併せて、地方公共団体が実際に 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脆弱性診断事業者やデジタル専門人材と連携し、全団体をカバーするサポート体制（「自治体サイバーセキュリティサポートチーム」）を構築し、実務に即した情報提供や必要な支援を行う。

【総務省】

（12）AI の実装を前提としたサイバーセキュリティ対策の強化：AI の実装を前提とし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 開発事業者等とも協力し、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、その結果をサイバー協議会等で共有する。また、令和８年１月に公表した AI システムで発生するインシデントへの対応体制の構築のための指針をまとめた文書を更新するとともに、英国 AISI との間での AI の重大な悪用事例に関する情報共有の枠組みの構築を目指す。【内閣府】

（13）通信事業者のサイバーセキュリティの強化：インフラ中のインフラを担う通信事業者におけるデータの保護やセキュリティに関する包括的な検討を行い、必要となる制度整備等を行う。特に、電気通信分野の中小事業者に対して伴走的な支援を行うため、中小企業の IT 資産の把握・更新、設定の不備やパッチの適用状況等の脆弱性診断、暗号化・多要素認証の実装を支援するためのガイドラインの策定等を行い、サイバーセキュリティ対策の実施を促す。【総務省】

（14）電気通信分野における対処能力の強化：国立研究開発法人情報通信研究機構（NICT）において、令和８年度内に、電気通信事業者を主な対象として高度な脆弱性検知能力をもつ人材の育成を行うとともに、実践的サイバー防御演習（CYDER）を追加して実施することにより対処人材の育成を加速し、電気通信分野の対処能力の強化を図る。【総務省】

（15）医療現場における専門人材の活用・対策能力向上：医療分野において、IPA の「サイバーセキュリティ対策支援者リスト」等を活用することで、外部専門人材の活用による専門知見・技術の補完を推進する。また、医療現場における人材活用と能力向上を推進するため、医療従事者や医療機関の経営層等の特性に合わ

せた実践的な研修を企画運営し、実際の医療機関におけるサイバー攻撃を想定したBCP訓練を含めた攻防演習、人材育成、指導者育成を実施する。【厚生労働省】

(16) 医療機関向け支援基盤・研修等の活用促進：医療従事者向けのサイバーセキュリティに関するオンライン研修コンテンツについて、医療機関等向けポータルサイトを通じて一層の周知を図る。また、サイバーセキュリティインシデントの疑いが生じた際の初動対応を支援するため、厚生労働省が運営する相談窓口等について改めて周知を行う。また、関係省庁において整備された被害企業等への支援策や、IPAや警察の相談窓口についてあわせて周知する。【厚生労働省】

(17) 医療現場におけるサイバー防衛標準化に向けた支援：医療機関におけるサイバーインシデントに特徴的な外部からの攻撃ルートの把握や、そのルートとなる情報資産管理を行い、各医療機関、特に規模が大きく診療機能が停止した際の影響が大きい医療機関におけるセキュリティ対策の現状把握を加速する。それらを踏まえ、医療機関の特性に応じた侵入経路の集約化・適正化等の戦略的な対策支援を迅速かつ着実に実施する。【厚生労働省】

(18) 学校における高いセキュリティ基盤の構築：教育委員会及び学校は、児童生徒や教職員に関する個人情報を取り扱う組織であり、学校の情報セキュリティを強化し、児童生徒や教職員が安心してAI等のデジタル技術を利活用できる環境を整えることが不可欠であることから、「教育情報セキュリティ・ポリシーに関するガイドライン」の改訂や教育委員会における教育情報セキュリティ・ポリシーの策定推進、セキュリティ対策の実施に係る支援を通じ、学校の高いセキュリティ基盤の構築を図る。【文部科学省】

(19) 大学等における情報セキュリティ体制の基盤構築・人材育成：日本全国1,000以上の大学や研究機関等の教育・学術情報の基盤として、国立情報学研究所（NII）が、「学術情報ネットワーク（SINET）」上にサイバー攻撃を観測・検知・分析するシステムを構築し、大学等と連携することで、サイバーセキュリティ人材育成等の取組を引き続き実施する。また、大学等の経営層・学生を対象としたセキュリティ教育の充実を図るとともに、大学等が保有する情報システムにおいて、特に重要度の高いシステムを対象として、AIを悪用したサイバー攻撃を想定した脆

