資料３－１

脅威ハンティングの普及促進・実施等に係る基本方針（案）の概要

令和8年7月31日
内閣官房　国家サイバー統括室（NCO）

「脅威ハンティングの普及促進・実施等に係る基本方針」(案)について

「サイバーセキュリティ戦略」に基づき策定するもので、我が国全体のサイバーセキュリティ及びレジリエンスの向上・能動的サイバー防御の取組の推進に資することを目的とし、
脅威ハンティングに関する政府の基本的な考え方や主要な取組を提示

基本方針策定の趣旨・基本的な考え方(Ⅰ/Ⅱ章)

- 近年、サイバー攻撃は巧妙化・高度化しており、
  重要インフラ等のシステムに至る高度な侵入能力や長期的な潜伏能力が確認されている
- 脅威ハンティング(従来のセキュリティ対策では検知が困難なサイバー脅威を自発的に探索する活動)は、
  巧妙化・高度化したサイバー攻撃への対策の一つとして挙げられ、その必要性が海外でも広く認識されている

政府の主要な取組(Ⅲ章)

※対象組織:政府機関、独立行政法人、指定法人、重要インフラ事業者等、
基幹インフラ事業者及びその他重要情報の漏えい等が我が国に
深刻・致命的な影響を生じさせるおそれがある民間事業者等

1. 脅威ハンティングの実施に必要な能力習得・体制構築等の促進

- 対象組織※の能力・体制等に応じた段階的な取組を促進する支援
  (ガイドブック、研修・実習機会、基盤整備、演習機会、人材育成プログラム等)

2. 脅威ハンティング活動の実効性向上

- 脅威ハンティングを行う対象組織に対する政府からの情報提供・助言・支援

3. 政府による脅威ハンティングの実施等に関する取組

- 官民一体となった脅威ハンティングの推進等
  (サイバー脅威に対する情報集約・分析、政府機関間連携・協力、官民組織への情報提供・支援等)
- 平時から有事までシームレスに対応するための取組(サイバー攻撃の実態解明、民間事業者等に対する注意喚起等、
  (有事等における)安全保障確保に向けた脅威ハンティングの能力・体制強化等)

4. 国内外の官民連携/協働

- (国内)新協議会等を活用し、国内の官民間の連携を更に促進・強化
- (国外)外国政府等との協力関係の構築、脅威ハンティングの高度化に資する各種情報の相互共有

基本方針策定の趣旨・基本的な考え方（Ⅰ/Ⅱ章）

サイバー空間を取り巻く環境

近年、サイバー攻撃の手法が巧妙化・高度化

公開サーバへの攻撃
ウェブサーバ・外向けサービスへの大量通信　等

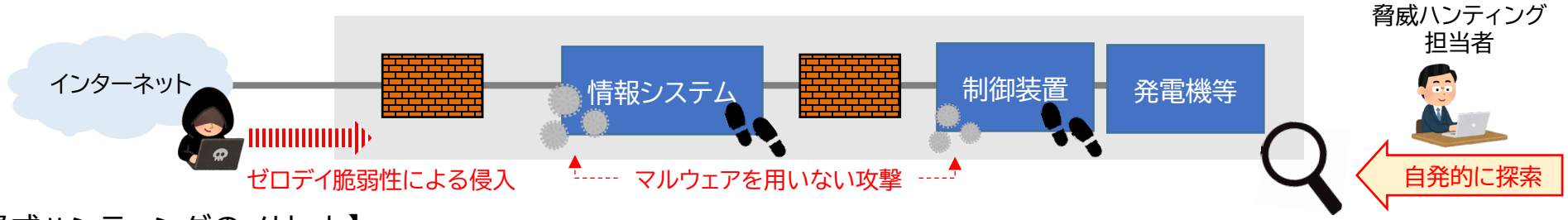
IT系システムの侵害
情報システム内部への侵入等
（主に既知の脆弱性を悪用）

有事を見据えた重要インフラ等への侵入
最深部・制御系システムに至る高度な侵入能力
（ゼロデイ脆弱性の積極活用等）
高度・長期的な潜伏能力
（システム内寄生戦術（Living-off-the-Land）等）

