脅威ハンティングの普及促進・実施等に係る基本方針

令和８年７月 31 日
サイバーセキュリティ戦略本部

目次

Ⅰ. 本基本方針の策定の趣旨

１. 背景・経緯等

近年、ゼロデイ脆弱性やLiving Off The Land戦術（以下「LOTL戦術」という。）[1]を用いた重要インフラ等のシステム等への侵入や情報システム・ネットワーク内等での潜伏が報告されるなど、サイバー攻撃は一層巧妙化・高度化している。

例えば、中国を背景とすると指摘される「VoltTyphoon」が、グアム等の米軍・政府機関や重要インフラの機能停止等を目的として、LOTL戦術等を用いて情報システム・ネットワークに長期間侵入・潜伏した事案が報告されている。事象の影響が容易に国境を越えるというサイバー空間の特性を踏まえると、我が国の政府機関や重要インフラ事業者等（サイバーセキュリティ基本法（平成26年法律第104号。以下「基本法」という。）に基づく重要社会基盤事業者等）、基幹インフラ事業者（経済安全保障推進法[2]に基づく特定社会基盤事業者）なども同様の脅威に晒され、我が国の国民生活・経済活動、ひいては国家安全保障に深刻かつ致命的な影響（以下「我が国に深刻・致命的な影響」という。）を及ぼすリスクがあることを十分認識する必要がある。また、大手民間事業者に対するランサムウェア攻撃により、国内のサプライチェーンに大きな支障が生じた事例も発生するなど、サイバー攻撃が民間事業者の事業活動の停止等を生じさせるリスクも顕在化している。さらに、サイバー攻撃にAIが悪用されることで、攻撃のスピード・規模が劇的に増加するおそれもある[3]。上述のような現状を踏まえると、サイバー脅威への一層の対応が急務となっている。

「国家安全保障戦略」（2022年12月16日国家安全保障会議決定及び閣議決定）では、「サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」ことを目標に掲げた。当該戦略に基づき、法制度の整備等について検討するため、2024年６月に「サイバー安全保障分野での対応能力の向上に向けた有識者会議」が立ち上がり、同年11月に取りまとめられた提言を踏まえ、2025年５月には能動的サイバー防御を導入可能とする、重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第42号。以下「サイバー対処能力強化法」という。）及び重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和７年法律第43号）が成立した。くわえて、同年７月にはサイバーセキュリティ戦略本部について、内閣総理大臣を本部長とし、全大臣で構成するなどの改組により新たな体制とするとともに、内閣官房に、サイバー安全保障も含め、官民を通じたサイバーセキュリティの確保に関する司令塔として、「国家サイバー統括室」が発足した。

この新たな体制の下、我が国のサイバーセキュリティの確保に向けた取組を着実に進める必要がある。しかし、情報資産管理やログ管理等といった従来のセキュリティ対策のみでは、長期間

---

[1] LOTL戦術（日本語では「システム内寄生戦術」という。）とは、ネットワーク機器の脆弱性の悪用等により初期侵入を行った後、従来から行われているマルウェアを用いたサイバー攻撃とは異なり、システム内に組み込まれている正規の管理ツール、コマンド、機能等を用いて、認証情報の窃取、システム情報の収集等の活動を行うサイバー攻撃のことをいう。

[2] 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第43号）

[3] これを踏まえ、AI性能の高度化を踏まえたサイバーセキュリティ対策に関する関係府省庁会議（令和８年５月18日開催）において、「AI性能の高度化を踏まえたサイバーセキュリティ対策の強化について～Project YATA-Shield～」が取りまとめられた。

の侵入・潜伏を可能とする、巧妙化・高度化したサイバー攻撃に対応することが困難である。このような攻撃に対しては、従来のサイバーセキュリティ対策を前提としつつ、自発的に状況を把握する対策が重要であり、その対策の一つとして「脅威ハンティング」が挙げられる。脅威ハンティングを通じて入手したサイバー脅威情報等を官民間で共有し防御に役立てるとともに、アクセス・無害化措置をはじめとする能動的サイバー防御に活用することは、我が国におけるサイバー攻撃による重大な被害の防止、拡大防止等にも極めて有効である。

