセキュリティ2026）**等にも反映していく予定。

施策の実施状況：重要インフラ事業者等への取組

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

５月１８日（月）に松本サイバー安全保障担当大臣ご出席の下、関係省庁会議を開催。ＡＩ性能の高度化を踏まえた政府全体としてのサイバーセキュリティ対策となる「Project YATA-Shield」を取りまとめた。

［金融庁］AI脅威に対する金融分野のサイバーセキュリティ対策強化に関する官民連携会議

［経済産業省］高性能AIへの対応に関する赤澤経済産業大臣と重要インフラ事業者との意見交換

［総務省］情報通信・地方行政・郵便分野のサイバーセキュリティ確保に関する会合

［厚生労働省］AI によるサイバー攻撃に関する情報共有と医療機関等におけるサイバーセキュリティ対策に関する厚生労働省との意見交換

［国土交通省］AI性能の高度化を踏まえた国土交通分野のサイバーセキュリティ対策強化に関する官民対話

（参考）フロンティアAIによる脅威変化を踏まえた金融機関等の短期的な対応の要請

- 5月22日（金）に金融庁・日銀から金融機関等に対して、作業部会が取りまとめた内容を要請文として発出。

① フロンティアAIへの対応を経営課題として扱う

- 経営トップは、フロンティアAIへの対応を**IT部門にとどまらない全社的な経営課題**として扱い、**関係部門が横断的に連携**して対応できるようにする。
- **経営トップのリーダーシップの下、CIO、CISOをはじめとする経営層が直接関与**する。

② 優先的に対応すべきサービス／ITシステムを特定する

- **優先的に対応すべきサービス／ITシステムを特定**し、リソースを重点的に配分する等、リスクベースで対応する。（例：インターネットバンキング）
- 当該システムが共同運営形態で提供される場合、**利用者側・提供側双方での十分な認識共有、責任分担の明確化が必要**する。

③ 特定した資産の技術負債を解消しておく

- 脆弱性発見時に**パッチ適用対象を即時に特定できる状態**を確保する。
- 特権ID削除や未対応パッチの適用等により**技術負債を極力解消**することで、迅速なパッチ適用が可能な状態を確保する。特にサポートが終了している製品は、**サポート対象のバージョンへ更新**する。

④ パッチ適用に係る人的リソースを追加する

- 金融機関等やベンダーにおいてパッチ適用に係る**人的リソース追加を検討**する。
- 脆弱性の優先度判断に係る評価体制についても、上記同様に人的リソースを確保する。

⑤ ベンダーとの維持保守契約の内容を確認する

- ①**パッチ適用作業が現行の維持保守契約に含まれていること**及び**役割分担が明確であること**、②緊急にパッチ適用作業が必要な場合に、**夜間・休日等も含めて適時に対応可能な契約内容となっていること**を確認する。
- ベンダー側で必要なリソース確保状況を確認しつつ、リソースがひっ迫すること等も想定し、パッチ適用の遅延に係るリスク受容等のプロセスを整備する。

⑥ パッチ適用プロセスをリスクベースにする

- 発見された脆弱性が自組織のサービス／ITシステムに及ぼし得る**影響と攻撃が成立する蓋然性も踏まえた評価**に基づき、**よいリスクの高い脆弱性から対応**する。
- パッチ適用作業に係る事前のテストについて、想定されるリスクを総合的に勘案し、テスト実施内容の合理的な縮小等の対応も検討する。

⑦ パッチ適用以外の対策も強化する

- パッチ適用そのものが困難である場合等は、**多層防御の強化**を図る。
- **パッチが適用できないことによる残存リスクを評価した上で**、パッチ適用に要する期間を踏まえた**適切なリスク受容手続**を講じる。

⑧ 優先サービス／ITシステムの停止に備える

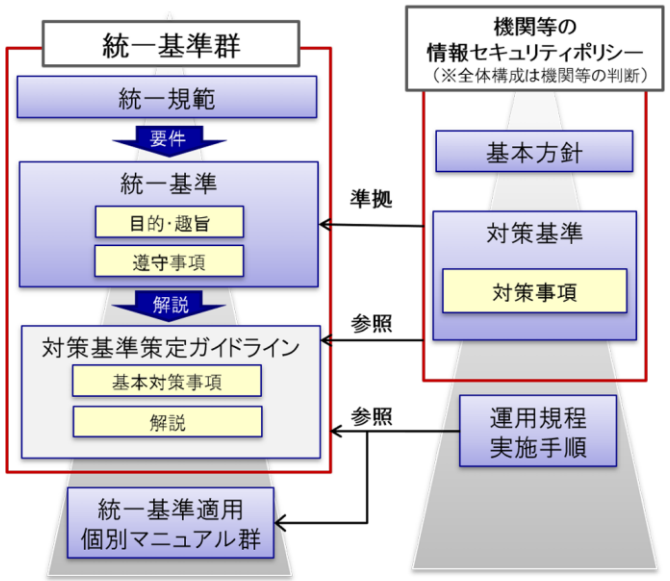
- **サイバー攻撃によりITシステムが停止する場合を想定**する。**システムを能動的に停止させざるを得ない場合もあらかじめ選択肢として検討**する。
- **BCPの有効性や顧客等への対応手順、緊急時の連絡体制等を点検**する。
- **能動的なサービス／ITシステム停止の判断基準及び手順を明確**にしておく。
- サードパーティが提供するソフトウェアやサービスの停止に備える。

⑨ 外部との連携を維持・強化する

- 金融ISACや各業界団体・コミュニティ、当局等からの情報に積極的にアクセスし、必要な情報収集をする。
- 自組織での取組を金融ISAC等の共助コミュニティで積極的に共有し、金融分野全体の強靭性の向上に努める。