本基本方針策定の背景

- 巧妙化・高度化したサイバー攻撃手法への対策として、**脅威ハンティングの必要性が海外でも広く認識**されている
- 外国政府の戦略・政策においても脅威ハンティングを重要なサイバーセキュリティ対策の一つとして位置付け

本基本方針における脅威ハンティング：「従来のセキュリティ対策では検知が困難なサイバー脅威を自発的に探索する活動」



【脅威ハンティングのメリット】

- 巧妙化・高度化したサイバー攻撃等の早期発見
- 組織内のセキュリティ対策の見直し・強化に寄与
- 能動的サイバー防御に有用な情報の取得
- セキュリティ能力の更なる向上や体制強化

本基本方針では、以下を実施

我が国全体のサイバーセキュリティ及びレジリエンスの向上・能動的サイバー防御の取組の推進に資することを目的とし、脅威ハンティングに関する政府の基本的な考え方や主要な取組を提示

政府の主要な取組（Ⅲ章）

1. 脅威ハンティングの実施に必要な能力習得・体制構築等の促進

◆概要

脅威ハンティングを実施するに当たり、対象組織の能力・体制等に応じた段階的な取組を促進する支援を政府が行う

段階的な取組の一例

Step4 脅威ハンティングの実施

Step3 ログ分析・分析結果の活用

Step2 ログの収集・集約

Step1 従来の対策

<例>
情報資産の管理
リスクアセスメント
OSアップデート
セキュリティソフト導入
ログの保存 等

政府による支援

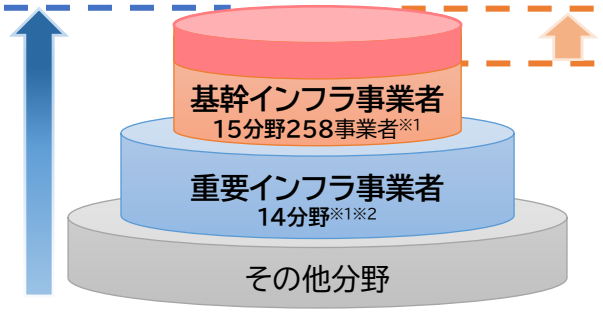
ガイドブック等の提供、研修・実習機会の提供 等

基盤の整備・提供、演習機会の提供 等

人材育成プログラムの提供 等

1. の主な対象
対象組織のうち、脅威ハンティングに関する取組を検討する必要のある組織

対象組織：政府機関、独立行政法人、指定法人 、重要インフラ事業者等、基幹インフラ事業者及びその他重要情報の漏えい等が我が国に深刻・致命的な影響を生じさせるおそれがある民間事業者等



各取組における主な対象（事業者）のイメージ

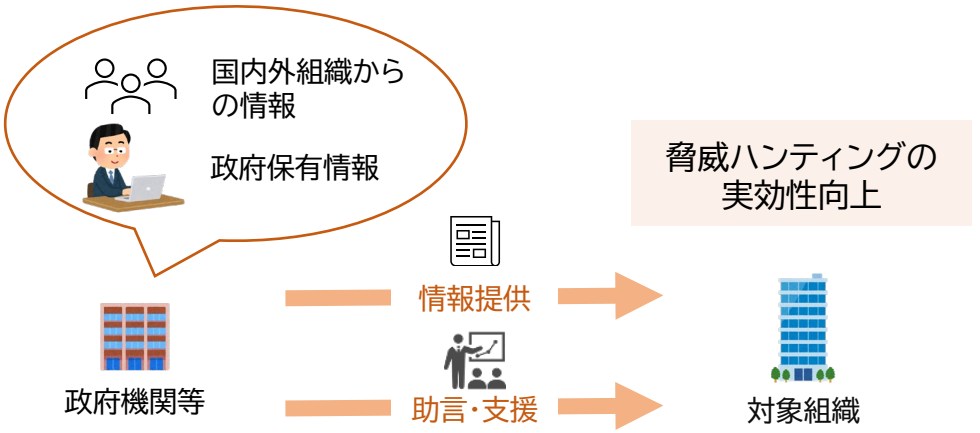
2. の主な対象
対象組織のうち、脅威ハンティングを行う能力・体制等を有する組織

