AIを悪用したサイバー攻撃の脅威への対応に関する緊急提言

2026 年 11 月 4 日

一般社団法人 オープンガバメント・コンソーシアム

2026 年 9 月以降、国内外でサイバー攻撃や情報漏洩等が急増し、企業や行政機関等に深刻な影響を及ぼす事案が相次ぐ等、サイバーセキュリティを取り巻く状況は急速に悪化しています。特に、AI 技術の急速な発展・普及に伴い、攻撃手法の更なる高度化や攻撃活動の効率化・大規模化・高速化も懸念されています。

このような AI 技術を悪用した攻撃が現実化し、政府・地方公共団体や重要インフラ事業者を含めた全ての企業が標的となっている危機的な状況を踏まえ、一般社団法人オープンガバメント・コンソーシアム（OGC）は、会員組織・関係者に対して以下の緊急提言をいたします。

記

提言１： インシデント発生時の内部即応体制の義務化及び「能動的防御ライフサイクル」の確立等（*対象：政府、大量の情報資産を保有する事業者や機微な情報を取り扱う事業者、重要インフラ事業者、地方公共団体*）

- **セキュリティ運用・監視機能（CSIRT/SOC）の設置義務化**: インシデント発生時に即座に対応指揮・判断を行えるセキュリティ運用・監視機能の設置を関係法令等で義務付けること。
- **能動的防御ライフサイクルの構築**: インシデントの主因である「システムの脆弱性」「クラウド等の設定ミス」「ID・過剰権限」を継続的に特定・評価・是正する能動的防御ライフサイクルの構築を義務付けること。
  - 参考：米国国立標準技術研究所のサイバーセキュリティフレームワーク（CSF 2.0）の「統治」「特定」のライフサイクル要求、欧州 NIS2 指令（第 21 条）等の「定期的な脆弱性特定・パッチ管理・厳格なアクセス制御（最小権限の原則）の義務化」、米国サイバーセキュリティ庁(CISA)の「既知の悪用脆弱性の期日内是正義務」
- **柔軟な代替措置・連携支援制度の併設**: 人材確保が極めて困難な地方公共団体等に対しては、地域・業界単位での「共同 SOC/CSIRT」の組成や、信頼性が高くインフラを横断的に監視・脆弱性スキャンできる外部機能（マネージドサービス等）をもって、必要なセキュリティ水準を確保しつつ、上記義務を充足する代替措置として認める仕組みを整備すること。
- **サイバー防御の強化等**: その他、以下の方策を講じ、サイバー防御の強化及び利用者保護・救済に努めること。
  - AIを悪用した攻撃の脅威に備える
    - 外部公開資産を継続的に把握し、不要な公開を停止する／認証・認可の管理を強化する／SBOM 等も活用し、悪用される可能性の高い脆弱性を継続的に把握・評価し、優先的に修正する／AI 等も活用し、サイバー攻撃の兆候に対する監視・検知や初動対応を強化する／AI エージェントの権限と通信先を厳格に管理する
  - 攻撃・侵害を受けることを前提に対応力を強化する
    - インシデント対応手順と意思決定基準を事前に明確化する／サービス停止・機能制限の判断基準を明確化する／封じ込めと証拠保全の手順を確立する／事業継続と復旧に必要な備えを確保する／AI システムの制御逸脱に備えた対応手順を整備する

- 情報漏洩に適切に対応し、利用者保護・救済及び再発防止につなげる
  - ✧ 影響範囲を把握し、影響を受ける個人・組織に適切に対応する／事故原因と対応の課題を検証する／情報管理を見直し、不要な情報の保有を減らす／事故の教訓を組織全体の点検・改善につなげる／被害者支援と適正な情報保有に向けた制度整備を進める

提言2：地方公共団体等におけるリスクに応じた ISMAP 活用とクラウド情報管理の強化（*対象：地方公共団体及び関連組織*）

- **地方公共団体・関連組織等へのリスクに応じたクラウド調達基準の標準化**：地方公共団体及び関連組織において、取り扱う情報の機密性やリスクに応じ、ISMAP（又は ISMAP-LIU 等）に登録されたクラウドサービスを利用することを重要インフラ統一基準等で推奨・標準化すること。併せて、導入後の運用実効性を重視した柔軟な調達を可能とすること。
- **導入支援と運用の効率化**：ISMAP 登録サービスの選択肢拡充と審査プロセスの迅速化を進めるとともに、地方公共団体における適切なクラウドの選定、移行および運用管理に関する実務指針及び財政的支援を一体として提供すること。

提言3：個人情報保護ならびに経営ガバナンスの強化に向けた方策を講ずること（*対象：関係政府機関*）

- **データ最小化原則の義務化**：GDPR 第 5 条(1)(e)等で規定される「保管制限・データ最小化」原則を国内法上も明示的な義務とすること。
- **インシデント報告の運用厳格化**：インシデント発生時の監督官庁及び本人への報告義務を徹底する等、適切な事後対応を担保し、サプライチェーン全体への被害波及と二次被害を最小化すること。
- **役員責任（ガバナンス）の明確化**：CISO の配置や取締役会におけるセキュリティ監視を義務付けるなど、企業のサイバーセキュリティに関する統治責任を強化すること。
- **実効性確保**：上記対策の実装に当たっては、諸外国の制度を参考に、その対応の懈怠等に対する厳格な課徴金等の実効性確保のための措置を検討すること。

提言4：サイバーセキュリティ投資促進に係る税制優遇・予算措置の拡充（*対象：関係政府機関*）

- **運用費・人材育成を含めた特別税制**：セキュリティ機器・ソフトウェアの導入だけでなく、サイバーセキュリティ人材の育成費、外部専門家への運用委託費やサイバーセキュリティ機能の強化が困難なレガシーシステム更新についても税額控除や特別償却の対象とする「サイバーセキュリティ投資促進税制」を創設・拡充すること。
- **補助金・予算措置の拡充**：地方公共団体や中小企業が高度なセキュリティ基盤を導入・維持できるよう、国の財政措置を大幅に拡充するとともに、利用者が申請しやすいよう、省庁の枠組みを超えた情報提供に努めること。

提言5：サイバーセキュリティ関係の登録・認証制度の効率化（*対象：関係政府機関*）

- **サイバーセキュリティ関係の登録・認証制度の効率化**：ISMAP、JC-STAR、SCS 評価制度等、審査項目等が重複するサイバーセキュリティ関係の登録・認証制度の一括申請・審査など、申請者側の負担軽減に努めることで、制度の一層の活用を促進すること。

以上