「サイバーセキュリティ緊急対策パッケージ」を踏まえた地方公共団体における対応及び支援策について

総務省

令和８年11月13日（金）

自治行政局住民制度課

サイバーセキュリティ対策室

ウェブシステム等に対する不正アクセスにかかる環境の変化

○ 昨今のサイバー攻撃では、インターネット上に公開された広範な事業者等の**ウェブシステム・スマホアプリに対して攻撃**が行われ、当該ウェブシステム等に登録されている**個人情報が漏洩**。

○ 一連の攻撃においてはAIを悪用した攻撃を推測させる状況証拠が増えてきており、**「防御」においても、AIを活用**して、脆弱性の診断や発見した設定不備・脆弱性の修正を行うことが必要。

従来の攻撃

【攻撃側】

- **人力で特定の脆弱性を探知して攻撃**
- **攻撃は低頻度で、拡散は遅い**

【防御側】

- **攻撃が拡散する前に既知の脆弱性への対策を講じることが可能**
- **ただし、こうした対策を行わず放置している事業者等が多い現況**

AI時代の攻撃

【攻撃側】

- **AIを用いて脆弱性を総当たり的に検出し攻撃**
- **攻撃は高頻度で、拡散は速い**

【防御側】

- **未知の脆弱性が高頻度で発見され、対策が追いつかない**
- **既知の脆弱性への対策不備を突く攻撃が拡散している**

これからの対策

- まずは、既知の脆弱性に対する**基本的な対策を徹底**することが前提。
- その上で、今後は**防御側もAIを活用してシステムに内在する脆弱性を診断し、予防的に対策を講ずる必要**がある。

【具体的な対策】

ソースコード診断

システムのソースコードを多面的に分析し、脆弱性候補と影響範囲を特定した上で攻撃の成立可否を判定。

AND / OR

ブラックボックス診断

（プラットフォーム診断、ウェブアプリケーション診断）

インターネットからの申請フォーム等をAIが攻撃経路を探索し侵害リスクを診断。

発見した設定不備・脆弱性を修正

※ NCOではこの対応を各省庁へ依頼予定

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　日 サイバーセキュリティに関する関係閣僚会議決定

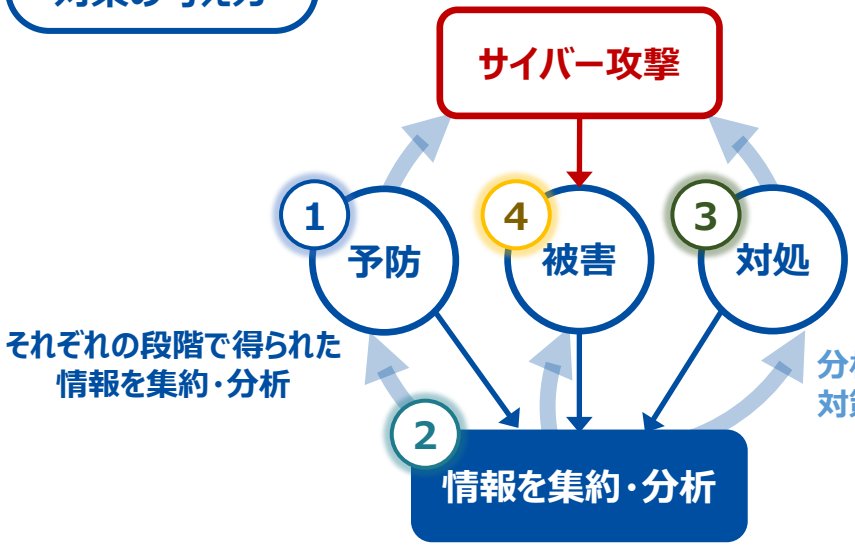
※地方公共団体関係部分抜粋

- 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】

AI脆弱性診断とサポートチームについて

➢ **＜地方公共団体のウェブシステム等の脆弱性対応＞**
地方公共団体に対し、**AIを活用した「ソースコード診断」又は「フロンティアAIテスト」による脆弱性診断及び修正対応**を要請。
（令和８年11月６日通知）

➢ **＜総務省の支援策＞** ⇒ **「自治体サイバーセキュリティサポートチーム」の構築**

① **脆弱性診断事業者チーム（経産省のお助け隊と類似のスキーム）**
地方公共団体及び委託先ベンダに対し、AI脆弱性診断等を実施するに当たり、技術的な観点からの助言をするとともに、具体的なシステムに関する**AI脆弱性診断等を実施**する事業者。

② **アドバイザーチーム**
地方公共団体に対し、AI脆弱性診断等を実施するに当たり、**対象システムの選定、AI脆弱性診断等のサービス提供事業者の選定等に関する助言**をするアドバイザー。

全体像

