資料３

サイバー対処能力強化法に基づく基本方針の策定に向けて

令和７年９月
内閣府政策統括官（サイバー安全保障担当）

サイバー対処能力強化法：基本方針に関する規定

■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）

（基本方針）

第３条　内閣総理大臣は、**重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針**（以下この条において「基本方針」という。）**の案を作成し、閣議の決定を求めなければならない**。

２　基本方針においては、次に掲げる事項を定めるものとする。

一　**重要電子計算機に対する特定不正行為による被害の防止に関する基本的な事項**

二　第十三条に規定する**当事者協定の締結に関する基本的な事項**

三　**通信情報保有機関における通信情報の取扱いに関する基本的な事項**

四　第三十七条の規定による**情報の整理及び分析に関する基本的な事項**

五　**総合整理分析情報の提供に関する基本的な事項**

六　第四十五条第一項に規定する**協議会**（第二十九条及び第三十七条において単に「協議会」という。）**の組織に関する基本的な事項**

七　前各号に掲げるもののほか、**重要電子計算機に対する特定不正行為による被害の防止に関し必要な事項**

３　内閣総理大臣は、第一項の規定による**閣議の決定があったときは、遅滞なく、基本方針を公表**するものとする。

４　第一項及び前項の規定は、基本方針の変更について準用する。

御議論いただきたい事項：その１

重要電子計算機に対する特定不正行為による被害の防止に関する基本的な事項

□ 本法による各種措置を行うこととなった背景

- 平素より**国家を背景として、重要インフラの機能停止や機微情報の窃取等を目的としたサイバー攻撃**が行われており、**サイバー分野における安全保障の確保が切迫した課題**となっている。このような認識の下、「**国家安全保障戦略**」では、**サイバー安全保障分野の対応能力を欧米主要国と同等以上に向上させる**こととし、**能動的サイバー防御を導入する**こととした。

□ 政府内の連携と総合調整

- 法目的を効果的に実現するため、**関係行政機関等は内閣府に対して必要な協力を行う**とともに、内閣府は法に基づき整理・分析した情報を必要な関係行政機関等に速やかに提供するなど、**相互に緊密に連携協力をする**。

□ 事業者等との連携

- 政府が率先して情報を提供し官民双方向での情報共有を促進するなど、**官民連携を強化し、我が国全体のサイバーセキュリティの強化を図ることが必要**。また、情報の整理・分析等に当たっては、**関係諸外国との連携に努めていく**。

□ 通信の秘密の尊重

- **通信の秘密は、最大限に尊重されなければならず、法に基づく通信情報の利用に当たっては**、法に規定する規律等の趣旨及び内容について、関連業務に携わる全ての**関係職員が十分な認識を持ちつつ、厳格に業務に取り組む**ことを徹底する。

□ 重要電子計算機の定義の考え方

- 法２条２項１号に規定する重要電子計算機については、**国の行政機関、地方公共団体等が使用する電子計算機**に関し、**管理される重要情報との関わり方又は重要な情報システムとの関係に着目**して**重要な電子計算機の範囲を明確化する**。
- 同項２号に規定する特定重要電子計算機には、**特定重要設備に限らず、特定重要設備と接続され、一定の情報のやり取りが可能な情報システム等が該当**。その詳細は、事業者等との協議を経て、**特別社会基盤事業者の業態別に明確化する**。

□ 機械的情報の考え方

- 機械的情報の範囲は、**分析に必要となる情報が適切に含まれる**よう検討するとともに、**意思疎通の本質的な内容に当たらないものに限定されるよう情報の項目を精査**し、適切な手続を経た上で内閣府令にこれを規定する。

御議論いただきたい事項：その２

第13条に規定する当事者協定の締結に関する基本的な事項

ロ 基本的な考え方

- **当事者協定の締結は任意**であるため、内閣府は、**当事者協定による対策の必要性について理解を求める**とともに、**当事者協定の内容や、発生する対応・負担等の事項を当事者が適切に理解**した上で、当事者協定が締結されるようにする。

ロ 当事者協定の締結に関して配慮すべき事項

➢ 当事者協定制度の運用に関する配慮事項

- 重要電子計算機に対する国外通信不正行為による**被害の防止の観点から優先度を考慮**し、当事者協定を締結する**重要性の高い特別社会基盤事業者等から当該締結に向けた協議を求めていく**。
- 当事者協定の締結により**協定当事者が受けることができるメリットが増進**されるよう努め、及びその**メリットの周知・啓発等**に努める。
- 当事者協定に基づき提供した**通信情報が法の規律により保護されること等について丁寧な説明**を行う。