しかしながら、我が国の多くの組織においては、脅威ハンティングの概念・活動について十分な理解が未だ浸透していない状況にある。他方、高水準のサイバーセキュリティ能力・体制を有する民間事業者であっても、巧妙化・高度化したサイバー攻撃による侵入を完全に防ぐことは困難であることを踏まえれば、脅威ハンティングによるサイバー脅威の早期発見は事業停止等の企業経営上のリスク回避に直結すると考えられる。また、民間事業者における脅威の見落としや侵入の放置は、サプライチェーン等を通じて、同業種の組織のみならず、重要インフラ事業者等や政府機関などに波及し、結果として我が国に深刻・致命的な影響を及ぼす可能性もある。このように、各民間事業者におけるリスク回避はもとより、国全体への被害拡大の阻止及び能動的サイバー防御に関する取組の着実な実施のために、脅威ハンティングを国全体に浸透させていかなければならない。

脅威ハンティングの必要性は海外でも広く認識されており、各国政府の戦略・政策[4]においても、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られている。

こうした内外の情勢を踏まえ、我が国においても脅威ハンティングの普及促進や実施等に積極的に取り組んでいくことが求められている。

２．目的

本基本方針は、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示すものである。対象組織（Ⅱ．３．参照）が、自らの能力・体制等や、サイバー攻撃を受けた際に社会に及ぼす影響やリスクを踏まえた上で、Ⅲ．に記載の政府の取組を活用しながら、脅威ハンティングを実施することで、我が国全体のサイバーセキュリティ及びレジリエンス[5]の向上並びに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する。

---

[4] 例えば、米国では CISA（Cybersecurity and Infrastructure Security Agency）が公表した「FY2024-2026 Cybersecurity Strategic Plan」において、脅威ハンティングを「即時的脅威への対応」を実行するための中核的な運用手段として位置付け、恒常的な探索を通じて脅威や侵害活動を早期に把握し、関係主体と連携して迅速な緩和・排除につなげていく取組が進められているほか、CISA には脅威ハンティング専門部門が設置されている。英国では「National Cyber Security Strategy 2016-2021」において、未知・高度なサイバー脅威への早期対処を実現するため、受動的な検知に加えて能動的な防御能力の強化を重要課題として位置付けており、2019 年に脅威ハンティングを各省庁や組織が SOC（※）を通じて担うべき運用能力として整理した文書を公表して、当該能力向上を図る取組を進めている。シンガポールでは 2022 年に Cybersecurity Act を改定し、重要情報インフラ（Critical Information Infrastructure：CII）のオーナーに対して、CII に対する脅威ハンティングを少なくとも２年に一度実施することを義務化している。

（※） SOC（Security Operation Center）とは、セキュリティ・サービス及びセキュリティ監視を提供するセンターのことをいう。

[5] レジリエンスとは、インシデントが発生した際に、その影響を最小化し、早急に元の状態に戻す仕組みや能力、耐性のことをいう。

３．法令・政府決定文書との関係

本基本方針は、サイバーセキュリティ戦略（令和７年 12 月 23 日閣議決定）の「Ⅲ．１．（２）②官民における脅威ハンティングの実施拡大」に基づき政府において策定を検討し、基本法第 26 条第１項第６号に基づき、サイバーセキュリティ戦略本部において決定したものである。

II. 本基本方針における基本的な考え方

１．本基本方針における脅威ハンティングの位置付け

脅威ハンティングは、近年、SIEM[6]やEDR[7]といったセキュリティ関連のログ分析や状態監視、攻撃遮断等の機能を提供する製品の普及とともに実行可能性が高い取組となってきている。また、各国政府のサイバーセキュリティ関連文書において記された脅威ハンティングの説明[8]も踏まえ、本基本方針における脅威ハンティングを「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」と定義する。ただし、当該定義は、新たなサイバー脅威や技術革新等の状況を踏まえ、必要に応じて見直されるものとする。