弱性診断やペネトレーションテストを実施する。これらの取組によって、大学等におけるサイバーセキュリティ対策の強化を支援する。【文部科学省】

(20) TOSの脆弱性診断、サイバー攻撃に対する訓練：港湾におけるサイバーセキュリティ対策の強化を図るため、港湾運送事業者が使用するターミナルオペレーションシステム（TOS）の脆弱性を診断し、その結果を踏まえ適切な対策を講じるための助言を実施するとともに、港湾運送を取り巻く関係者全体で、TOSの支障発生時の態勢を確認する訓練を実施する（五大港のうち、京浜港及び名古屋港については令和７年度に実施済み、大阪港、神戸港、博多港については、令和８年度中に実施予定）。【国土交通省】

(21) 大規模インフラ障害への対応に係る机上演習：サイバー攻撃の影響が、情報流出やサイバー空間におけるものを越えて、電力・通信・水道等の物理インフラに波及し、国民生活・経済活動に甚大な被害が生じる可能性があることを踏まえ、国、地方公共団体、及び主要インフラ事業者において、社会的影響が特に深刻な大規模インフラ障害のリスクを評価し、官民合同演習を実施する。【内閣官房】

(22) 国民生活・経済活動の基盤となる重要なインフラの安定的なサービス確保：アタックサーフェスマネジメント（ASM）により、インターネット上に公開されている情報資産の脆弱性やリスクを継続的に把握・可視化し、その結果を事業者等に速やかに共有することで、サイバー攻撃の脅威への迅速な対応を促進する。併せて、交通ISACと等連携した経営層や中小事業者を含む幅広い層との官民対話の実施や、港湾運送事業者、専門家、国土交通省等で構成される「港湾運送分野セキュリティ連絡会」を活用した情報共有・相互連携の強化等により、サイバーセキュリティを巡る最新の動向を共有し、官民が一体となった業界全体のサイバー対処能力の向上を加速させる。【国土交通省】

(23) 重要インフラ統一基準に基づく重要インフラ事業者等の自己評価「CI-CSA」の実施：重要インフラ統一基準に基づき、全ての重要インフラ事業者等を対象とした自己評価「CI-CSA」※を実施し、自己点検の促進と実態把握を図る。その際、各種の注意喚起等とCI-CSAの対策事項との対応関係をまとめて周知することにより、各重要インフラ事業者等が注意喚起等の実施状況を自らチェックすること

を可能とする。【国家サイバー統括室】

※　CI-CSA（Critical Infrastructure Cybersecurity Self-Assessment）は、政府機関による重要インフラ分野の取組状況の把握に加え、事業者自らが自己評価やギャップ分析、優先順位の明確化等を行い、継続的なセキュリティ水準の向上を図るもの。

２．情報収集・集約、捜査・分析体制の強化

（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に対し、令和８年 10 月に発足したサイバー協議会への参加と連携の強化を速やかに働きかける。あわせて、総務省と連携し、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て、同様にサイバー協議会への参加と連携の強化を促す。さらに、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。これらの取組により、被害企業の対応現場への負担に配慮しつつ、幅広い地域・業種を対象とする攻撃関連情報を早期に国家サイバー統括室（NCO）に収集・集約するとともに、攻撃被害の全体像や発生しうる連鎖被害等についての的確かつ迅速な状況認識を実現させ、さらに、情報の収集・集約を超えて、その後の攻撃情報の分析と対処まで含む官民の連携体制を構築する。【国家サイバー統括室・総務省】

（２）事業者からの被害情報収集：重大な被害が生じている事案について、所管省庁において「重要インフラのサイバーセキュリティに係る行動計画」に基づく重要インフラの情報共有制度と同様に、迅速に情報を収集し、NCOに報告することで、NCOへの情報収集・集約の徹底を図る。【国家サイバー統括室・関係省庁】

