

サイバーセキュリティ対策の抜本的強化に関する提言

～サイバー有事前夜／AIのサイバー飽和攻撃に備えよ！～ 概要

令和8年10月20日 自由民主党政務調査会 国家サイバーセキュリティ戦略本部

はじめに（基本認識と危機感）

- ・我が国の企業等に対するサイバー攻撃により個人情報の流出事案が急増。国民のプライバシーと財産が著しく脅かされており、不安が広がっている。今後これまでも影響の大きな事態が発生することも否定できない「サイバー有事前夜」とも言うべき重大な危機。
- ・重要インフラ企業に限らず、重要情報を大量保有する企業での対応強化も必要。
- ・生成AI等の急速な発展と普及に伴い、サイバー攻撃はより自律化・高度化しつつある。
- ・ゼロトラスト思想への転換、最先端技術の社会実装、平時からの積極的なサイバー防衛網の構築が急務。
- ・必要な予算確保と体制整備の実施。

政府全体に対する基本提言

官邸主導で「サイバー対処本部（仮称）」を立ち上げ、司令塔として迅速に本部会議を開催。不安の払拭へ。

（１）サイバー対処能力強化法の取組強化

自衛隊・警察の能力構築、官民協議会の活用、通信情報の利用、同盟国連携の加速

（２）経営層の意識改革と開示の充実

経営の最重要課題とし、平時からの体制構築を促す

（３）人材の育成・確保

「トップガン」人材の待遇のため、公務員の新たな人事・給与制度、実践演習を通じた人材の裾野拡大

関係省庁に対する個別提言

● NCO（国家サイバー統括室）

- ✓能動的サイバー防御の実行体制構築
- ✓サイバー攻撃情報の集約・分析及びインシデント対応力の強化
- ✓Project YATA-Shieldの推進（防御側もAI技術活用）
- ✓米国のAI事業者との連携
- ✓政府調達における対策強化
- ✓同盟国・同志国とのインテリジェンス共有
- ✓指揮権の発動
- ✓漏洩被害者への安全な連絡方法の確立
- ✓PQC（耐量子計算機暗号）移行の加速

● 内閣府AI室/AISI

- ✓産業界の安全なAI実装に向けた指針改訂
- ✓Project YATA-Shieldの推進
- ✓米国フロンティアAI事業者等との戦略的連携

● デジタル庁

- ✓ゼロトラスト思想の徹底とガバメントクラウドの厳格な監査
- ✓マイナンバーカードの利用による本人確認の徹底（マイナンバーカードの取得の義務付けの検討等）
- ✓次世代認証基盤（DID/VC）及びマイナンバーカードの活用

● 経済産業省及び金融庁等

- ✓上場企業等の開示の充実（サイバーセキュリティに関する重要事項の有価証券報告書への記載の充実）
- ✓経営ガイドラインの厳格化
- ✓サプライチェーン防衛への投資支援と「サイバーお助け隊サービス」の拡充
- ✓サプライチェーン観測網の導入
- ✓ホワイトハッカーをはじめとするセキュリティ人材の育成と、AIを活用したペネトレーションテストの実現
- ✓OTシステム特化型サイバーセキュリティAIの開発と秘密計算技術の実装による安全なデータ利活用（重要データを暗号化したままクラウド上で処理）
- ✓事業者におけるAIエージェントの安全な利活用に向けたガイドライン作成
- ✓ベンダーの対応能力、クライアント企業への支援能力の向上
- ✓信用情報機関への通報のワンストップ化の仕組みの整備の検討
- ✓金融分野における官民連携、防御力及びレジリエンスの強化
- ✓IoT製品やセキュリティ事業者のセキュリティ対策状況可視化

● 個人情報保護委員会

- ✓不正アクセスに関する個人情報保護法の厳格な執行（必要な場合の報告徴収、立入検査、勧告・命令）
- ✓保有する個人データの最小化
- ✓罰則の広報啓発
- ✓漏洩被害者への安全な連絡方法の確立

● 警察庁

- ✓攻撃者の特定能力の抜本的強化と体制拡充
- ✓国際共同捜査による犯罪インフラの無害化の主導
- ✓被害組織が相談しやすい環境整備等
（事業者等との信頼関係の醸成及び協力関係の構築）
- ✓個人情報漏洩事案における2次被害対策の徹底
（「警察庁推奨アプリ」の活用の周知）

● 総務省

- ✓通信事業者による対策の強化
- ✓NICTによる研究開発等の推進（サイバー攻撃手法の分析と周知）
- ✓機器の踏み台化等の防止
- ✓地方公共団体による対策と国による支援
- ✓量子暗号通信（QKD）の社会実装の加速

● 防衛省

- ✓「能動的サイバー防御（ACD）」を含むサイバー防衛能力の強化
- ✓重要インフラ等のシステムへの支援も見据えたスレット・ハンティング機能の強化
（自衛隊の任務遂行に不可欠な重要インフラ等システムの防護）

● 厚生労働省

- ✓医療現場におけるサイバー防衛の標準装備化
- ✓医療現場における専門人材の活用
- ✓重要インフラにふさわしい防御力の整備

● 消費者庁

- ✓消費者への注意喚起

● 国土交通省

- ✓重要インフラの安定的なサービスの確保

【おわりに】～国民の安全と我が国の産業競争力を死守する責務～

■サイバー空間の優劣は、国力を左右

来るべき「AIのサイバー飽和攻撃」を前に、政府は直ちに必要な予算措置及び法制化の検討に着手し、国民の安全と我が国の産業競争力を死守する責務がある。

■国内通信情報の利用検討を含む強い対応

サイバー対処能力強化法における外国関連通信情報の利用にとどまらず、国内通信情報の利用の検討も求める。