２．脅威ハンティングと従来のサイバーセキュリティ対策の関係性

脅威ハンティングの実施に当たっては、情報資産管理を行い、リスクアセスメント[9]によって組織が抱えるサイバーセキュリティリスクを的確に把握・評価した上で、必要なOSアップデートやセキュリティ製品の導入、適切なログ管理等を実施するなど、従来のサイバーセキュリティ対策[10]の実施状況を踏まえて、段階的に対策を高度化するアプローチが求められる。これにより、組織内の情報システムやネットワーク等の状況把握が進み、脅威ハンティングの実効性の向上につながる。一方、脅威ハンティングの実施を通じて得られる知見[11]は、組織内のサイバーセキュリティ対策の見直しや強化に活用できるほか、能動的サイバー防御に有用な情報になる場合がある。このように、従来のサイバーセキュリティ対策を前提として、脅威ハンティングの実施に向けた準備を進めていくことで、セキュリティ能力の更なる向上や体制強化につなげることができる。

---

[6] SIEM（Security Information and Event Management）とは、セキュリティ関連のログを分析・監視することを目的とし、ログの一元管理、異常の自動検出機能を有する製品をいう。

[7] EDR（Endpoint Detection and Response）とは、端末やサーバ装置（エンドポイント）における活動を可視化し、不正プログラムの検知や記録、攻撃遮断などの対処といった機能を提供する製品をいう。

[8] サイバーセキュリティに関する国際標準的なガイドラインを発行している NIST（National Institute of Standards and Technology）では、脅威ハンティングを「Threat hunting is an active means of cyber defense in contrast to traditional protection measures.（脅威ハンティングは、従来の防御手段とは対照的な、能動的なサイバー防御手段である。）」と解釈している。また、英国政府 Cabinet Office（内閣府）では、「Cyber threat hunting is the process of proactively searching across networks and endpoints to identify threats that evade security controls.（サイバー脅威ハンティングとは、セキュリティ対策をすり抜けた脅威を特定するために、ネットワークや端末を能動的に調査する取組を指す。）」と解釈している。

[9] 国家サイバー統括室では、リスクアセスメントの実施のために、リスクアセスメントの手順や考え方を解説した「機能保証のためのリスクアセスメント・ガイドライン」を公表しているほか、リスクアセスメントを実践的に学べる「リスクアセスメント実践ラーニングキット」を学習用コンテンツとして提供している。

[10] 従来のサイバーセキュリティ対策については、国家サイバー統括室をはじめ、各政府機関からガイドライン等が公表されており、個々の組織の属性に応じて当該ガイドライン等に基づく対応が求められている。国家サイバー統括室は、政府機関等のサイバーセキュリティ対策のための統一基準群等を公表しているほか、今後「重要インフラのサイバーセキュリティ対策のための統一基準」を施行する。また、各府省庁も分野別のガイドラインを公表している。

[11] 脅威ハンティングの実施を通じて得られる知見には、必要なログの不足、管理されていない資産の把握、システムの設定不備等の対策不備の発見等が想定される。

３．脅威ハンティングの普及促進・実施等の対象組織

巧妙化・高度化したサイバー攻撃は、情報の窃取に留まらず、重要なシステム等の機能停止をもたらし得ることから、当該攻撃による被害によって我が国に深刻・致命的な影響を生じさせるおそれがある組織において脅威ハンティングの実施が望まれる。これらを踏まえ、本基本方針では、当該組織を脅威ハンティングの普及促進・実施等の対象組織（以下「対象組織」という。）として位置付ける。

具体的には、政府機関、独立行政法人、指定法人[12]、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が対象組織に該当する。

４．本基本方針における官民の役割

本基本方針においては、対象組織がサイバーセキュリティ対策の観点で実施する脅威ハンティングに加えて、政府が主導して我が国に深刻・致命的な影響を及ぼし得るサイバー脅威への対応の観点で実施する脅威ハンティングも念頭に置く。すなわち、我が国全体のレジリエンスを向上させるため、潜在的な侵害や不審な挙動の探索のみならず、国家を背景とする脅威アクターの発見にも寄与することを意識して取り組むことが重要である。

