サイバーセキュリティ緊急対策パッケージ（概要）

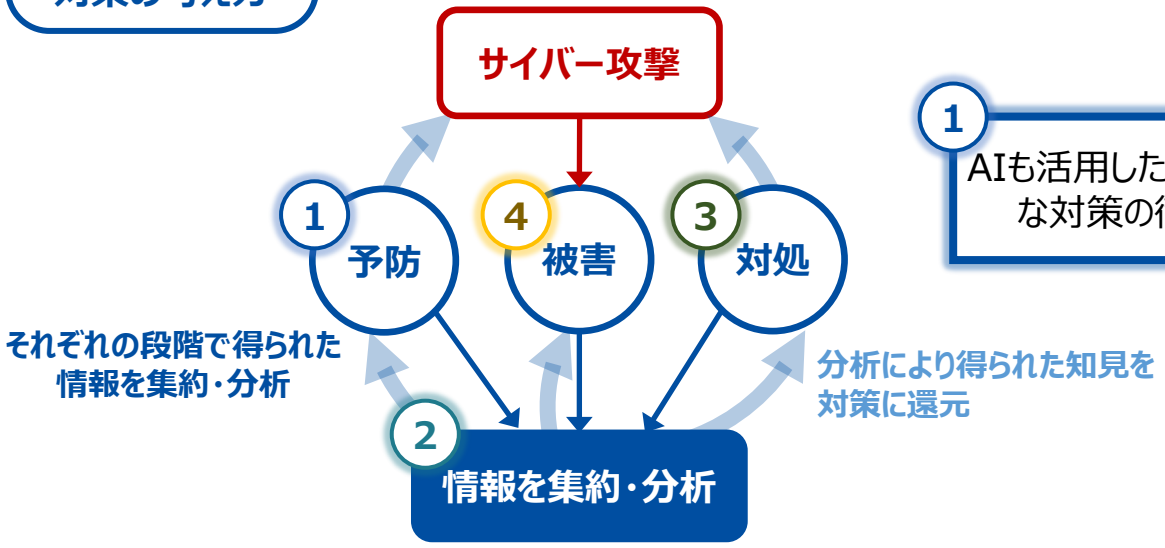
令和８年11月6日 サイバーセキュリティに関する関係閣僚会議決定

- サイバー攻撃による情報漏えい等が相次ぎ、国民生活・企業活動に大きな不安と影響
- 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、自組織・委託先の**基本的な対策の不備が多くの事案に共通**
- 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ことから、**特定の組織・業界に限らず我が国社会全体**で対応することが必要

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、サイバー攻撃を受けたとしても、官民が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 を目指す

対策の考え方

情報の集約・分析と、その結果の対策への活用という循環を作ることで社会全体のサイバー対処能力の向上につなげる



1. AIも活用した基本的な対策の徹底
2. 情報収集・集約、捜査・分析体制の強化
3. サイバー攻撃への対処の戦略的な実施
4. 被害者支援・被害拡大防止策の強化

- 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、スピード感をもって実施
- 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

１．AIも活用した基本的な対策の徹底

【現状・課題】
- 昨今の漏えい事案の多くは、基本的な対策の徹底で防止・軽減が可能。AIにより脆弱性の発見から攻撃までの時間が短縮し、未知の脆弱性も悪用され得る中、被害の規模を抑える対応も必要

【目指す方向】
- あらゆる組織が基本的な対策を「当たり前」に講じる社会へ

基本的な対策を「当たり前」に	• 最近の情勢を踏まえ、ウェブサイト・モバイルアプリの基本的な対策について注意喚起【国家サイバー統括室】
攻撃を受けたとしても被害を最小限に	• 不要な個人データの消去を求めるとともに、安全管理措置ガイドラインを改正（R9.1中の施行を目指す）【個人情報保護委員会】 • 画像による本人確認に代え、マイナンバーカード等のICチップによる安全かつ確実な本人確認の利活用場面を拡大【デジタル庁・関係省庁】
AIを活用し、攻撃者より先に脆弱性を見つけて塞ぐ	• IPAにトップガン人材チームを立ち上げ（11月中）、ペネトレーションテストの実施を民間企業を含め推進【経済産業省】 • 政府の情報システムについて、システムを構成する機器・ソフトウェアを把握・管理するとともに、AIを活用した脆弱性診断を前倒しで実施【国家サイバー統括室・デジタル庁・関係省庁】 • 地方公共団体にAI脆弱性診断等を要請し、自治体サイバーセキュリティサポートチームが全ての団体の取組を支援【総務省】 • AISIの機能を強化し、英国AISIとも連携して高性能なAIモデル等のサイバー攻撃性能を評価・共有【内閣府】

