別紙１

サイバーセキュリティ緊急対策パッケージ

サイバーセキュリティに関する関係閣僚会議決定
令和８年 11 月６日

昨今、サイバー攻撃による不正アクセスや情報漏えいの事案が相次ぎ、国民生活や企業活動に大きな不安と影響が生じている。昨今の漏えい事案では、既知の脆弱性の放置、ウェブサイト等の設定不備、アプリケーション開発時のセキュリティ対策の不足などにおいて、自組織又は委託先における基本的な対策が十分でなかった事例が多くみられる。AI の進展により、こうした隙が短時間かつ大規模に突かれる時代となっている。これは特定の組織や業界に限らず、我が国社会全体で対応すべき課題である。

我が国が目指すべきは、あらゆる組織が基本的な対策を当たり前に講じることで被害を予防することができ、仮にサイバー攻撃による被害が生じたとしても、官民が攻撃の情報を共有していち早く対処し、迅速に支援を受けて立ち直ることができる世界最高水準のサイバーレジリエンスを確保した社会である。

その実現に向け、既に一部の取組を先行して実施したところであり、さらに、政府一丸となって、被害を予防する AI も活用した基本的な対策の徹底、情報収集・集約や捜査・分析体制の強化、サイバー攻撃への対処の戦略的な実施、被害者支援・被害拡大防止策の強化に一体的に取り組む。あわせて、情報収集の在り方を含む制度面の整備、政府の基準の見直し、ベンダとその契約事業者のシステム関連契約の在り方の周知、政府システム等のサプライチェーンにおけるリスク点検とこれを踏まえた対応、高性能 AI のサイバー攻撃への悪用や量子技術の進展など将来の脅威への備えといった中長期的な課題についても検討を深め、官民一体となって我が国全体の対処能力を不断に高めていく。

本パッケージは、その第一歩として、早期に実施又は着手できる施策を中心に、４つの柱の下に取りまとめたものであり、AI 時代にふさわしいサイバーセキュリティの在り方へと我が国を移行させていく出発点である[1]。

施策の実施に当たっては、必要な財政措置を確保するとともに、司令塔である国家サイバー統括室をはじめ、警察、防衛省・自衛隊及び関係省庁における人員等の体制を、民間人材の活用を最大限進めつつ強化する。関係省庁は、施策の進捗状況を国家サイバ

[1] 別添の施策一覧は、中長期的な課題も含めて、実行・検討していくものである。

一統括室に報告し、国家サイバー統括室は、それに基づき関係省庁への情報共有や必要な施策の推進を促す。政府は、関係省庁が一体となって、本パッケージに盛り込んだ施策の実行にスピード感をもって取り組む。

１．AI も活用した基本的な対策の徹底

昨今の漏えい事案の多くは、既知の脆弱性への対応、適切な設定、開発時や委託先の管理といった基本的な対策の徹底により、被害を防止・軽減することが可能となる。また、AI の活用により、脆弱性の発見から攻撃までに要する時間が短縮し、さらに未知の脆弱性が攻撃に活用される可能性も踏まえれば、個人情報を必要以上に保有しないといった被害の規模を抑える対応も必要である。

政府や重要インフラについては、これまでも基本的な対策の徹底を求めてきたところであるが、昨今のサイバー攻撃による不正アクセスや情報漏えいの事案が相次いでいることに鑑み、政府・地方公共団体・企業を問わず、発注者・委託先・経営層それぞれが責任を持ち、基本的な対策を「当たり前」に講じる。あわせて、万一侵入されても被害を最小限にとどめられるよう、保有する情報を必要な範囲に絞る。こうした意識を社会全体に根付かせる。

このため、基本的対策の徹底、サイバー攻撃を受けた場合の被害最小化のための取組、AI を活用した脆弱性の発見と対策等を推進していく。具体的には、以下に取り組む。

（１）最近の情勢を踏まえた注意喚起の実施

ウェブサイトやモバイルアプリに関する基本的な対策の徹底を事業者に呼び掛けるため、運用・管理段階におけるセキュリティ対策、設計・開発段階におけるセキュリティ対策、サプライチェーンを通じた侵害への対策についての注意喚起を発出する。【国家サイバー統括室】