（３）被害企業からの証拠の確実な収集による捜査・実態解明の更なる推進：サイバー攻撃による被害を将来にわたって防止するためには、捜査を通じて攻撃主体や手口等の実態を解明することが必要不可欠である。捜査・実態解明のためには、サイバー攻撃に関するログ等の証拠を収集することが必要不可欠であることか

ら、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】

（４）企業のセキュリティ対策状況を評価し、企業間の取引において共通の尺度として活用できる「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」を令和９年３月から開始し大企業の委託先管理手法として推奨する。また、サプライチェーン企業の弱点となりやすい中小企業への取組として「サイバーセキュリティお助け隊サービス」を拡充する。また、制度について国内外の情勢変化に応じて機動的に見直しを行う。【国家サイバー統括室・経済産業省】

（５）サイバー攻撃分析能力の強化：国内で相次ぐ不正アクセスによる情報漏えい事案の原因の一つである「A2B攻撃」※を特定したNICTのサイバー攻撃分析能力を強化し、サイバー対処能力強化法の枠組みも活用し、NCOや関係機関と連携しつつ、政府全体の分析能力を向上させる（令和８年度内に実施）。

また、複数の AI エージェントが自律的に連携して外部システムを侵害するなど、新たな脅威に対応するため、NICTにおいて、人による攻撃に加え、AI エージェントの連携、制御回避、外部への脱出等の AI エージェントによる攻撃も安全に再現・観測・分析できる「STARDUST Bed」の構築に着手する。得られた攻撃経路・通信・操作等の知見を関係機関・事業者と共有し、情報漏えいの原因分析、早期検知、防御策の高度化につなげる。【総務省】

※　App-to-Backend Attack攻撃。一般に公開されているアプリを解析し、その情報を悪用してアプリの接続先であるバックエンドサーバを攻撃する手法のこと。

（６）SCS評価制度における企業等からの情報収集： NCOと経済産業省が構築中の「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」（SCS評価制度）において、令和９年３月頃の運用開始後、「★」を取得した企業等がサイバー攻撃を受けた場合に、NCOから「★」取得企業に対して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】

（７）サプライチェーンセキュリティの強化：異常検知を早期の対策に繋げるとともに、他の参加企業への攻撃の連鎖を防ぐなど AI を活用したサイバー攻撃から

中小企業を守るため、IPAはサプライチェーン企業が参加する攻撃観測網を導入し、人間の専門家に代わって24時間365日監視する実証事業を令和９年始目途で開始し、NICTが実施する観測事業から脅威情報の共有を受けるなど、IPAとNICTが連携しつつ取組を進める。【総務省・経済産業省】

（８）サイバー協議会における官民連携の情報収集・分析等の仕組み（Trusted Group）の活用：基幹インフラ事業者やセキュリティベンダが参画するサイバー協議会の中に、参加する事業者と国との間で双方向に情報共有を行う枠組（Trusted Group）を立ち上げたところ、これを活用し、サイバー攻撃に関する事案や脅威の情報を収集し、官民が連携して分析を行う。この中で、攻撃元IPアドレス等の技術情報、攻撃手口や攻撃背景に関する評価・見解等を共有し合うとともに、こうした情報を活用して官民共同で分析等のプロジェクトを行うことで、民間事業者にとってアクショナブルな情報の作出を行う。【国家サイバー統括室】

（９）事案分析や注意喚起情報の作出を担う専門の体制の構築：社会的影響の大きい事案発生時において、司令塔となるNCOのインシデント対処（情報収集、各所との調整、事案の分析）の仕組みを、民間と連携し、強化する（R9年度～）。具体的には、事案分析の専門的知見を持つ民間人材の登用（政策調査員等）を拡充するとともに、事案分析や注意喚起情報の作出を担う専門の体制を構築する（令和９年度～）。当該人材による情報収集・事案分析も活用し、民間の被害の拡大を防ぐためのアクショナブルな情報を作出し、これを対外発信していく。【国家サイバー統括室】