サイバーセキュリティ対策の観点で、対象組織は脅威ハンティングを実施するに当たって、対象となる情報システムやネットワーク等の利用状況を理解し、自組織の能力・体制等に応じて主導的に脅威ハンティングの成熟度[13]を高めていくことが期待される。これに対し、政府は対象組織の脅威ハンティングの実施に必要な能力習得・体制構築等の促進に資する取組を講じていくことが求められる。

他方、我が国に深刻・致命的な影響を及ぼし得るサイバー脅威への対応の観点で、政府は国内外のサイバー脅威に関する情報を集約・分析し、対象組織に対し脅威ハンティングの実施を必要に応じて慫慂する。国家サイバー統括室等は、国家安全保障局のほか、必要に応じて対象組織の所管省庁とも連携しつつ、サイバー脅威の発見につながる情報等を対象組織に提供する。こうした取組を通じて得られた結果や知見を各対象組織が政府と共有することで、我が国全体における巧妙化・高度化したサイバー攻撃による被害の拡大防止に寄与することが期待される。

その上で、対象組織が組織内の人材を十分に確保できない場合等には、必要に応じて外部組織への業務委託（以下「外部委託」という。）や政府による助言・支援の受入れを行うことが望ましい。政府による支援の受入れには、対象組織と政府との間での緊密な情報共有及び対象組織における政府による支援への理解が不可欠である。この点、対象組織が求める支援内容に応じて、国家サイバー統括室が中心となり、警察及び防衛省・自衛隊等が講じ得る支援を円滑に活用できるようにする。

---

[12] ここでの指定法人は、基本法第 13 条の規定に基づきサイバーセキュリティ戦略本部が指定する法人を指す。

[13] 例として、すぐに取り組み始められる初期段階から、データ分析や自動化を活用して継続的に脅威を発見・共有できる最適化段階まで、段階的に整理される。

５．我が国に深刻・致命的な影響を及ぼし得るサイバー脅威への対応において認識すべき事項

Ⅱ．４．で言及した我が国に深刻・致命的な影響を及ぼし得るサイバー脅威への対応の観点で政府や対象組織に含まれる民間事業者が役割を果たしていくためには、以下の認識を持つ必要がある。

国家機能及び国民生活に直結するサービスを提供する対象組織が、国家を背景とする脅威アクター等による巧妙化・高度化したサイバー攻撃の標的とされた場合、我が国に深刻・致命的な影響を及ぼす懸念がある。この点、対象組織に含まれる民間事業者のサイバーセキュリティの向上を目的に、政府が率先して脅威ハンティングを当該民間事業者に普及促進することはもとより、国家安全保障のために必要と認められる場合には、当該民間事業者が求める支援内容に応じて、我が国に深刻・致命的な影響を及ぼし得るサイバー脅威を当該民間事業者が発見・対処することを政府自ら支援することが必要不可欠である。

また、サイバー攻撃に起因するサービス停止リスクが高まる中、政府が提供する脅威ハンティングをはじめとするサイバーセキュリティ対策支援を当該民間事業者が積極的に受け入れることは、民間事業者のセキュリティ投資における費用対効果の観点からも合理的である場合もある。一般に、我が国に深刻・致命的な影響を及ぼし得るサイバー脅威への対処に必要な専門人材の確保・育成及び最新の脅威インテリジェンス基盤の整備において、民間事業者が単独で取り組む場合には相当程度の費用負担を要するが、政府との連携を通じて政府特有の知見・ツール・既存の能力を共同活用することによって、同等以上の防護水準を低廉な費用で実現できる可能性がある。くわえて、サイバー攻撃の結果として生じ得る事業継続費用や情報漏えい等に伴う法的対応費用、信用失墜による経済的損失等を未然に抑制する効果は大きいと考えられる。このため、こうした被害の防止、拡大防止の観点から、当該民間事業者において、政府によるサイバーセキュリティ対策支援の受入れを積極的に検討することが望ましい。

６．脅威ハンティングに関連する人材・組織

我が国において脅威ハンティングを普及させるに当たっては、人材・組織に関する実情を踏まえた対応が必要である。対象組織においても、自組織における当該実情を把握して脅威ハンティングの実施に向けて取り組むことが重要である。