（２）保有する個人データの最小化と安全管理の強化

個人情報保護委員会は 10 月７日、事業者に対し、保有する個人データの必要性の確認と不要なデータの消去について注意喚起を行った。今後、本人確認のために取得した画像等の保存に関する基本ルールについて、令和８年度中に業種ごとの注意喚起等を検討する。あわせて、安全管理措置に関するガイドラインの改正を加速し、令和９年１月中の施行を目指す。【個人情報保護委員会】

（３）マイナンバーカードの活用による安全な本人確認の徹底

運転免許証の画像による本人確認については、国民が不安を感じているところ、民間や行政でのマイナンバーカード等に格納された IC チップの読取による安全かつ確実な本人確認の利活用場面の拡大を進める。その際、その裏付けとなる認証基盤であるデジ

タル認証サービス等のシステムのセキュリティ等の強化を図る。【デジタル庁・関係省庁】

（４）AI を活用した脆弱性の発見と対策等

AI を活用して、民間企業、政府機関、地方公共団体など、社会全体での脆弱性の発見と対策等を進める。具体的には、以下に取り組む。

①　トップガン人材チームの立上げ

独立行政法人情報処理推進機構（IPA）において高性能 AI の活用環境を整備するとともに、模擬的な攻撃テスト（ペネトレーションテスト）を実施し積極的なセキュリティ対策強化を行うトップガン人材などからなるチームについて、人材の信頼性確保にも配慮しつつ 11 月中に立ち上げる。同チームにおいては、自らによる実施とともに、民間企業への支援を担うセキュリティ企業に対し、ペネトレーションテストを行うための人材育成や AI を活用した検証環境の提供に取り組むほか、テストに必要となるツール等の開発・提供も進めていく。【経済産業省】

②　政府システムの脆弱性の検証の前倒し等

政府の情報システムについて、システムを構成する機器やソフトウェアの把握・管理の徹底を図り、AI を活用した脆弱性診断を前倒しできるものについては可及的速やかに実施し、判明した事項に早急に対応する。

また、ガバメントソリューションサービス（GSS）やデジタル認証サービス、マイナンバー情報連携システムなどを含む政府の重要な共通業務システムにおけるガバメントクラウドの活用や総合的な運用監視体制の強化等により、政府システムのセキュリティ基盤を速やかに強化し、セキュリティ・安全性や事業継続性を一層高める。【国家サイバー統括室・デジタル庁・関係省庁】

③　地方公共団体の緊急対策と全団体へのサポート体制

総務省から地方公共団体に対し、①委託先が提供するものを含む全てのウェブシステム等とそのセキュリティ対策を把握すること、②多要素認証の導入や保有情報の最小化など、基本的な脆弱性対応を徹底すること、③AI を活用した脆弱性診断を行い、対策の完了までは一時的なサービスの停止も検討することを要請する。

あわせて、地方公共団体が AI モデルを活用した脆弱性診断等を行うことができるよう、高度な専門能力を持つ専門事業者等と連携した「自治体サイバーセキュリティサポートチーム」を構築し、全ての団体の取組を支援する。【総務省】

④　高性能 AI モデルの評価等

AI の実装を前提としたサイバーセキュリティを進めるため、AI セーフティ・インスティテュート（AISI）の機能を強化し、活用する。国内外の AI 開発事業者等との協力や英国 AISI との情報共有枠組の構築により、高性能な AI モデル等のサイバー攻撃性能を迅速に評価し関係者に共有する。AI 関連のインシデントへの対応体制に関する指針等を速やかに更新する。【内閣府】

２．情報収集・集約、捜査・分析体制の強化

政府に情報が集まる経路を広げ、攻撃の兆候を先回りして探り、手口を分析する能力を高めるとともに、集約・分析した情報を、被害組織への支援や国民・事業者への注意喚起、攻撃への対処の手段の検討に速やかに活用することで、社会全体のサイバー対処能力の向上につなげていく必要がある。

