（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。