➢ 当事者協定の締結に向けた協議に関する配慮事項

- 当事者協定の締結に向けた協議においては、必要事項の説明など**協議の相手方の判断に資するよう丁寧に協議を行う**よう努める。
- **当事者協定の締結が事実上の強制とならないよう十分配慮**するとともに、**当事者協定を締結しなかった者に対して一切の不利益な取扱いをしない**。
- **当事者協定の内容に関する**予見性を高めるため、**ひな型を事前に作成**し、協議に際して提示できるようにしておくことを検討する。

➢ 当事者協定に基づく他目的利用に関する配慮事項

- 法23条４項１号の規定による特定被害防止目的以外の目的のための選別後通信情報の利用又は提供（**他目的利用**）**については、法目的の範囲内で行う必要**があり、選別後通信情報は**サイバーセキュリティの対策においてしか利用又は提供しない**。
- 他目的利用については、**協定当事者から個別に具体的かつ明確な同意を得て、その範囲内で利用する必要**がある。また、同意の範囲が明示された書面を取り交わすなど**実効的な観点から明確に同意を得る**ことも重要である。

御議論いただきたい事項：その３

通信情報保有機関における通信情報の取扱いに関する基本的な事項

□ 基本的な考え方

- 法に基づく通信情報の利用に関する制度では、**通信の秘密等に十分に配慮するために様々な制約を課している**ところ、その利用に当たっては、**通信情報保有機関は、法による規定を適切に遵守して、適正に通信情報を取り扱う**。

□ 通信情報の取扱いに関して配慮すべき事項

➢ 通信の秘密への十分な配慮

- 法に基づく**通信情報の利用を通信の秘密との関係で必要やむを得ない限度に留める**ため、その業務に携わる全ての職員は、**法５章及び７章における通信情報の取扱いに係る規律を厳格に遵守して適正に業務を遂行することを徹底**する。

➢ 安全管理措置についての考え方

- 内閣府令に定める通信情報の安全管理措置は、**通信情報の取扱いの業務を行わせる職員の範囲等の組織的な安全管理措置**や**通信情報のアクセス権限の付与等の技術的な安全管理措置**、**通信情報を取り扱う区域の設定等の物理的な安全管理措置**などの各種措置について、**適切な手続を経た上で規定**する。

➢ 通信情報の利用に係る機能強化の考え方

- 高度化・巧妙化するサイバー攻撃にも有効に対処できるよう、**通信情報の自動選別や整理・分析等を行うためのシステム・設備の的確な整備やその分析能力の向上を図る**ほか、**適切な人材確保・育成を図る**など、**政府機関における機能強化を適切に推進**する。

➢ 電気通信事業者の協力に関する配慮事項

- 法20条の規定による**電気通信事業者の協力**については、**正当な理由がある場合には当該協力を拒み得る**ものであり、これに該当しない場合でも、協力に関する**負担が過度にならないように配慮**し、**協力の内容等について事前に丁寧に説明を行う**ものとする。

➢ 他法令の遵守に関する配慮事項

- 通信情報の利用に関する事務の実施においては、個人情報保護法をはじめとした**他法令を適切に遵守する必要がある**ことに留意。
- 一方、**他の法律に基づき通信情報の提供を求められた場合**には、提供しなければならない場合を除き、これを**利用又は提供しない**。

御議論いただきたい事項：その４

第37条の規定による情報の整理及び分析に関する基本的な事項

□ 報告等情報の収集の考え方

- **特定重要電子計算機の届出情報**に関しては、内閣府が横断的に管理し、必要な整理・分析を行った上で、**特別社会基盤事業者に対して、脆弱性情報等を提供するために活用する**。届出を求めるに当たっては、**事業者の負担にも配慮する**。
- **特定侵害事象等の報告**については、報告を行う事業者において判断に迷うことがないよう、**その閾値が明確となるよう設定する**。報告内容については、**タイミングに即して過度な負担とならないよう設定する**。また、事業者自らが直接管理していない特定重要電子計算機に係る報告については、その**情報の取得可能性にも配慮する**。