昨今の漏えい事案では、政府機関や重要インフラ事業者等に限らず、幅広い分野・規模の事業者が被害に遭っている状況を踏まえれば、官民の攻撃情報を国家サイバー統括室を中心に関係省庁が連携して迅速に収集し、AI も活用して分析の上、その結果を社会に還元する循環が常に機能する仕組みを確立する。具体的には、以下に取り組む。

（１）セキュリティベンダ等からの情報収集の強化

攻撃対処の最前線で多数の攻撃情報を有するセキュリティベンダや、ISMAP に登録されたクラウドサービスを提供するクラウド事業者等に対し、サイバー協議会への参加と連携の強化を促し、脅威や事案の情報収集・分析等を行う。また、海外の大手デジタル企業やフロンティア AI 企業等との協力関係を拡大・深化させ、攻撃関連情報や公表前の脆弱性情報を早期に入手することで、分析と対策の検討を加速させる。【国家サイバー統括室・総務省】

（２）被害を受けた事業者からの迅速な情報集約

関係省庁は、個人情報の漏えいなど重大な被害が生じている事案について、被害を受けた事業者から迅速に情報を収集し、国家サイバー統括室に報告する。また、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（令和９年３月頃に運用開始）において、評価を取得した企業が被害に遭った際に関係情報を求めることが可能な仕組みを導入する。【国家サイバー統括室・経済産業省・関係省庁】

（３）サイバー攻撃分析能力の強化

国内で相次ぐ情報漏えい事案の原因の一つである「A2B 攻撃」を特定した国立研究開発法人情報通信研究機構（NICT）の分析能力を強化し、国家サイバー統括室や関係機関と連携して、政府全体の分析能力を令和８年度内に向上させる。あわせて、AI エージェントによる攻撃も安全に再現・分析できる環境の構築に着手し、令和８年度中に設計に

取り組む。得られた知見は関係機関・事業者と共有し、早期検知と防御策の高度化につなげる。【総務省】

（４）サプライチェーンセキュリティの強化

サプライチェーン企業へのサイバー攻撃を早期に発見・対応するとともに、他の企業へと連鎖させないよう、IPA において NICT とも連携しつつ、攻撃を 24 時間 365 日監視する観測網の実証事業を年始目途で開始する。

【国家サイバー統括室、経済産業省、総務省】

（５）被害企業からのログ等の確実な収集による捜査・実態解明の更なる推進

捜査・実態解明を通じた将来の被害防止の観点から、サイバー攻撃に関するログ等の証拠を収集すべく、警察、内閣官房及び所管省庁が連携し、所管企業等から通報や証拠の提供が得られるよう、必要な要請を行う。【国家サイバー統括室・警察庁・関係省庁】

３．サイバー攻撃への対処の戦略的な実施

高速化・大規模化するサイバー攻撃に追いつくためには、被害が顕在化する前に、サイバー攻撃を把握し、対応する必要がある。また、攻撃の基盤が残る限り、被害は続くおそれもある。

政府は、２．で把握した攻撃の実態等の情報を踏まえ、「アクセス・無害化措置」も含めた様々な対処オプションを戦略的に実施していくとともに、同盟国・同志国と連携して、攻撃者に対しコストを賦課し続ける環境を整備することが必要である。

このため、重大な事案への政府一体の対応を始動させるとともに、攻撃の基盤に対してあらゆる手段を戦略的に講じ、国際的な連携を強化する。具体的には、以下に取り組む。

（１）サイバー攻撃事案への官民一体となったシームレスな対応

潜在的な被害へのおそれがある場合、政府による支援が必要な場合、重大なサイバー攻撃が発生した場合、中小企業が被害に遭った場合について、官民それぞれの能力を活用し、シームレスな対応を行う。具体的には、以下に取り組む。

①　潜在的なサイバー攻撃被害のおそれがある場合

攻撃情勢の分析等に基づき、潜在的な被害のおそれがある組織に国家サイバー統括室から能動的に接触する「アウトリーチ・チーム（仮称）」を今月中に新設する。同チームは、不審な動向や対策状況の確認、必要な助言、脅威ハンティングの調整等を行い、まだ気付いていない侵害の早期発見と対策を促す。