2．情報収集・集約、捜査・分析体制の強化

【現状・課題】
- 政府機関等や重要インフラに限らず幅広い事業者が被害に遭う中、政府だけでは攻撃の兆候を捉え、攻撃主体・手口を解明する情報と分析力に限界

【目指す方向】
- 民間の力も活用して政府の情報集約・分析能力を高め、攻撃の兆候を先回りして捉え、その結果を社会に還元する循環を常に機能させる

民間の情報・知見を政府に集める	• セキュリティベンダ・クラウド事業者のサイバー協議会への参加や、海外大手・フロンティアAI企業との連携により、攻撃関連情報・脆弱性情報を早期に集約【国家サイバー統括室・総務省】 • 重大な被害事案は関係省庁が被害事業者から迅速に情報を収集して国家サイバー統括室に報告。SCS評価制度の取得企業にも関係情報を求めることが可能な仕組みを導入【国家サイバー統括室・経済産業省・関係省庁】
政府自身の分析能力を高める	• 「A2B攻撃」を特定したNICTの分析能力を強化するとともに、AIエージェントによる攻撃も再現・分析可能な環境の構築に着手【総務省】
サプライチェーンで被害を連鎖させない	• 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を開始【国家サイバー統括室・経済産業省・総務省】
捜査で攻撃主体・手口を解明する	• 捜査・実態解明を通じた将来の被害防止の観点から、所管企業に対し、被害の通報とログ等の証拠の提供を要請【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

【現状・課題】
- 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。また、攻撃の基盤が残る限り被害が続くおそれ。

【目指す方向】
- 潜在的な被害のおそれの段階から官民一体でシームレスに対処し、同盟国・同志国と連携して攻撃者にコストを賦課し続ける

事案に応じたシームレスな対応	• 国家サイバー統括室が、被害の状況、攻撃の背景・手法、対策状況等を踏まえて、政府による対応の必要性・緊急性を判断した上で、事案の内容や段階に応じて、官民それぞれの能力を活用して、シームレスな対応を行う。 ＜潜在的な被害のおそれがある場合＞ 能動的に接触し、侵害の早期発見と対策を促進 ＜支援の必要性が特に認められる場合＞ 民間の専門機関とも連携し、官民の専門人材チームを派遣 ＜重大な事案＞ 複数の省庁等の職員からなる専門人材チームを派遣し、必要な支援等を実施 【国家サイバー統括室・内閣官房・警察庁・防衛省・関係省庁】 連携 • 警察に新設する「ファスト・フォレンジック・フォース（仮称）」で、ログの保全等の初動的な措置を確保【警察庁】 ＜中小企業等の被害＞「サイバーセキュリティお助け隊サービス」に復旧・バックアップ等の支援メニューを追加し、初動から復旧まで一貫して支援【経済産業省】
攻撃を能動的に探索し、基盤を断つ	• 事業者等に脅威ハンティングを働き掛け、マニュアル・検知ツールを提供（年内目途）【国家サイバー統括室・警察庁・防衛省】 • アクセス・無害化措置を含む手段を戦略的に選択・実行し、攻撃インフラのテイクダウンや踏み台機器への対策を推進【国家サイバー統括室・内閣官房・警察庁・防衛省・総務省】
同盟国・同志国との連携	• 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」を構築し、国際共同捜査やパブリック・アトリビューション等を推進【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

【現状・課題】
- 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
- 漏えいした個人情報を悪用した詐欺電話・フィッシング・なりすまし、偽・誤情報の拡散などの二次被害が、事案のたびに起こり得る

【目指す方向】
- 被害に遭った組織・個人を孤立させず、どこに相談しても必要な支援につなげ、国民が正しい情報で自らを守れるようにする

迷わず相談・支援につなぐ

＜事業者向け＞ 警察の法人被害の専用窓口に加え、IPA・よろず支援拠点等の無料相談や業所管省庁の分野別窓口を設置【警察庁・経済産業省・関係省庁】

＜個人向け＞ 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った方や不安のある方向けに相談内容に応じた各種窓口を官邸ホームページで案内【内閣広報室、総務省、消費者庁、関係省庁】

- 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、窓口間で連携して、どこに相談しても必要な支援につなげる【国家サイバー統括室、関係省庁】
- 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の研修を受講し、デジタルに不慣れな方に助言・支援【デジタル庁】

必要な情報を確実に届ける

- 対象と目的に応じて情報を発信（例：経営層には事案の影響の大きさや切迫度、専門家には直ちに講じるべき技術的な対応等）【国家サイバー統括室・関係省庁】
- 「サイバー対応特設サイト」（10/30開設）で、相談窓口・注意喚起など必要な情報を一元化し、分かりやすく案内【国家サイバー統括室】

二次被害を防ぐ

- 国外由来を含む偽・誤情報に対し、業所管省庁と連携して注意喚起・正確な情報を迅速に発信するとともに、通信事業者によるアクセス抑止策の在り方を検討【国家サイバー統括室・内閣官房・内閣府・総務省・政府広報室・関係省庁】