□ 収集した情報の整理及び分析の考え方

- 内閣府は、重要電子計算機に対する特定不正行為による被害の防止に資する情報を作出し、これが有効に活用されるよう、収集した情報について、**総合的かつ業種横断的に整理及び分析を行い、総合整理分析情報を作出する**。
- 総合整理分析情報にはその取扱いに十分な配慮が必要となる通信情報が含まれることから、内閣府は、**提供用総合整理分析情報として、総合整理分析情報を加工して選別後通信情報を含まない情報を作出する**。
- 提供用総合整理分析情報には秘密が含まれ得ることから、広くインフラ事業者等に対して提供するため、内閣府は、**周知等用総合整理分析情報として、提供用総合整理分析情報を加工して秘密を含まない情報を作出する**。

□ 関係機関等への協力の要請

- 内閣府は、**効果的な総合整理分析情報を作出するため、必要に応じて関係機関等に情報の提供その他必要な協力を求める**こととする。

□ 事務の委託に関する考え方

- 具体的には、**特定重要電子計算機の届出情報や特定侵害事象等の報告情報等の内容の整理・分析**、**重要電子計算機の脆弱性情報の整理・分析**、特定重要電子計算機の届出情報と特定侵害事象等の報告情報や脆弱性情報との**照合等の事務を委託することが想定**される。

御議論いただきたい事項：その５

総合整理分析情報の提供に関する基本的な事項

□ 総合整理分析情報等の提供先と提供する内容の考え方

分類	考え方
➢ **行政機関等**に対する情報提供	内閣府において、**行政機関が使用する重要電子計算機の被害発生の可能性を把握した場合**や、**特別社会基盤事業者における役務提供に支障を及ぼすおそれがあると認める場合**、**特定の選別後通信情報がアクセス・無害化措置に資すると認める場合**等には、該当する行政機関等に対し、**対策や措置に必要となる情報を、速やかに提供する**。
➢ **外国の政府等**に対する情報提供	①当該提供が法の規定による**提供目的の制限に適合するかを個別かつ適切に判断する**とともに、②提供する外国の政府等が法に規定する**情報の取扱いに係る適切な措置を講じていることを明示的に確認する**。
➢ **協議会の構成員**に対する情報提供	内閣府は、**提供用総合整理分析情報**を提供する。例えば、**サイバーの専門家が求める技術情報**に限らず、**経営層の判断に必要となる攻撃の目的や背景等に関する情報**を、適切なタイミングで積極的に提供する。
➢ **特別社会基盤事業者**に対する情報提供	内閣府から情報提供を受けた特別社会基盤事業者の所管省庁は、特別社会基盤事業者に対して**、攻撃技術情報などの周知等用総合整理分析情報**を積極的に提供する。
➢ **電子計算機を使用する者**に対する周知等	内閣府は、重要電子計算機を使用する者に限らず、特定不正行為に用いられるおそれのある電子計算機を使用する者や、重要電子計算機の維持管理を任されている者、その他の者に対して、**周知等用総合整理分析情報**を提供する。
➢ **電子計算機等供給者**に対する情報提供、**脆弱性情報に係る情報提供**	内閣府又は電子計算機等供給者の所管省庁は、必要に応じて、**公表前の脆弱性情報をその重要電子計算機の供給者に対して迅速に提供する**。また、脆弱性情報の公表に際しては、利用者が膨大な脆弱性情報の中から優先的に対応すべきものを特定できるよう、**国内で悪用されている脆弱性情報を一元的にわかりやすく発信できるよう努める**。また、本法による官民連携の強化に係る規定やその趣旨も踏まえ、**関係省庁・関係機関による脆弱性関連情報の取扱いに関する制度の見直しを検討する**。

御議論いただきたい事項：その５（続き）

総合整理分析情報の提供に関する基本的な事項

□ 情報提供に当たっての関係行政機関の連携

- 法に基づく内閣府からの情報提供や関係行政機関等からの情報提供において、**特に緊急性の高いものについてワンボイスで機関ごとにその内容に差異が生じないよう、関係行政機関等の間で緊密に連携を図る**。

□ 守秘義務・安全管理措置の具体的内容

- 特別社会基盤事業者の所管省庁及び内閣府は、情報の安全管理のために必要かつ適切な措置として、例えば、**職員研修等の組織的な安全管理措置**や**保管庫の施錠等の物理的な安全管理措置**、**電子ファイルのアクセス制御等の技術的な安全管理措置**などを講じる。

