「ICTサイバーセキュリティ政策の中期重点方針」（案）の概要

資料10－2

➢ 総務省では、本年２月から「ICTサイバーセキュリティ政策分科会」（主査：後藤厚宏　情報セキュリティ大学院大学学長）を開催し、総務省が取り組むべきサイバーセキュリティ政策について、2030年頃も見据えた中長期的な方向性について検討。

【政府の主な動き】

- **国家安全保障戦略**
- **経済安全保障推進法の施行（特定社会基盤事業者の指定等）　等**

【サイバーセキュリティを巡る主な課題】

- **厳しさを増す国際情勢とサイバー攻撃リスクの高まり**
- **多様化・複雑化するサプライチェーンとアタックサーフェス（攻撃対象領域）の増加**
- **セキュリティ人材の確保**
- **生成AI等の新たな技術への対応**

１．重要インフラ等におけるサイバーセキュリティの確保

- 通信分野（総合的なIoTボットネット対策（新NOTICEの推進やC&Cサーバの検知・対処能力の向上）、スマートフォンアプリのセキュリティ対策やサプライチェーン対策の推進等）
- 放送分野（安全・信頼性に関する新たな技術基準に基づくセキュリティ対策の着実な推進等）
- 自治体分野（クラウド化・標準化等の環境変化を見据えた人材育成やCSIRT能力向上の取組等）
- クラウドセキュリティの確保やトラストサービス（eシールの認定制度を2024年度中に創設等）の推進

２．サイバー攻撃対処能力の向上と新技術への対応

- CYNEX・CYXROSSを強力に推進し、国産のサイバーセキュリティ情報・技術による自律的なサイバーセキュリティ対処能力を抜本的に強化
- CYXROSSとGSOCとの連携により政府システムの一元的な監視体制の構築に貢献
- CYDER等を通じた国や地方公共団体等におけるCSIRT対処能力の抜本的強化
- サイバーセキュリティ研究分野の国際競争力向上を図るため、NICT内に米国との連携を強化するための結節点を形成
- 生成AI等の新技術への対応（AIを起因とするセキュリティリスクの回避・低減に向けた取組、AIを活用したサイバーセキュリティ対策の促進、耐量子計算機暗号技術（PQC）等の研究開発等の推進）

３．地域をはじめとするサイバーセキュリティの底上げに向けた取組

- 地域SECUNITYの活動強化（他機関との更なる連携、持続的な推進体制の整備等）
- 各種ガイドラインの周知啓発等

４．国際連携の更なる推進（国際連携全般、人材育成支援）

- 日ASEANサイバーセキュリティ能力構築センター（AJCCBC）の活動強化（プログラムの拡充、有志国との連携強化等）
- 大洋州島しょ国向け人材育成支援プロジェクトの2025年度以降の本格的な実施