Project YATA-Shield を踏まえた総務省の対応状況

資料6－3

➢ **所管分野代表との会合で、林大臣から対策強化を要請**（5月21日）。その後、各分野で具体的対応を実施。
- **情報通信分野**：**ICT-ISACにおいて、通信事業者が取り組むべき事項等をとりまとめ**、関係者に展開（6月30日）。
- **地方行政分野**：有識者会議を通じ、**リスクに応じた対応方針**を検討するとともに、**基本的なセキュリティ対策を確実に実施**していくことを確認。**全地方公共団体において情報資産の脆弱性管理に関する点検**を実施。

情報通信分野

ICT-ISACにおいて、通信事業者・業界団体等からなるWGを設置。

✓ ①フロンティアAIの**正しい理解**、②フロンティアAIの**活用方法**、③電気通信事業者として**取り組むべきことなど**を文書でとりまとめ。

✓ **攻撃スピード・規模の増大**を念頭に、**優先度**を付けて対応するとともに、大量パッチ対応等に必要な**予算・体制確保**等に向けた**経営層のリーダーシップ**の下での必要な対応も訴求。

＜電気通信事業者としての整理＞

整理事項	整理した考え方
正しい理解	• フロンティアAIにより、攻撃のスピード・規模が拡大するも、基本的対策が重要
活用方法	• リスク等を踏まえ守りでも活用
優先度の考え方	• 通信の可用性が最重要
必要な対応	• インターネット面・認証系等の対策を優先 • 通信の維持に係わる重要設備を保護 • 可用性確保のためBCPの具体化を検討

地方行政分野

＜リスクに応じた対応方針の検討＞

✓ **地方版ASMシステムの活用**
本年度に構築予定の地方版ASMシステムにより、地方公共団体が自ら診断システムを保有せずに外部公開IT資産における脆弱性を把握できるようにするとともに、総務省において情報を集約し、適切な対策に活用。

✓ **自治体システムの確認**
AI性能の高度化を踏まえた情報資産の脆弱性管理に関する点検を促すとともに、各団体においてリスクの状況を踏まえた必要な対策を検討。

＜基本的なセキュリティ対策の確実な実施＞

✓ **実効性の確保**
情報資産の脆弱性管理に関する点検を通じ、適正な脆弱性管理を促進。

✓ **セキュリティ・バイ・デザインの周知・啓発**
セキュリティ・バイ・デザインの手引書を作成し、今後周知。

✓ **人材育成支援**
自治大学校での特別研修の実施や実践的サイバー防御演習(CYDER)受講の推奨。

➢ その他、Project YATA-Shieldに基づく取組として、情報通信研究機構（**NICT**）とともに、

① 「**人材育成支援**」として、重要インフラ事業者等へ実践的サイバー防御演習（CYDER）を提供
※本年度は、全ての演習でフロンティアAIモデルへの対応について紹介するとともに、一部の演習では、その脅威も踏まえたシナリオを試行する予定

② 「**技術開発の推進**」として、ビッグテック等と連携した脆弱性の発見等に関する研究を推進
※NICT北米拠点において、複数の機能別AIエージェントを活用して脆弱性を自動で検知する技術（ファジング）を開発中