②　サイバー攻撃被害のうちで政府による支援の必要性が特に認められる場合

国家サイバー統括室は、認知したサイバー攻撃事案について、民間の専門機関とも連携しつつ、被害組織から支援の要請があり、かつ、被害の状況、攻撃の背景・手法、被害組織による対策状況等を踏まえてその必要性・緊急性等が特に認められる場合には、官民の専門人材から構成される「官民サイバー救援隊（仮称）」を被害組織に機動的に派遣して、初動対応を支援する仕組みを速やかに整備する。

このため、令和８年度中の早期に国家サイバー統括室内に事務局を設置した上で、派遣の開始に向けた準備を加速する。

③　重大なサイバー攻撃被害が発生した場合

②のサイバー攻撃事案のうちで、国民の生命、身体又は財産に対する重大な危害が現に発生し又はそのおそれが大きい事案であって、我が国の安全保障や社会経済に重大な影響を与える場合については、国家サイバー統括室、所管省庁、警察、防衛省・自衛隊等からの職員で構成するジョイント・レスポンス・チーム（仮称）を被害組織に派遣した上で必要な支援等を行う運用について、令和８年度中の早期に開始する。

同チームは、国家サイバー統括室が国家安全保障局と緊密に連携した上で行う総合調整の下で、被害組織の同意を得て派遣して、政府一体で対応することで、複数回の聴取を避けるなど被害組織の負担を軽減しながら、被害状況の確認、必要な支援の聴取、助言、脅威ハンティングの検討、早期復旧に向けた調整等を行う。

④　得られた知見の活用と警察との連携

①から③までの個々の対応で得られた知見については、政府における情報の集約・分析にも活用するほか、対策の改善等に還元して、社会全体の防御力の強化につなげる。

また、これらの対応に際しては、警察庁を通じて、都道府県警察や、これを支援し事案発生時のログの保全や早急な原因究明等の初期対応を担うために新たに警察に設置されるファスト・フォレンジック・フォース（仮称）と緊密に連携した上で、証拠保全その他の捜査上の初動的な措置が迅速かつ適切に確保されるようにする。

⑤　中小企業等がサイバー攻撃被害にあった場合

これらに加え、中小企業等がサイバー攻撃被害にあった際に、一定の基準を満たす専門事業者が現場で初動対応を支援する「サイバーセキュリティお助け隊サービス」について、復旧やバックアップ等の支援メニューを追加する。これにより、初動対応から復旧、その後の備えまで一貫して支援できるようにする。

【国家サイバー統括室・内閣官房・警察庁・防衛省・経産省・関係省庁】

（2）政府主導の脅威ハンティング

侵害された場合に社会への影響が大きい事業者等に対し、攻撃の痕跡を能動的に探索する「脅威ハンティング」の実施を働き掛ける。年内を目途に、サイバー協議会を通じて国家サイバー統括室からマニュアルや検知ツールを提供する。あわせて、専門機関や民間セキュリティ事業者の知見を活用した支援の仕組みを構築し、国家サイバー統括室の総合調整の下、事業者等からの要請に応じて警察・自衛隊も実施・支援する。得られた情報は、攻撃の分析に活用する。【国家サイバー統括室・警察庁・防衛省】

（3）攻撃の基盤への対処

国家サイバー統括室の総合調整の下、集約・分析した攻撃の実態を関係省庁間で共有・協議し、アクセス・無害化措置を含むあらゆる対処の手段を戦略的に選択・実行する。また、捜査で把握した攻撃インフラについて、関連事業者と連携してテイクダウンを進める。あわせて、攻撃の踏み台として悪用される国内の機器への対策を年内に取りまとめ、必要な対応を行う。【国家サイバー統括室・内閣官房・警察庁・防衛省・総務省】