□ 情報提供に当たって必要な配慮

- 政府は、各種の情報を提供するに当たっては、その情報が重要電子計算機に対する特定不正行為による被害の防止に有効に活用されるよう、情報を整理し、**正確な内容を適切なタイミングで情報提供するよう努める**。また、情報提供後も、**情報提供を受けた機関からのフィードバック等を踏まえて、情報提供のあり方についても不断に改善を図っていく**。
- また、**政府に情報提供した事業者が不利益を被らないよう、**情報提供した事業者以外に対して情報提供を行う際には、当該事業者に関する秘匿性の高い情報を削除して情報提供を行うこと等に取り組み、**事業者等の権利利益の保護に十分に配慮する**。また、情報提供した事業者に対しては、**政府から積極的にフィードバック等を行い、官民の情報共有がより活発となるよう取り組む**。

□ 事務の委託に関する考え方

- 法72条１項の規定により、電子計算機を使用する者に対する周知等の事務の一部を委託することができることとされている。具体的には、**周知等用総合整理分析情報の提供を行うべき者の整理やその提供等の事務を委託することが想定**される。
- また、法72条２項の規定により、電子計算機等供給者に対する脆弱性情報の提供等の事務の一部を委託することができることとされている。具体的には、**脆弱性情報に関する電子計算機等供給者との調整・公表等の事務を委託することが想定**される。

御議論いただきたい事項：その６

第45条第１項に規定する協議会の組織に関する基本的な事項

□ 協議会の趣旨

- 政府から特定不正行為による被害を防止するための情報を提供することや、被害の防止に資する情報を関係者間で共有・協議を行うこと等により、**協議会の構成員における被害を防止することを目的として、協議会を設置する**。

□ 協議会の取組内容・運営方針

- 協議会では、**政府から被害防止のための情報を提供すること**や**被害防止に資する情報を構成員間で共有・協議を行うこと**のほか、**政府から演習や初動対応支援等の機会を提供する**。

□ 協議会で共有されるべき情報・協議する内容

- 内閣府は、協議会の構成員に対して、**サイバーの専門家が求める技術情報に限らず、経営層の判断に必要となる攻撃の目的や背景等に関する情報を、適切なタイミングで積極的に提供する**。この情報の中には、**攻撃者の詳細な活動状況やインフラ設備の具体的な脆弱性に関する情報などの秘匿性の高い情報も含まれ得る**ことが想定される。
- また、協議会では、**被害防止のための対策や、被害防止情報を適正に管理するために必要な措置等について、構成員で協議を行う**。例えば、特定事案に関して被害組織間で被害状況や対策等に関する協議を行うこと等が想定される。

□ 協議会の構成員

- 協議会の構成員は、協議会で知り得た情報の適正な管理や資料の提出の求めがあった場合における対応が必要となるため、**内閣府が必要と認めた構成員として協議会に参加いただくに当たっては、当事者から事前の同意を得る**。

□ 守秘義務・安全管理措置の具体的内容

- **協議会の構成員に対しては、一定の情報管理及び守秘義務を設ける**。加えて、**政府が保有する秘匿性の高い情報**についても適切な情報管理の下で協議会の構成員が取り扱えるようにするために、**重要経済安保情報保護活用法に基づくセキュリティ・クリアランス制度の活用についても必要な検討をしていく**。

御議論いただきたい事項：その７

その他重要電子計算機に対する特定不正行為による被害の防止に関し必要な事項

ロ 基本方針の見直しに関する事項

- 政府は、**不断に取組状況の検証・評価を行う**こととし、**それに伴う制度の見直しを適時に行う**。また、**基本方針についても、国際情勢及び社会経済構造の変化等に応じて見直しを行う**。

ロ 官民連携に関する関係省庁・関係機関等との連携等に関する事項

- 重要電子計算機に対する特定不正行為による被害の防止に向けては、**関係省庁や関係機関は、各機関が保有する情報の共有など、緊密な連絡・協力が不可欠**である。特に、被害を受けた事業者の負担軽減や政府の対応迅速化、特定社会基盤事業者の安定的な役務提供の確保等の観点から、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や個人情報保護法、その他関連する業法を所管する省庁とは、相互に連携しつつ合理的な制度設計・運用に努める。
- **内閣府、国の行政機関、情報処理推進機構、情報通信研究機構その他関係者は、重要電子計算機に対する特定不正行為による被害の防止に関する事項について、法その他の法令、基本方針に基づき、相互に連絡・協力する**こととする。また、法に基づく内閣府の事務については、内閣官房の総合調整の下で実施する。