脅威ハンティングにおいて、サイバー脅威を発見する機会は必ずしも多くなく、その取組の成果が可視化されにくいことから、組織は脅威ハンティングを担当する人材の意欲を維持させる工夫が求められる。

また、経営層が脅威ハンティングの意義を理解し、実務者層（システム運用や脅威ハンティングを実施する担当者等）が自らの役割を果たすことができるように環境を整備することが重要である。特に、セキュリティ上の課題を経営課題や事業運営の観点に置き換えて経営層に伝える役割を担う橋渡し人材の存在が必要である。

さらに、脅威ハンティングは、システムの通常の挙動を把握する部署と攻撃手法やリスクの分析を担う部署等が緊密に連携することが望まれる。

くわえて、自組織だけで脅威ハンティングを実施できない場合には、外部委託も選択肢となるが、外部委託する際には外部組織を適切に管理・監督できるだけの知識・能力を自組織内に保持することが重要である。

III. 政府の主要な取組

Ⅰ．２．の目的を達成するべく、Ⅱ．４．で言及した役割を政府や対象組織が十分に果たせるよう、脅威ハンティングの普及促進や実施等に向けた政府の主要な取組事項を以下に掲げる。

○ 脅威ハンティングの普及促進に関する取組
- 対象組織における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
- 対象組織における脅威ハンティング活動の実効性向上

○ 政府による脅威ハンティングの実施等に関する取組

○ 国内外の官民連携／協働

１．対象組織における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

対象組織が脅威ハンティングを実施するためには、その意義等に関する意識改革を行った上で、Ⅱ．の基本的な考え方に加えて、以下の点への理解が重要である。政府は、脅威ハンティングの実施に必要な能力習得・体制構築等の促進を行うに当たって、これらの点に留意し、対象組織に脅威ハンティングに関する理解を浸透させていくことが求められる。

まず、Ⅱ．２．で言及した従来のサイバーセキュリティ対策の実施を前提として、必要に応じて外部委託しながら、脅威ハンティングを行うことができる人材の確保と組織体制・技術基盤等の整備等を実施することが必要である。これらの実施に当たっては、相応の投資・時間を要するため、組織の能力・体制等に応じて段階的に取り組んでいくことが重要である。

また、これらの取組を組織として実行に移していくためには、対象組織の経営判断が必要であり、脅威ハンティングを実施する意義のみならず、費用対効果等の面でも経営層の理解を得ることが不可欠である。さらに、脅威ハンティングを実施するには様々なログをある程度の期間にわたって取得し分析を行う必要があり、システム運用部署等の負担が増加する可能性もあることから、脅威ハンティングを実施する部署とシステム運用部署等との間で良好な関係性を構築することも必要となる。

くわえて、近年では OT システムのデジタル化も進展し、情報システムやインターネットに接続された機器経由の攻撃等により、OT システムに影響が及ぶリスクが高まっていることを踏まえると、対象組織においては、情報システムだけでなく、OT システムに係るリスク及び固有の要件・セキュリティ対策についての理解も踏まえた脅威ハンティングの実施が求められる。

以上を踏まえ、対象組織のうち、従来の対策の向上と併せて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を主な対象として、脅威ハンティングに必要な能力・体制・技術・役割等を学ぶ機会を通じて脅威ハンティングに関する理解を浸透させるとともに、脅威ハンティングの実践を通じて自組織が抱える課題を把握できるようにする必要があるため、国家サイバー統括室は、以下の３点に取り組む。あわせて、政府機関等のサイバーセキュリティ対策のための統一基準群[14]・「重要インフラのサイバーセキュリティ対策のための統一基準」等の各種基準や関係省庁の施策との連携を検討し、連携する施策の双方が効果的な取組になるように促す。

[14] 政府機関等のサイバーセキュリティ対策のための統一基準群とは、国の行政機関及び独立行政法人等の情報セキュリティ水準を向上させるための統一的な枠組みであり、国の行政機関及び独立行政法人等の情報セキュリティのベースラインや、より高い水準の情報セキュリティを確保するための対策事項を規定している。