- 「Project YATA-Shield」を踏まえて、本年６月12日に**政府統一基準に紐づくガイドラインを改定した**。加えて、**高性能AIを活用した、政府の重要システムにおける脆弱性の確認・対応等**を、**国家サイバー統括室（NCO）を中心に、デジタル庁を始めとする各府省庁とも連携して進めていく**。

「政府機関等の対策基準策定のためのガイドライン」の主な改定事項



○**脆弱性対策（セキュリティパッチ適用等）の強化**	• 高性能AIの悪用などのサイバー攻撃の高度化・自動化等をふまえ、 – **全情報システムについて、セキュリティパッチ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)を行う。 – **サイバー攻撃の高度化・自動化等の状況をふまえ、運用設計を見直す。** – **迅速な適用の要否を判断した上で、脆弱性対策計画を策定・実施する。** – 迅速な適用が必要な場合、**情報システムの運用を一時停止することも検討**する。

これまでの取組及び今後の取組方針②

- **AI性能の高度化を踏まえた、政府全体としてのサイバーセキュリティ対策パッケージ「Project YATA-Shield」**に基づき、関係省庁において、**対策を迅速に進めていく**。

脆弱性の発見・修正等への対応

① 外国政府機関等：

- 「Project YATA-Shield」の取組について、国家サイバー統括室（NCO）や外務省が直接又は在外公館を通じて、**同盟国・同志国等の関係当局に説明する**とともに、**各国の課題認識や取組状況等の情報収集を進めている**。
- 諸外国の**政府のみならず、産業界の要人**に対し、我が国の取組の**発信**や対応等に関する**意見交換**を積み重ねたところ。
- 引き続き、**情報収集や対外発信に取り組み、同盟国等と連携して対応を進めていく**。

② ビッグテック・ベンダ等

- 金融庁や外務省等の支援の下、**国家サイバー統括室（NCO）を中心**に、政府機関や重要インフラ事業者等が高性能AIにアクセスできるよう、**関係国政府やビッグテック等とも意見交換を積み重ねている**ところ。
- 我が国のサイバーレジリエンスの強化の観点から、**高性能AIの活用**は重要であり、種々のAIツールがある中で、**様々な選択肢を踏まえつつ、必要な対応を進めていく**。
- また、**国内ソフトウェア・ベンダへの注意喚起**（経済産業省・NCO連名）を実施（5/18付）。同日、**ベンダ関係団体トップとも意見交換**を実施。引き続き、**ベンダによる脆弱性の早期発見・対応を促していく**。

③ AISIによる技術支援等

- AISIでは、本年６月以降、**一般公開されているAIモデルのサイバーセキュリティ性能（一連の攻撃能力やソフトウェア脆弱性の発見能力）の評価**や**AIセキュリティに関する情報の取りまとめ・公開**に取り組む予定。

（参考）米国：高度なAIのイノベーション及びセキュリティの促進に関する大統領令

高度なAIのイノベーション及びセキュリティの促進に関する大統領令（2026年６月２日付）
（PROMOTING ADVANCED ARTIFICIAL INTELLIGENCE INNOVATION AND SECURITY）

概要

１．目的

- 高度なAI能力は米国をより強固にする一方で、**新たな国家安全保障上の懸念**をもたらす。米国は産業界と緊密に連携し続け、あらゆる脅威に立ち向かうため、最良かつ最も安全な技術の迅速な導入を確保。
- 米国は、**国家安全保障**と世界的な**AI優位性**の両方を強化する「アメリカ・ファースト」のサイバーセキュリティへの取組を、引き続き牽引。
- 米国の政策は、**民間部門と協力**し、**官民の情報システムを近代化**し、外部の脅威に対する耐性を強化すること、敵対勢力による搾取や盗用から米国の独創性及び知的財産を保護すること、そして米国の高度なAI活用能力を育成することにより、**AIのイノベーションとセキュリティを促進する**こと。

２．高度なAIに向けた米国システムのアップデート

- 本大統領令発令から**30日以内**に、
  （１）国家安全保障システム委員会は、**国家安全保障システムのサイバー防衛**を優先的に実施。
  （２）戦争長官は、**戦争省の情報システムのサイバー防衛**を優先的に実施。
  （３）国土安全保障長官は、**連邦政府の情報システムのサイバー防御等に関する拘束力のある適切な運用指針**を公表。
  （４）財務長官及び国土安全保障長官は、**AI産業及び重要インフラの運営事業者と自主的に連携**し、ソフトウェア脆弱性の検証・修正、脆弱性パッチの配布の調整等を行う**「AIサイバーセキュリティ・クリアリングハウス」を設立**。

３．セキュアなフロンティアモデルの展開

- 本大統領令発令から**60日以内**に、財務長官、戦争長官及び国土安全保障長官は、
  （１）AIモデルの高度なサイバー能力を評価し、**特定のフロンティアモデルの閾値を決定するベンチマークプロセス**（非開示）を策定。
  （２）**AI開発者と協力**し、開発者が以下を行うことができる**自主的な枠組み**を策定。
  ア　開発中のモデルが特定のフロンティアモデルの閾値を満たすか決定するため、**連邦政府と協議**。
  イ　特定のフロンティアモデルへのアクセスを、他の信頼できるパートナーに公開する前に**最大30日間、連邦政府に提供**。
  ウ　連邦政府と連携し、特定のフロンティアモデルに**早期アクセス可能な信頼できるパートナーを選定**。
  （３）本節のいかなる規定も、フロンティアモデルを含む新しいAIモデルの開発・公表等に関する政府による**強制的なライセンス、事前承認又は許可要件を設けることを認めるものと解してはならない**。