サイバーセキュリティ2025のポイント（「エグゼクティブ・サマリー」）

※1 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）
※2 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の施行に伴う関係法律の整備等に関する法律（令和７年法律第43号）

- 巧妙化・高度化したサイバー攻撃や国家を背景とした攻撃キャンペーン等により、国民生活・経済活動及び安全保障に対し、深刻かつ致命的な被害を生じさせるおそれがあることや、その標的・被害が急速に多様化・複雑化していることが、国内においても、これまで以上に顕在化。
- 政府においては、政府機関等のセキュリティ確保に係る取組や、近時のサイバー攻撃に係る注意喚起、脅威アクター対応からルールメイキングまで幅広に国際連携の強化を実施。
- サイバー対処能力強化法等※1 2（令和７年５月16日成立、同月23日公布）施行に向けた施策及び「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」に掲げられた施策を、2025年度の「特に強力に取り組む施策」に位置づけるとともに、新たなサイバーセキュリティ戦略を2025年内目途に策定。

2024年度における主な国内のサイバー攻撃事案

- 中国の関与が疑われるサイバー攻撃グループ「MirrorFace」による、安全保障や先端技術に係る機微情報の窃取を狙う攻撃キャンペーン
- 北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」による、暗号資産関連事業者からの暗号資産窃取
- 金融機関や地方公共団体等からの受託企業に対し、個人情報を漏えいさせたランサムウェア攻撃
- 出版事業等を行う大手企業に対し、提供するウェブサービスの停止や、書籍の流通事業等に影響を生じさせたランサムウェア攻撃
- 航空会社の国内便・国際便の遅延や、インターネットバンキングへのログイン障害等、複数の重要インフラ分野に対するDDoS攻撃　等

政府のサイバー攻撃への対応

- 政府機関等のセキュリティ確保に係る取組
  - アタックサーフェスマネジメント及びPDNSの導入による横断的監視の強化
  - 「政府機関等の対策基準策定のためのガイドライン」の一部改定
  - 生成ＡＩを含む約款型のサービス等の業務利用に係る注意喚起　等
- サイバー攻撃に係る注意喚起
  - Living Off The Land戦術等を含む最近のサイバー攻撃に関する注意喚起
  - MirrorFaceによるサイバー攻撃に関する注意喚起
  - DDoS攻撃への対策に関する注意喚起　等
- 国際連携の強化
  - 「TraderTraitor」に係る米国と共同のパブリックアトリビューション
  - 「APT40 Advisory PRC MSS tradecraft in action」の共同署名
  - イタリア議長国の下でのＧ７サイバーセキュリティ作業部会の設立・参画　等

特に強力に取り組むべき施策

サイバー対処能力強化法※1及び同整備法※2の施行に向けた施策

＋

「サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項」（2025年5月29日サイバーセキュリティ戦略本部決定）

- **新たな司令塔機能の確立**
- **巧妙化・高度化するサイバー攻撃に対する官民の対策・連携強化**
  官民連携エコシステムの実現
  政府機関・重要インフラ等を通じた横断的な対策の強化
  政府機関等のセキュリティ対策水準の一層の向上及び実効性の確保
- **サイバーセキュリティを支える人的・技術的基盤の整備**
  我が国の対応能力を支える技術・産業育成及び先進技術への対応
- **国際連携を通じた我が国のプレゼンス強化**

期限を設けて取り組むべきとされた事項

- **インシデント報告様式の統一**（本年10月から）
- **JC-STARの政府機関等における選定基準への反映**（本年度内）
- **官民共通の「人材フレームワーク」の策定**（本年度内）
- **脅威ハンティングの行動計画の基本方針の策定**（来年夏目途）
- **重要インフラ事業者等のサイバーセキュリティ対策に係る基準の策定**（来年度内）
- **中小企業の対策のための環境整備**（サプライチェーン強化に向けたセキュリティ対策評価制度は来年度内）
- **耐量子計算機暗号（PQC）の移行の方向性の検討**（本年内目途）

新たな『サイバーセキュリティ戦略』を2025年内目途に策定