（10）NCOの分析力強化とそれに基づく対象と目的を明確にした情報発信：NCOで収集・集約した情報を迅速かつ横断的に分析し、成果を発信していくため、AIを全面的に活用するとともに、サイバー対処能力強化法による法定業務委託先の３専門機関（IPA・NICT・JPCERT/CC）の高度な能力と知見、人材、民間セキュリティベンダの高度な知見の活用を可及的速やかに進める。

その上で、経営層、セキュリティ専門家、国民といった対象ごとに目的を明確にして、情報発信に取り組む※。また、政府や専門機関による情報発信については、NCOがあらかじめ公的機関の特性に応じて関係機関の役割分担を総合調整す

るとともに、影響の大きな事案ではとりまとめのウェブサイトを開設して、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。加えて、SNSを通じた拡散力・浸透力を強化していく。【国家サイバー統括室】

※　①直ちに対策を講じてもらうための情報発信（例：攻撃情報の横断的な分析による攻撃手口・傾向の注意喚起〔専門家向け〕、PHP2Shell 等の要注意脆弱性情報〔経営層向け/専門家向け〕、国内で悪用が確認された脆弱性の情報（日本版 KEV）〔専門家向け〕）、②状況を認識してもらうための情報発信（例：攻撃状況の横断的な分析レポート〔経営層向け/専門家向け〕、経済団体等を通じた情勢ブリーフ〔経営層向け〕、「何が起きているか（AI 悪用の有無を含む）」「誰に関係するのか」「一人一人が何をすればよいか」をわかりやすく伝える報道発表〔国民向け〕）、③攻撃者に攻撃を続けにくくさせるための情報発信（例：攻撃者の攻撃基盤や手口の公表〔専門家向け〕）。

（11）迅速かつ能動的な事案認知と NCO への情報集約：警察、防衛省・自衛隊及び外務省においては、認知・収集した情報に関する NCO への迅速な情報集約を徹底する。【警察庁・防衛省・自衛隊・外務省】

（12）警察に設置された協議会を中核とした官民連携の拡充：全都道府県警察に設置された協議会を中核とした地域の事業者や地方自治体等との官民連携を一層強化する。特に、都道府県知事部局と緊密に連携し、多様な事業者や業界団体への協議会への参画を働き掛け、企業への支援の裾野を拡大する。協議会において、最新の攻撃手口や被害事例等の共有を図るとともに、必要に応じて共同対処訓練を実施し、地域の対処能力の底上げを図る。こうした取組を通じて平素から「顔の見える関係」を構築することで、事案発生時の被害の届出や相談が速やかに行われる環境を整備する。事案認知時には、被害企業等に対して必要な協力を求め、迅速・的確な捜査・実態解明を図る（令和８年中に実施予定）。【警察庁】

（13）捜査・実態解明等、サイバー対処能力の強化に向けた人的・物的基盤の整備：①捜査・実態解明、パブリック・アトリビューション、アクセス・無害化措置といった多様な手段を駆使し、粘り強くサイバー攻撃に対処するため、全国の司令塔機能を担うサイバー警察局及びサイバー特別捜査部の体制の充実・強化を行う（令和８年度以前から継続的に実施）。②都道府県警察においてサイバー事案を

扱う一元化組織を整備し、一元化組織の効用を最大化するため、これまで分散していた物的基盤についても、ワンフロア化も含めた一体的な運用を確保できるよう、環境整備を推進する。法人被害への対処のための官民連携・情報収集のための都道府県警察の体制の強化を行う（継続的に実施）。③サイバー事案に対する実践的な訓練を行うためのサイバー演習環境「サイバーレンジ」を活用し、全国のサイバー人材の育成を推進する（令和８年度以前から継続的に実施）。④サイバー空間の匿名性を悪用した事案は、AI の悪用も相まって高度化・巧妙化していることから、暗号資産追跡や AI の利活用を含む捜査・実態解明の推進のために必要な資機材を整備する（令和８年度以前から継続的に実施）。【警察庁】

（14）食料の安定供給確保に向けた農林水産業・食品産業界との情報連携強化：サイバー攻撃によって農林水産物・食品の生産、加工、流通、販売等が影響を受け、食料の安定供給に支障を生じさせないよう、農林水産業・食品産業の関係団体等との情報連携を強化する。具体的には、以下に取り組むことにより、双方向の情報連携を通じて、サイバーセキュリティ対策の取組を推進し、食料供給のサプライチェーンの維持・確保を図る。