(1) 前提となる従来のサイバーセキュリティ対策や、脅威ハンティングの実施に必要な能力習得や体制構築等に向けた取組、さらに、AI 等の先端技術の脅威ハンティングでの活用可能性や外部委託する際の役割分担等を整理し、脅威ハンティングを実施しようとする組織等が参照可能なガイドブック等を作成・提供する。
(2) (1)の資料も活用しつつ、経営層、実務者層に加え、経営層と実務者層との橋渡し人材等を対象にした研修機会等を提供する。
(3) 対象組織における脅威ハンティングの実施に必要な能力・体制等の課題を可視化し、改善策等の検討を目的にした実習機会等を提供する。

また、総務省は、対象組織が脅威ハンティング等の実施に必要な能力習得のための大規模演習基盤を国立研究開発法人情報通信研究機構（NICT）に整備し、本基本方針に記載の取組の実施主体や対象組織での必要性に応じて当該基盤を活用できるようにする。このほか、本基本方針に記載の取組成果を踏まえつつ、当該基盤を活用した実践的な演習の機会を提供する。また、総務省はNICTに当該基盤を整備するに当たり、演習の実効性向上のための技術開発を推進する。さらに、NICTを通じて実施・運用する、実践的サイバー防御演習「CYDER」や分野別実践演習の開発・実施基盤「CYROP」[15]等の既存の取組についても、必要な組織・人材が脅威ハンティングの意義や有用性について理解し、その組織的な実施に向けた体制構築等に資するよう、内容の充実化を図る。

くわえて、経済産業省は、独立行政法人情報処理推進機構（IPA）の産業サイバーセキュリティセンター（ICSCoE）を通じて、社会インフラ・産業基盤を有する民間事業者などにおいて将来的に経営層と実務者層との橋渡し人材を対象に、情報システム及びOTシステムに係るリスクを認識しつつ必要なサイバーセキュリティ対策を総合的に判断できる人材に育成するための中核人材育成プログラム等を提供しており、同プログラム等において、対象組織におけるOTシステムに係るリスクも踏まえた脅威ハンティングの実施に必要な能力習得を図る。

２．対象組織における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効果的に実施するに当たっては、信頼性の高い情報源から様々な情報を収集・分析する必要があることから、サイバー脅威や攻撃手法等に関する情報等を政府が状況に応じて提供することも対象組織における脅威ハンティングの実施に効果的であると考えられる。

上記を踏まえ、国家サイバー統括室は、仮想環境等を活用して、サイバー脅威や攻撃手法等に関する分析を行うほか、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を主な対象として、情報等を受領した組織が自組織のシステム環境に応じた脅威ハンティングを容易に実施できるよう、当該分析結果を含む政府が保有する情報等を提供し、必要に応じて助言・支援を行う。また、経済産業省がIPAを通じて運営するサイバーレスキュー隊（J-CRAT）において、巧妙化・高度化したサイバー攻撃の被害組織に対して、脅威ハンティングを含む初動対応支援を行う。

さらに、こうした取組の一環として、警察及び防衛省・自衛隊は、サイバー攻撃被害による、国民生活・経済活動、ひいては国家安全保障への影響が特に深刻であると考えられる対象組織に対し、その求める支援内容に応じて、自身が有する高度な脅威ハンティングに関する能力を活用

[15] CYROP（CYber Range Open Platform）とは、CYDER等の演習基盤・教材を国内組織に展開し、各組織において分野に応じた実践的演習を容易に開発・実施可能とするNICTの演習基盤のことをいう。

した支援を行う。

３．政府による脅威ハンティングの実施等に関する取組

（1）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

脅威ハンティングに関して政府が行う取組の実効性を確保するためには、当該取組を実施する政府担当者と対象組織の脅威ハンティング担当者等との間の平素からの円滑なコミュニケーションが重要であり、当該政府担当者の脅威ハンティングに関する専門的知識・能力の維持・強化も必要となる。また、対象組織における脅威ハンティングの実施プロセスだけでなく、当該プロセスに関する経営層の意思決定、実務者層が行うログ分析、橋渡し人材が担う組織横断的な調整等の具体的な業務内容について、当該政府担当者も十分に理解する必要がある。