基本方針の策定に係るスケジュール案

- サイバー対処能力強化法に基づく「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針」を、本有識者会議での検討を踏まえ、本年中に策定するとともに、制度施行※に向けて、同方針に基づき、関係する政省令等の整備を進める。

※官民連携部分の施行は、法律の公布（令和７年５月23日）後１年６月を超えない範囲において政令で定める日
通信情報の利用部分の施行は、法律の公布後２年６月を超えない範囲において政令で定める日

【基本方針の策定】

令和７年５月	サイバー対処能力強化法の成立・公布
９月（本日）	第１回 有識者会議：基本方針に関する御議論
10月上旬目途	第２回 有識者会議：関係団体からのヒアリング【P】
10月中・下旬目途	第３回 有識者会議：基本方針に関する御議論
11月目途	パブリック・コメント（意見募集）の実施
12月目途	第４回 有識者会議：基本方針に関する御議論
	→ 基本方針の閣議決定

【基本方針の策定を受けた政省令等の整備】

令和８年４月目途	政令の整備、官民連携部分に係る省令等の整備
（公布後１年６月以内）	制度施行（官民連携部分）
	通信情報の利用部分に係る府令の整備
（公布後２年６月以内）	制度施行（通信情報の利用部分）

【参考】基幹インフラ事業者との意見交換（1/5）

- 今後の基本方針策定や政省令の検討に向け、本年７月末頃から、
  基幹インフラ事業者15業種（令和７年８月１日時点）への説明、意見交換の場を設けてきているところ。
- 意見交換では、特に以下の４点について運用に向けた現時点の考え方を説明。今後の検討に当たって、
  引き続きステークホルダとの意見交換を実施していく。
  ①特定重要電子計算機の届出（資産届出）について
  ②特定侵害事象等の報告（インシデント報告）について
  ③協議会・情報共有について
  ④情報共有システム（官民連携基盤）について
- これまでに事業者から寄せられた主なご意見、ご質問は以下のとおり。

総論

- ✓ そもそも「新法とはなにか。」という事業者も多いので、**丁寧な説明、周知を重ねてお願いする**。
- ✓ 新法施行準備として、**登録資産情報の洗出し、登録更新・インシデント報告・脆弱性情報受領等への態勢整備等に時間を要することが想定される**中、新法の運用ルールの開示スケジュールについて教えていただきたい。
- ✓ **経済安保、安全管理規程、セキュリティクリアランス、行動計画等、他の施策等との関係性がわかりづらい**。関係性を提示していただきたい。

【参考】基幹インフラ事業者との意見交換（2/5）

① 特定重要電子計算機の届出（資産届出）について

- ✓ **脆弱性情報を迅速に受け取れる点は大きなメリット**であると認識。一方で、対象範囲が広範に及ぶ場合、登録および更新（棚卸し）作業が大きな負担となることが懸念**。対象範囲については合理的かつ最小限になるよう、また、事業者ごとの実態に即した柔軟な運用を要望**。
- ✓ 経済安保法における特定重要設備の構成設備単位で登録を想定しているのか、構成設備よりも詳細な製品やサービスのバージョン等の情報まで登録を想定しているのか。例えばクライアントが含まれた場合、**OSのバージョン、設定、適応パッチ、アプリケーションとそのバージョンなど加速度的に管理対象が増えてしまうのを懸念**している。
- ✓ 当社において**重要設備がSaaSにあるため、その場合に登録すべき対象の考え方を明確化頂きたい**。
- ✓ 資産登録について、例えば、**事業者８社が同じ者にシステム管理を委託している場合、そのシステムの設備所有者が登録するということを検討してもらいたい**。
- ✓ 登録する資産は、特定社会基盤事業者である当社のみが実施し、グループ会社所有の資産は登録不要なのか。
- ✓ 経済安全保障推進法の特定重要設備・構成設備については、法施行前にそれらの特定のために当局への複数回の説明の機会があり、当局と合意した設備について、法施行後に導入した場合に届出が必要となった。特定重要電子計算機の届出は事後であるため、法施行後所定のタイミングで各社一斉に届出が必要になるという理解でよいか。
- ✓ 届出の対象について、特定重要電子計算機の導入時とあるが、これは経済安全保障推進法で用いられている言葉の意味と同様か。（新規導入だけでなく老朽取替等も対象か）