（4）同盟国・同志国の関係機関との「顔の見える関係」の構築

国際共同捜査やパブリック・アトリビューション等の国際社会一体となった取組を推進するため、国際会議への積極的な参画、共同訓練等を通じて、外国のサイバーセキュリティ当局や捜査機関その他の関係機関との「顔の見える関係」を構築する。こうした信頼関係や相互理解を基盤として、攻撃者の特定やテイクダウン等の被害拡大防止措置のため、必要な情報連携や捜査協力を機動的に実施する。【国家サイバー統括室・警察庁】

4．被害者支援・被害拡大防止策の強化

情報漏えい等の被害に遭った個人や企業においては、被害に遭っても、何が起きたのか、どこに相談し何から手を付ければよいのかが分からず、孤立したまま対応を迫られている状況にある。また、漏えいした個人情報を悪用した詐欺電話やフィッシング、なりすまし、事案に関する偽・誤情報の拡散などの二次被害は、今後も事案のたびに起こり得る。被害に遭った組織を孤立させず、身近な相談先と専門家の支援によって早期に事業を再開できる環境を整えるとともに、国民一人一人が正しい情報に基づいて自らを守れるようにすることが必要である。

そのため、当面、身近な相談先と専門家による直接支援を拡充し、被害に遭った組織や個人が迷わず支援につながる体制を整えるとともに、二次被害を防ぐための発信等を強化する。併せて、官民の専門人材を機動的に派遣する全国的な仕組みの構築に着手す

る。具体的には、以下に取り組む。

（１）相談・通報窓口の全国整備と一元的な案内

事業者向けには、警察における法人の被害に関する専用窓口による相談・通報の受付を開始することに加え、IPA・よろず支援拠点等による無料相談や、業所管省庁による分野ごとの相談窓口を設けた。個人向けには、地方公共団体の消費生活センター（188）を総合的な入口とし、個人情報流出の被害に遭われた方や不安のある方向けに相談内容に応じた各種相談窓口の案内を官邸ホームページでも行っている。国家サイバー統括室を中心に、共通の対処手順や最新の手口情報等を各窓口と共有し、窓口間で連携することにより、相談者がどこに相談しても適切なサポートが得られる体制を整える。

加えて、全国約 6 万人のデジタル推進委員がサイバーセキュリティに関しても研修を受講して知見を強化し、デジタルに不慣れな方々に対して新たにセキュリティに関しても助言・支援等を行う。【国家サイバー統括室・内閣官房・デジタル庁・警察庁・総務省・経済産業省・消費者庁・関係省庁】

（２）国民・事業者に向けた情報発信の強化

経営層、セキュリティ専門家、国民といった対象ごとに、例えば、経営層には事案の影響の大きさや切迫度、専門家には直ちに対策を講じるべき技術的な対応など目的に応じて明確に情報発信を行う。また、10 月 30 日に、国家サイバー統括室が「サイバー対応特設サイト」を開設した。このサイトを活用し、相談窓口や注意喚起など必要な情報を一元化し分かりやすく案内するなど、情報への導線を設定し、必要な情報が受け手に確実に届くようにする。【国家サイバー統括室・関係省庁】

（３）二次被害、偽・誤情報の防止

漏えいした個人情報を悪用した詐欺やなりすまし、国外に由来するものも含め特定の業界に関する根拠のない情報の拡散などによる二次被害を防ぐため、政府が集約・分析した攻撃の手口等の情報も踏まえ、国家サイバー統括室と業所管省庁が連携して、注意喚起や正確な情報を迅速に発信するなど必要な対応を行う体制を強化する。発信に当たっては、個人向けの相談窓口の案内と連動させ、不安を抱える方が具体的な相談・対応につながるようにする。加えて、漏えいした個人情報等の悪用等を防ぐため、通信事業者によるアクセス抑止策の在り方について法的課題を含め早急に検討する。あわせて、二次被害の防止や、社会の混乱を招く偽・誤情報から影響を受けないようにするための注意喚起・周知広報を推進し、偽・誤情報に対する社会の対応力を高める。【国家サイバー統括室・内閣官房・内閣府・総務省・関係省庁】