※1 重要インフラ事業者・基幹インフラ事業者の数は、2026年7月1日時点のもの
※2「政府・行政サービス」を除く

2. 脅威ハンティング活動の実効性向上

◆概要

脅威ハンティングを行う対象組織に対し、政府から有効な情報等を提供することで、各組織の脅威ハンティングの実効性を向上



政府の主要な取組（Ⅲ章）

3. 政府による脅威ハンティングの実施等に関する取組

◆概要

我が国に深刻・致命的な影響を及ぼし得るサイバー脅威に対する官民一体での取組等

深刻なサイバー脅威に関する情報集約・分析、政府機関間の連携・協力、官民組織への情報提供・支援等、官民一体となった脅威ハンティングの推進等を実施する

サイバー脅威に対する情報集約・分析、政府機関間連携・協力

官民組織への情報提供・支援等

平時から有事までシームレスに対応するための取組

脅威ハンティングを含むサイバー攻撃に関する能動的な解明や、民間事業者等を対象にした注意喚起等を推進するとともに、これらを支える体制の充実・強化や資機材の整備・高度化を推進する

サイバー攻撃の実態解明

民間事業者等に対する注意喚起等

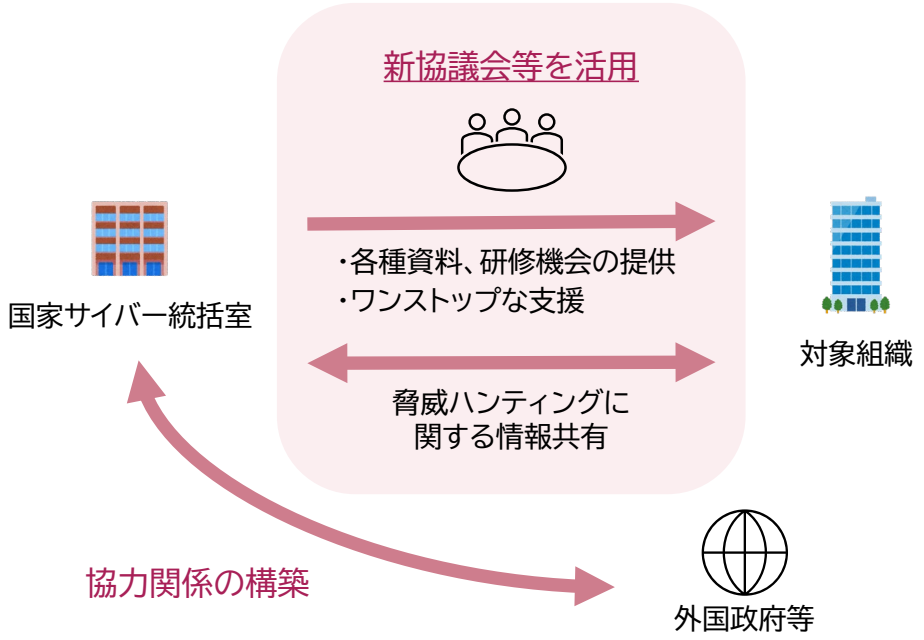
我が国におけるサイバー攻撃の被害の防止や拡大防止等の観点から、能力や体制の強化を図るとともに、民間事業者等への脅威ハンティングの支援のための検討等を行う

（有事等における）安全保障確保に向けた脅威ハンティングの能力・体制強化等

4. 国内外の官民連携／協働

◆概要

国内においては、新協議会※等を活用し、
国内の官民間の連携を更に促進・強化するほか、
国外においては、外国政府等との協力関係を構築し、
脅威ハンティングの高度化に資する各種情報の相互共有を目指す



※サイバー対処能力強化法により新たに設立される協議会