① サイバー事案等に関する NCO等の注意喚起について、関係部局庁を通じ、一次産業から三次産業までの幅広い関係団体等に随時周知し、必要なセキュリティ対策の実施を促進。

② 各団体・事業者に対し、サイバー被害が発生した場合等の情報提供を求めるとともに、一元的な連絡窓口の設置を予定。

③ 関係団体からの要請に基づき、勉強会等に情報セキュリティの専門家を派遣し、業界の知識向上・対策強化を支援。

④ サイバー協議会のスキームを通じた農林水産省関係の構成員や傘下の組織との連携強化。

【農林水産省】

３．サイバー攻撃への対処の戦略的な実施

（１）アウトリーチ・チーム（仮称）の新設：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 NCO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、気付かれていない侵害の早期発見と対策を促す。【国家サイバー統括室】

（２）官民サイバー救援隊（仮称）の創設：NCO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。【国家サイバー統括室】

（３）ジョイント・レスポンス・チームの新設・運用：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、NCO、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、NCOがNSS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。【国家サイバー統括室・内閣官房】

（４）オール・ジャパンの捜査の推進、「ファスト・フォレンジック・フォース（FFF）（仮称）」の設置：大規模かつ広域に及ぶ事案に対処するため、警察法の規定に基づき、関東管区警察局サイバー特別捜査部及び全都道府県警察によるオール・ジャパンでの合同捜査体制を構築する（速やかに実施）。被害企業等の負担軽減と実態解明に向けた証拠の収集のため、高度な専門的知識及び技術を有する専門人材によって構成される、事案発生時のログの保全等や早急な原因究明等の初期対応を担う「ファスト・フォレンジック・フォース（FFF）（仮称）」を警察庁及び管区警察局等に立ち上げる（速やかに実施）。【警察庁】

（５）「サイバーセキュリティお助け隊」の支援メニューの拡充：中小企業・小規模事業者が「サイバーセキュリティお助け隊サービス」を十分に活用できるよう、速やかに支援メニューを拡充する。具体的には、「サイバーセキュリティお助け隊サービス」で提供する異常監視やサイバー攻撃を受けた際の初動対応支援、保険などのサービスに、新たに復旧・再発防止等に関するサービスを追加し※、事業者を総合的に支援する。【経済産業省】

※　①被害発生時の診断、②定期バックアップと復旧支援、③定期脆弱性診断等のサービスを追加。

（６）政府主導の脅威ハンティング：攻撃・侵害された場合に社会や国民生活等に与える影響が大きい事業者等に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。具体的には、自発的な脅威ハンティングの実施能力のある事業者等には、サイバー協議会を通じて、年内を目途にマニュアル・検知ツール等を提供して迅速な実施を促進する。また、関係省庁との連携の下、高度な専門能力を有する専門機関や民間セキュリティベンダの知見も活用し、脅威ハンティングの実施に関して支援する仕組みを構築する。加えて、事業者等から要請があった場合に、警察・自衛隊は、NCOの総合調整の下、必要に応じて脅威ハンティングを実施・支援する。これらの過程を通じて被害有無や攻撃手法等の情報を更に収集し、攻撃の更なる分析に活用する。【国家サイバー統括室・警察庁・防衛省】

（７）攻撃基盤への対処：NCO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、サイバー攻撃の基盤として悪用されている国内の踏み台設備群について、電気通信事業者やNICTの能力を活用し、その構築を防止するための対策を年内にとりまとめ、必要な対応を行う。【国家サイバー統括室・内閣官房・警察庁・総務省・防衛省】