上記を踏まえ、国家サイバー統括室は、当該政府担当者に対して、脅威ハンティングに関する専門的知識・能力の維持及び強化並びに対象組織が行う脅威ハンティング業務の理解に資する講義・演習等を組み合わせた研修等を実施する。

一方、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しては、必要に応じて政府が脅威ハンティングを主導して実施する必要がある。

そのため、国家サイバー統括室は、国家安全保障局と緊密に連携して総合調整機能を発揮し、国内外の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、必要に応じた対象組織に対する脅威ハンティングの実施の慫慂、政府が保有する情報の提供を含む脅威ハンティングに関する対象組織への支援とそれらに基づく対象組織からの結果等の受領等、官民一体となった脅威ハンティングの実施を推進する。この点、国家安全保障のために必要と認められる場合には、対象組織に含まれる民間事業者と十分な調整を経た上で、我が国に深刻・致命的な影響を及ぼし得るサイバー脅威を当該民間事業者が発見・対処することを政府自ら支援する。

（2）平時から有事までシームレスに対応するための取組

ア　サイバー空間の匿名性を悪用した事案については、認知段階では、事案の背景や目的等が判然としないことが多いものの、国民の生命、身体及び財産の保護の任に当たる警察として、平時から有事に至るまでシームレスに対処する必要がある。そのため、警察においては、従来からサイバー攻撃に関する能動的な解明と脅威ハンティングを含む対策の充実に向けた官民連携の取組を推進しており、サイバー攻撃被害が発生した具体的な事案を認知していない場合においても、全国の対象組織等からの依頼に基づきセキュリティ診断を実施し、診断結果に基づく注意喚起を実施しているほか、対象組織等で構成されるサイバーテロ対策協議会や高い先端技術を有する全国の民間事業者等で構成されるサイバーインテリジェンス情報共有ネットワーク（CCI ネットワーク）の枠組みを通じて、全国警察が収集したサイバー攻撃者に関する各種情報を提供するなど、サイバー攻撃対策に資する注意喚起等を実施している。また、セキュリティ診断等の結果として得られた脆弱性情報等を警察庁で集約・分析して、サイバー攻撃の実態解明を行っている。引き続き、これらの取組を継続するとともに、情報提供や注意喚起の機会等を通じた脅威ハンティングに係る助言・支援についても検討する。

こうした脅威ハンティングをはじめとするサイバーセキュリティ施策の推進に当たっ

ては、優秀な人材の確保と高度な解析技術を持つ職員の育成が不可欠であることから、警察においては、サイバー事案への対処に係る高度な専門的知識・技術を有する人材を確保・育成するための取組を計画的に推進するとともに、同人材が、その専門性を継続的に活かすことができるようなキャリアパスの構築に取り組んでいるほか、従来の枠組みにとらわれない形で独自の専門採用を推進して人材の確保に努めている。また、確保した人材を育成し、脅威ハンティング等にも対応できるよう、高度かつ実践的な訓練を行うためのサイバー演習環境の整備・構築を進め、高度な解析技術を持つ職員の育成を行うために、最新の技術を有する民間事業者や研究機関との技術協力を推進するなどしている。これらの取組を継続するとともに、端緒情報が増加し、警察が実施する脅威ハンティングの件数も増加することが見込まれることから、サイバー特別捜査部等における必要な体制の一層の充実・強化に努める。

このほか、人的・物的資源を効率的かつ最大限に活用するため、全国警察を結ぶネットワークにより、高度な解析を実施するためのソフトウェアの共有・利用や相互支援を可能とする解析基盤装置や、暗号により隠ぺいされたデータ等の解析を行う高速演算装置を運用するとともに、最新の資機材の整備を進めるなど、サイバー事案の対処に必要な資機材の整備・高度化を推進している。こうした資機材は、脅威ハンティングの有効性を高めることにも資することから、引き続き、必要十分な資機材の整備・高度化を推進する。

