資料１

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

対策パッケージ(Project YATA-Shield)及び関係機関への注意喚起

政策統括官付サイバーセキュリティ担当参事官室

Ministry of Health, Labour and Welfare of Japan

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。

出典：内閣官房国家サイバー統括室作成資料より
https://www.cyber.go.jp/pdf/press/20260518_AI_CS_gaiyou.pdf

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

出典：内閣官房国家サイバー統括室作成資料より
https://www.cyber.go.jp/pdf/press/20260518_AI_CS_gaiyou.pdf