（８）政府機関等に対する「攻撃の検知に関する支援の仕組み」の強化（GSOCの強化）：政府機関や独立行政法人等の初動対処の支援の仕組みの一つであるGSOCに

ついて、民間の高度な専門能力を活用した強化に取り組む。具体的には、検知・分析に長けた専門の民間人材の更なる登用（令和９年度～）や、AI 活用等によるGSOCの更なる機能強化のためのプロジェクト（現行 GSOC: ～令和 10 年度、次期GSOC: 令和 11 年度～）、GSOCの基盤となる処理能力の向上や検知ポイントの拡充（センサ設置の拡充等。令和９年度～）、GSOCの増強・発展に繋がる監視能力の強化（令和９年度～）を行う。これらを通じて、政府機関等への攻撃・侵害の検知能力を高め、政府機関や独立行政法人等に対し、迅速な注意喚起を行う。【国家サイバー統括室】

（９）アクセス・無害化措置等の実効性確保・向上に向けた態勢等の強化：アクセス・無害化措置等の実効性を確保・向上させるため、NCO、警察及び防衛省・自衛隊の態勢（情報部門及びオペレーション部門）を増強するほか、必要となる予算の充実・強化を図る［中長期］。【国家サイバー統括室・警察庁・防衛省】

(10)「アクセス・無害化措置」を確実に実施できる体制強化：適時・適切にアクセス・無害化措置を講じることができるよう、対処を担う警察のサイバー人材の育成を進め、対処に必要な人員を確保するとともに、AI を活用した資機材の整備等を推進するなど、警察におけるアクセス・無害化措置の実施体制の更なる拡充・強化を可及的速やかに実施していく（令和８年度以前から継続的に実施）。【警察庁】

(11) 実践的かつ高度な訓練の実施：アクセス・無害化措置の実効性を確保・向上させるため、NCO、警察庁及び防衛省・自衛隊とで、サイバーレンジ※合同訓練の実施、海外関係機関との意見交換・TTX（Table Top Exercise：机上訓練）の実施等の取組を継続する（既に運用開始）。

※　サイバーレンジ：サーバ等の中に仮想の空間を用意して、その中に仮想のサーバ、端末やルータ等を構築した疑似インターネット環境。実インターネットと隔絶した環境であるため、サイバー攻撃の再現やアクセス・無害化措置の訓練を実施したとしても、影響を仮想空間内に留めることができ、訓練や試験等を安全に実施できるもの。【国家サイバー統括室・警察庁・防衛省】

(12) 戦略的な対処オプションを検討するための関係省庁局長級会合の開催：令和

８年 10 月末、サイバー攻撃キャンペーン※への戦略的な対処オプションを検討するための関係省庁局長級会合を初開催したところ、今後も、定期的又は情勢に応じて機動的に会合を開催することなどにより、NCOによる総合調整の下で、アクセス・無害化措置の効果的かつ適切な実施も含めて、あらゆる対処オプションを戦略的に選択・実施する（既に運用開始）。【国家サイバー統括室・内閣官房】

※　サイバー攻撃キャンペーン：一定期間内において特定の主体が国・重要インフラ等の特定の組織・分野に対して特定の攻撃手法・攻撃インフラを用いて繰り返し行うサイバー攻撃活動。

（13）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、外国捜査機関や関係機関との「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（令和８年度以前から継続的に実施）。【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

（１）警察の相談対応の充実・強化：全ての都道府県警察本部サイバー部門に、企業等がサイバー攻撃による被害等を受けた際の通報・相談を受け付ける「法人専用相談・通報窓口　サイバー被害 110 番（仮称）」を開設するとともに、専用ダイヤルを整備し、警察による被害企業への支援の強化を図る（窓口の開設は令和８年中、専用ダイヤルの開設は令和８年度中に整備予定）。この窓口において、知事部局等に設置された中小企業・小規模事業者向けの相談窓口と緊密に連携し、被害企業から相談があった際の情報共有や相互の窓口の引継ぎ等を通じ、被害企業に必要な支援が行き届くようサポート体制を整える（令和８年中に実施予定）。【警察庁・経済産業省】

（２）無料相談窓口の設置：IPAに 10 月 16 日に特別相談窓口を設置し、各都道府県の「よろず支援拠点」及び中小企業基盤整備機構の「IT経営サポートセンター」