イ　防衛省・自衛隊は、従来から脅威ハンティングの実施及びその能力強化を行っている。これは、脅威ハンティングにより得られるサイバー脅威情報の収集・蓄積・分析によりサイバー攻撃キャンペーンの特徴や弱点を把握し、平時から有事に至るまで、我が国に深刻・致命的な影響を与えるサイバー攻撃キャンペーンにシームレスに対応するとともに、自衛隊及び在日米軍の任務保証[16]を確保するという考え方による。

具体的には、現在の防衛力整備計画（令和４年 12 月 16 日国家安全保障会議決定及び閣議決定）の下、令和５年度以降、自衛隊の運用する情報システムを対象に脅威ハンティング能力を強化するとともに、能力強化に必要となる資機材の整備や人材の確保等を進めており、引き続き取り組む。

他方、国家を背景とする脅威アクターは、政府機関はもとより政府機関以外の対象組織もターゲットとすることが考えられる。平時から有事に至るまでシームレスに我が国におけるサイバー攻撃の被害の防止、拡大防止を図り、また、自衛隊等の任務保証を確保するためには、対象組織の防護に加え、対象組織が直面するサイバー脅威情報の収集等がますます重要となる。このような観点から、防衛省・自衛隊として、今後は、対象組織に含まれる民間事業者等からの脅威ハンティングの要望にも可能な限り幅広く対応できるよう、脅威ハンティングに関する能力や体制の強化を一層積極的に進めることが重要である。具体的には、自衛隊の運用する情報システムのみならず、OT システムを含む当該民間事業者

[16] 任務保証とは、企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、かかる「任務」を着実に遂行するために必要となる能力及び資産を確保することをいう。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方である。

等が使用するシステムへの脅威ハンティングを適切に支援できるよう、必要となる資機材の整備や人材の確保、必要な隊員教育等の実施に向けた検討を進める。また、対象組織への脅威ハンティングの支援のためには、平素から国家サイバー統括室を含む関係省庁や対象組織との間で適切にコミュニケーションを図ることが重要であり、そのための要員の確保や枠組みの検討を行う。

４．国内外の官民連携／協働

政府による脅威ハンティングに関する取組の効果を高めるには、官民の継続的なコミュニケーションにより、政府による対象組織の的確なニーズ把握及び当該取組に関する政府と対象組織間の双方向のフィードバックが不可欠である。また、脅威ハンティングにより得られたサイバー脅威情報等は、サイバー攻撃キャンペーンやその他サイバー脅威への国家サイバー統括室による対応に活用し得るものである。具体的にはサイバー脅威情報の適切な共有は、被害の防止、拡大防止に資するほか、注意喚起やパブリック・アトリビューション、アクセス・無害化措置、その他の能動的サイバー防御等に関する各種施策の実施のために有用な場合がある。さらに、対象組織間において脅威ハンティングに関する知見が相互に共有されることは、脅威ハンティング能力の底上げに寄与すると考えられる。

そのため、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（以下「新協議会」という。）等の活用により、国内の官民間の連携を更に促進・強化していくことが重要である。その際、政府機関内の他の取組との連携や、脅威ハンティング以外のサイバーセキュリティ対策に係る施策との連動にも配意する。

以上を踏まえ、以下の２点を実施する。

⑴ 国家サイバー統括室は、新協議会等を活用し、Ⅲ．１．で言及したガイドブックや研修機会等の提供、Ⅲ．２．で言及した情報等の提供や助言等を行う。

⑵ 国家サイバー統括室は、国内のニーズに一元的に対応するために他の官民連携に係る取組を含め、ワンストップで機動的な支援を行う。

また、事象の影響が容易に国境を超えるというサイバー空間の特性を踏まえると、巧妙化・高度化したサイバー攻撃に対して我が国が単独で対応することは困難であり、国際連携の推進が不可欠である。同盟国・同志国等との情報・運用面での協力の強化を進めるに当たり、脅威ハンティングについても、その高度化に資する各種情報の相互共有等を進め、国内での脅威ハンティングの普及促進・実施等に係る取組の充実に役立てるとともに、かかる情報を国際的に共有することを目指す。

Ⅳ. 本基本方針の見直しについて

本基本方針は、脅威ハンティングの普及状況、対象組織の能力・体制状況等に応じて、今後適時適切に見直すものとする。