【参考】基幹インフラ事業者との意見交換（3/5）

② 特定侵害事象等の報告（インシデント報告）について

- ✓ インシデント発生時は、国への報告よりインシデント対応に注力する必要がある。**期限が設定された国への報告や資料提出が求められることにより、インシデント対応に影響することが懸念**される。労務管理上もギリギリの中での対応が迫られるのが実態であり、**事業者の過度な負担にならないよう、配慮いただきたい**。
- ✓ あるクラウド事業者のシステムを複数の事業者で利用している場合もあるため、**仮にクラウド事業者でインシデントが発生した場合に各社からバラバラと報告が必要となるようなことはない、あるいは報告内容を簡略化するなどの軽減策を検討いただきたい。**
- ✓ インシデントの報告期限は既に広く利用されている個人情報保護委員会の個人情報漏洩時の報告期限に合わせていただくのがよいのではないか。（速報３～５日以内、不正アクセスの場合確報６０日以内）
- ✓ 不審なアクセスは日々検知される。**ただしその時点で特定重要設備および特定重要電子計算機への影響有無はすぐには判断できず、相応の調査期間（場合によっては長期間のこともある）必要となる**ので、インシデント報告の期間などは、考慮いただきたい。
- ✓ 本法の報告対象となるのは、自社システムでの被害発生にとどまるか、使用しているSaaSや業務委託先での事象のうち自社に影響がある場合も含めるのか。

【参考】基幹インフラ事業者との意見交換（4/5）

③ 協議会・情報共有について

- ✓ 守秘義務がある前提ではあるものの、協議会には様々な企業が参加することが見込まれる。**協議会でインシデントを共有する場合**、守秘義務があるとしても企業の信頼失墜や存続にかかわるシステムの事案は、非常に機微であり、報告しにくいと考えられ、国益に資すると判断されるケースに限定すべきであり、**報告者が共有すべきと判断される必要最低限の情報に絞って報告することを可能にしていただきたい**。
- ✓ また、侵害をうけたシステム名の明記を避けるなどの報告項目を絞るなど、一定の配慮をしていただけるよう考慮いただきたい。
- ✓ 協議会について、メンバー数が多いと組織が機能しないのでは。また、義務や負担感はどのように考えているか。
- ✓ **「情報共有及び対策に関する協議会」と、既存の「サイバーセキュリティ協議会」、「重要インフラにおける各セプター」との役割分担について、ご教示いただきたい**。連絡系統や業務上の重複はないか。
- ✓ 協議会参加にあたり、罰則付きの守秘義務やクリアランス取得が求められているが、**取得手続きや運用負担が過大にならないよう、簡素化・合理化を要望する**。また、情報共有のメリットや、参加事業者への支援策も可能であれば明示して頂きたい。

【参考】基幹インフラ事業者との意見交換（5/5）

③ 協議会・情報共有について（続き）

- ✓ 事業者側の判断にはかなりのセキュリティスキルを必要とする場合が多い。**単純に脆弱性情報を提供するだけではなく事業者側の判断に役立てられるように整理された形で提供されることを望む**。
- ✓ 構成員に共有される情報で、含み得る秘密の具体的なイメージはあるか。（例えば個社が公開していないインシデント情報を、社名含め共有されることはあるか）**セキュリティの情報を共有頂く際は、攻撃の手口と対策（守り方）も共有いただけるとありがたい**。
- ✓ **まずは資産登録した事業者に対し早期警戒的に情報が提供され、事後的に広く社会に向けて注意喚起される運用も考えられないか**。
- ✓ **官民の様々な発信源から同一の脅威情報や脆弱性情報がバラバラに発信されており、量も多く、受け取る側での識別・分別に手間がかかっている**。これらを重複排除・不要な情報は入らない形で発信される統一プラットフォームとして整備され、情報の活用方法も示されるようにしてもらえるとありがたい。

④ 情報共有システム（官民連携基盤）について

- ✓ システムでDB登録、送信することで関連する報告先に同報できると良い。事業者側が複数の箇所に連絡をしなければいけないことになっているため、事業者からの報告は1か所であることが理想と考える。
- ✓ 他社のインシデントも公開可能な範囲で（匿名化するなどして）ナレッジとして閲覧できるようにしてほしい。特に同じ設備を使用している事業者でのインシデントは対策の参考になり得る。