資料８

日薬情発第　170　号
令和 8 年 11 月 9 日

都道府県薬剤師会担当役員　殿

日本薬剤師会
副会長　原口　亨

サイバーセキュリティ緊急対策パッケージの公表を踏まえた
サイバーセキュリティ対策の強化について

平素より、本会会務に格別のご高配を賜り厚く御礼申し上げます。

標記につきまして、厚生労働省医政局総務課より別添のとおり事務連絡がありましたのでお知らせいたします。

昨今のサイバー攻撃の激化に対して、政府全体として、「サイバーセキュリティ緊急対策パッケージ」（別紙１）及び「サイバーセキュリティ緊急対策パッケージ：施策一覧」（別紙２）がとりまとめられたとのことです。

別紙１には方針を、別紙２にはその方針に基づいた各省庁の具体的な施策が記載されています。

会務ご多用のところ誠に恐れ入りますが、貴会会員にご周知下さるようお願い申し上げます。

事　　務　　連　　絡
令 和 ８ 年 11 月 ６ 日

公益社団法人 日本薬剤師会　御中

厚生労働省　医政局総務課

サイバーセキュリティ緊急対策パッケージの公表を踏まえた
サイバーセキュリティ対策の強化について（周知依頼）

医療行政の推進につきましては、平素より御理解、御協力を賜り、厚く御礼申し上げます。

今般、サイバー攻撃による大規模な情報漏えいが相次ぐ中、令和８年 11 月６日、政府全体として、「サイバーセキュリティ緊急対策パッケージ」（別紙１）及び「サイバーセキュリティ緊急対策パッケージ：施策一覧」（別紙２）がとりまとめられました。

これらの中で民間事業者の主な関係箇所（抜粋）を共有いたしますので、貴団体の会員等に対し、別紙１、２とともに周知いただきますようお願いいたします。

また、国家サイバー統括室のサイバー対応特設サイト※や公式Ｘアカウント「国家サイバー統括室（注意・警戒情報）」（アカウント名:@cyber_forecast）において、サイバーセキュリティに関する注意喚起等を発信しておりますのでご活用ください。

※https://www.cyber.go.jp/tokusetsu/contactpoint_advisory_hub/index.html

（別紙１及び別紙２の抜粋）

サイバーセキュリティ緊急対策パッケージ（抄）

１．AI も活用した基本的な対策の徹底

（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。

（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。

（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。

２．情報収集・集約、捜査・分析体制の強化

（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。

（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。

（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**。

３．サイバー攻撃への対処の戦略的な実施

（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

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。

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。

（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。

４．被害者支援・被害拡大防止策の強化

（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。

（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。

（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。

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】

別紙２

サイバーセキュリティ緊急対策パッケージ：施策一覧

１．AI も活用した基本的な対策の徹底

（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：個人情報取扱事業者は、個人データを利用する必要がなくなったときは当該データを遅滞なく消去するよう努めなければならないこととされていることから、10 月７日に、個人情報取扱事業者に対し、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を適切に行うことを含めて注意喚起を行った。本人確認等のために取得した画像等の保存期間・保存方法などに関する基本ルールについて、令和８年度中に、それぞれの業種の個人情報取扱事業者に対し注意喚起等を行う。

安全管理措置に関するガイドラインにおいて、不正アクセス防止のために個人情報取扱事業者が行うべき対策を強化することに資するよう、ガイドラインの安全管理措置の全項目の「手法の例示」の改正作業を加速させて、令和９年１月中の施行を目指す。【個人情報保護委員会】

（３）不正アクセスに関する個人情報保護法の厳格な執行：報告された漏えい等について、適時適切に事実関係の調査を行い、個人情報保護法上の問題点がみられた場合には、事業者に対し、必要に応じて随時、指導・助言等の監視・監督権限の行使を行う。また、個別の事案の調査等の過程において、共通してみられる問題点や今後の再発防止に向けて事業者等の参考となる点がみられた場合には、広く注意喚起等を行う。【個人情報保護委員会】

（４）マイナンバーカードと関係システムの安全性確保・強化：国民によるマイナンバーカードの利用に不可欠な「個人番号カード管理システム」及び「公的個人認証システム」について、発行・利用実績を踏まえつつ、中長期的視野でこれら

のシステムの安全性を強化する。【デジタル庁】

（５）利用推進の広報：マイナンバーカードを活用した認証基盤が広く官民で活用されることで、マイナンバーカードを使うことが当たり前になり、安全かつ便利に官民の手続やサービスを利用することを可能とし、全ての国民が生活の様々な場面でデジタル社会の利便性を安全に享受できる社会の実現に寄与する。【デジタル庁】

（６）デジタル認証サービス等の機能拡充・体制強化と民間事業者の導入支援：なりすましやサイバー攻撃等による被害を防ぎ、国民が官民のサービスを安心して利用できるよう、マイナンバーカードで安全・確実に本人確認ができる「デジタル認証サービス」について、以下の取組に速やかに着手する。（令和８年度から実施中の運用・保守体制も強化）

① 不正利用対策：認証時の証明書の有効性確認、ログアウト時のトークン制御等の機能を強化し、不正利用によるアクセスを防止する。

② 利用場面の拡大：年齢確認において、生年月日等の必要以上の情報を提供することなく、年齢や年齢幅など必要な情報のみを提供できる機能を整備し、安全な本人確認を官民の幅広い場面に広げる。【デジタル庁】

（７）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 の利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・提供を進めていく。【経済産業省】

（８）金融分野におけるサイバーレジリエンス強化及び AI 活用による防御力向上：金融システムの安定性を確保していく観点から、金融機関等において経営陣関与の下、要請文（５月 22 日）で示した「短期的な対応」を進めるとともに、ガイドライン等で示している多層防御やインシデント発生時の備えといった基本的な

サイバーセキュリティ対策を着実に実施することを促す。また、金融業界全体のレジリエンス強化に向けて、業界横断的なサイバーセキュリティ演習の実施や、金融 ISAC 等を通じた知見の共有等の取組を強化する。加えて、金融機関におけるサイバーセキュリティ対策の高度化を推進するための方策を検討する。【金融庁】

（９）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、ソフトウェア構成情報（SBOM：Software Bill of Materials）を含む IT 資産管理の徹底を図りつつ、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。併せて、機微な情報を安全に取り扱いながら高度な脆弱性診断等を行うため、ソブリンティを確保した AI 環境についても検証・整備を進める。【国家サイバー統括室・デジタル庁・関係省庁】

(10) ガバメントクラウドへの着実な移行：マイナンバー情報連携システム、公金受取口座登録システム、給付支援サービス及び G ビズポータル等の政府が所管する国のシステムのガバメントクラウドへの移行を着実に行う。また、ガバメントクラウドを利用するシステムについては、システムの所有者において、令和９年度中までに高性能 AI を用いたソースコードの脆弱性検査を実施することを求める。【デジタル庁】

(11) 地方公共団体のサイバーセキュリティの強化：昨今のウェブシステム等に対する AI による攻撃に対応するため、緊急的な対策として、総務省から地方公共団体に対し、次の事項について要請を行う。

① 庁内に CISO 等によるガバナンス体制を構築し、担当課が独自判断で導入したものを含めた全てのウェブシステム等（委託先が提供するものも含む。以下同じ。）とそのセキュリティ対策を把握すること。

② 多要素認証等の認証機能の強化、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。

③ ウェブシステム等について、AI モデルを活用した脆弱性診断及び診断結果を踏まえた脆弱性対策を行うこと。また、脆弱性対策が完了するまで一時的なサービスの停止を検討すること。

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 等と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 BD」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。