に 10 月 27 日に無料の「サイバーセキュリティ特別相談窓口」を設置した。また、全国の商工団体、金融機関、税理士等の支援機関を通じ、中小企業・小規模事業者に対してプッシュ型で相談窓口や支援策の情報提供を実施しており、今後、支援機関職員等向けの説明会を開催して普及の担い手を育成する。さらに、年内から、各経済産業局及び IPA による説明・相談会を税理士会・商工団体・都道府県警察と連携して実施し、令和９年度中に周知する。【経済産業省】

（３）サイバーセキュリティ相談窓口の対象の拡充：所管重要インフラ６分野の事業者向けに設置しているサイバーセキュリティに係る相談窓口について、対象を国土交通省所管の事業者全体に速やかに拡充する。【国土交通省】

（４）二次被害の防止・お困りの方のための情報発信の強化：個人情報流出の被害に遭われた方・ご心配のある方のための相談窓口を、関係省庁と連携しつつ、首相官邸ホームページ等を活用して速やかに周知する。また、個人情報流出事案の対策のため、NCO と連携しつつ、個人向けの注意喚起動画を作成し、11 月中を目途に公表するなど、二次被害の防止、お困りの方のための情報発信を強化する。【内閣官房】

（５）国民に向けた情報発信強化：サイバーセキュリティに関する関係省庁・機関の相談窓口や注意喚起等について対象を明確にしてとりまとめた「サイバー対応特設サイト」を 10 月 30 日に開設した。信頼できる情報発信をまとめたサイトとして、随時更新していくことにより、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。また、国民や企業のサイバーセキュリティ対策に対する意識向上を図るため、「サイバーセキュリティ月間」において、関係機関・団体と連携した集中的な普及啓発活動を展開する。さらに、「インターネットの安心・安全ハンドブック」などの普及により、関係省庁が連携しながら、国民や企業に正確な情報を発信し必要な対策が講じられるよう取組を進める。また、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関係省庁が設置した窓口と共有し、窓口間で連携することにより、引き続き周知や情報発信を行う。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。【国家サイバー統括室・関係省庁】

（６）通信事業者によるアクセス抑止策に関する検討：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。【総務省】

（７）偽・誤情報への対策：流出した個人情報が悪用され、メールやSNSを通じた偽のリンクが張られたフィッシングメール等の偽情報等による二次被害を防止するため、①発信者が信頼できるかを容易に確認し、正しい情報かどうかの判断を支援する偽・誤情報対策技術の開発・実証、②幅広い世代を対象に二次被害の防止や、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・周知広報の推進を図る。また、SNSをはじめとするインターネット上で「偽・誤情報」が拡散している状況を踏まえ、デジタル空間をより健全かつ信頼できるものにするため、特に、ネットの利用率や情報拡散リスクの高い「若年層」をコアターゲットとして、情報拡散に伴うリスクへの注意喚起を行うとともに、真偽不明な情報の不用意な拡散防止等のリスク回避への理解を求めるなど、「偽・誤情報」対策の周知に向けた広報を実施する。【内閣府・総務省】

（８）二次被害防止のための情報発信の強化：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、NCO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。【国家サイバー統括室・関係省庁】

（９）情報流出による二次被害防止：特殊詐欺の犯人が流出した個人情報を悪用し、架電することが考えられるため、携帯電話への詐欺電話を遮断する機能を持つ「警察庁推奨アプリ」の普及促進を一層強化する。流出した個人情報を悪用したなりすましによる口座の開設等を防ぐため、口座開設や金銭の貸付け等の取引を行う事業者に対し、関係省庁と連携し、犯罪収益移転防止法等に定められる本人確認の徹底を要請する。不審な電話の着信を受けた場合等の警察相談専用電話「＃9110」番への相談について広報啓発を行う。個人情報の流出に係る相談対応・防犯指導を実施するとともに、関係者の意向を踏まえ、必要に応じて保護対策を

講じる。【警察庁・関係省庁】

(10) 消費者の安全・安心の確保に向けた取組：消費者の安全・安心を確保するため、全国の消費生活センター等に寄せられた消費生活相談情報を取りまとめ、関係省庁に共有するとともに、関係省庁と連携して、消費者の被害・二次被害の防止に向けて、必要な注意喚起を行う。また、全国の消費生活センター等における相談対応を支援する。【消費者庁】

(11) デジタルに不慣れな方々に対する助言・支援等：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。【デジタル庁】

５．その他

（１）人材育成及び体制の強化：現下のサイバー攻撃の激化の情勢を踏まえ、平時だけでなく有事に対しても迅速かつ適切に対応するべく、NCO及び各省庁の人材育成及び体制強化を図る。【国家サイバー統括室・関係省庁】

（２）脆弱性対応の円滑化に向けたシステム関連契約に関する検討：先般公表されたPHPの重大な脆弱性に見られるように、情報システムの運用開始後に脆弱性が発見されるリスクは常に存在する一方で、システム開発契約や運用保守契約においては、脆弱性対応の実施主体が明確に定められていない場合が多く、緊急の対策が必要となった際に支障が生じる事例が発生している。こうした脆弱性への対応円滑化の観点で、システム開発契約や運用保守契約において留意すべき事項の普及促進の方策の具体化に向け、検討を進める。【国家サイバー統括室】

（３）耐量子計算機暗号（PQC）移行の加速：我が国政府機関等における耐量子計算機暗号（PQC）への移行について、原則として2035年までに行うことを目指すこととしており、欧米主要国のPQC移行に関する動向や政府機関等における暗号技術の利用状況等も踏まえ、優先度が高いと判断する情報システムについてはよ

り早期に移行する期限を定めることも含め、関係省庁の連携の下で検討を行い、2026年度に工程表（ロードマップ）を策定する。【内閣官房・国家サイバー統括室・関係省庁】

（４）量子暗号通信（QKD）の社会実装の加速：政府機関や重要インフラ等の機微なデータを取り扱う重要機関間の通信の安全性を一層高めるため、機微情報の盗聴・改ざんを確実に防ぐ量子暗号通信（QKD）について、NICTが主体となり、広域量子暗号通信ネットワークの実証環境として2026年度中に東名阪を結ぶ都市間の幹線ネットワークを構築するとともに、段階的に拡充する。本実証環境における技術実証に加え、様々な分野における民間等による活用検証を推進することで、東名阪におけるQKDの社会実装を加速する。【総務省】

（５）上記以外の中長期的課題への対応：上記に明記した中長期的課題に加え、サイバー情勢の変化の状況も踏まえて検討を要する中長期的課題についても適切に検討を行う。

サイバーセキュリティ緊急対策パッケージについて

資料3

- ＡＩの進展により、サイバー攻撃は増加し、その被害も大規模化しています。基本的な対策の不備により、多くの事案で被害につながっています。
- これは一時的なものではなく、長く続くものであり、社会全体で一丸となって対応することが必要です。
- 攻撃を受けることを前提に、社会の機能を止めない、止まってもすぐに立ち直る「サイバーレジリエンス」を確保します。
- **そのために政府も、待たずに動く。国民の皆さんとともに我が国全体の対処能力を高めていく。**

自ら率先して守りを固め、被害を待たずに動き、立ち直るまで支える

目指す方向	今回の主要な施策
社会全体で **「当たり前の備え」を整える**	• 政府のシステムをＡＩで総点検します。また、企業・自治体のシステムの点検を専門チームが支援します。 • 顔写真などの画像を使わずに本人確認ができる仕組みや、必要以上に個人情報を持たない仕組みを広げます。
攻撃やその兆しを **「先回りして見つけ、解明する」**	• 民間企業や海外の関係機関と協力して、サイバー攻撃に関する情報を集め、ＡＩも活用して分析します。 • 分析で得られた情報を社会に還元し、社会全体のセキュリティ対策を後押しします。
攻撃や被害の状況に応じて **「切れ目なく、対応する」**	• 被害のおそれがある段階から実際に被害が発生した段階まで、官民の専門チームが企業の対応を支援します。 • 海外とも連携してサイバー攻撃に悪用される基盤への対応を進め、攻撃者の活動を困難にします。
被害に遭っても **「ひとりにしない」**	• どの窓口に相談しても、関係機関が連携し、必要な支援につなげます。 • 詐欺や偽情報などによる二次被害を防ぐ取組を強化します。