資料2-3

サイバー対処能力強化法の施行に伴う告示・ガイドライン見直しの方向性（案）

令和７年12月
内閣府政策統括官（サイバー安全保障担当）付
／内閣官房国家サイバー統括室

強化法施行に伴う告示・ガイドラインの見直しの基本的な考え方（案）

資料2-3

- 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。
- こうした中で、サイバー対処能力強化法（強化法）では、**行政機関や基幹インフラ事業者等が使用する、国家・国民の安全や国民生活・経済活動の観点から重要な電子計算機（重要電子計算機）の被害の防止を図る**ことを目的として、①**情報の収集**、②収集した**情報の整理・分析**、③整理・分析を踏まえて作成した**情報の提供**　の３つの機能を措置している。
- 脆弱性のうち、**重要電子計算機の被害防止の観点から必要と認められるもの**については、**政府に情報共有され、政府が**強化法及び同整備法の下で重要電子計算機の被害防止のため、また、サイバー安全保障の観点から**必要な対応を行う**ことができるよう、**脆弱性情報の取扱いに関する告示・ガイドラインの見直し**を行うこととしたい。

【強化法の枠組み】

① 情報の収集

通信情報の利用

（ア）当事者協定
（イ）同意によらず通信情報を利用する措置
（外外通信目的送信措置等）

官民連携の強化

（ウ）基幹インフラ事業者の一定の電子計算機（特定重要電子計算機）の届出義務
（エ）基幹インフラ事業者のインシデント報告義務
（オ）協議会の枠組

重要電子計算機の被害防止の観点から必要と認められる脆弱性に関する情報【告示・ガイドラインの見直し】

② 情報の整理・分析

- (ア)～(オ)の制度に基づき収集した情報
- その他の手法により取得した情報

整理・分析

次の情報をそれぞれ作成：

- 総合整理分析情報
（通信情報や秘密を含み得る）
- 提供用総合整理分析情報
（通信情報は含まないが秘密は含み得る）
- 周知等用総合整理分析情報
（通信情報や秘密は含まず）

③ 情報の提供

作成した総合整理分析情報等を被害防止等に役立てるため、次の者に適切に提供

- 行政機関等
- 外国の政府等
- 協議会の構成員
- 基幹インフラ事業者
- 電子計算機を使用する者
- 電子計算機等供給者（ベンダ）

【参考】サイバー対処能力強化法に基づく基本方針案：関係部分

資料2-3

サイバー対処能力強化法に基づく基本方針（案）より引用

■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（案）

第５章　総合整理分析情報の提供に関する基本的な事項

第２節　総合整理分析情報等の提供先と提供する内容の考え方

⑹ 電子計算機等供給者に対する情報提供等、脆弱性情報に係る情報提供

イ　脆弱性情報に係る情報提供

（略）

また、**関係省庁・関係機関による脆弱性関連情報の取扱い**については、**特に、国家を背景とした、より高度なサイバー攻撃への対処能力の強化のため**、重要電子計算機に関して官民連携を強化し、**政府が集約した情報を整理・分析し率先して民間事業者等に対し提供する**という、本法による官民連携の強化に係る規定やその趣旨に基づき、**政府が本法に基づく官民連携に係る事務を着実かつ効果的に実施できるよう、関係する告示・ガイドラインの必要な見直しを行う**。その上で、政府は、脆弱性に関して、重要電子計算機の被害防止のため効果的な情報提供を積極的に行う。

【参考】サイバーセキュリティ戦略改訂案：抜粋

サイバーセキュリティ戦略（案）より引用

■サイバーセキュリティ戦略（案）

Ⅲ．目的達成のための施策

１．深刻化するサイバー脅威に対する防御・抑止

（１）国が要となる防御・抑止

③ アクセス・無害化措置を始めとする多様な手段を組み合わせた能動的な防御・抑止

国家を背景としたサイバー攻撃キャンペーンを含め、日常的、持続的に行われているサイバー攻撃に対しては、**既存の防御の取組と、アクセス・無害化措置を始めとする能動的サイバー防御に係る新たな施策を組み合わせ、多様な手段で粘り強く能動的に対応していく**必要がある。そのための体制を早期に確立し、強化を図っていく。

具体的には、武力攻撃に至らないものの、安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、攻撃者のサーバ等への直接的な働きかけを通じ、攻撃による被害の防止を目的として、国際法上許容される範囲内でアクセス・無害化措置を実施する。この措置は、サイバー攻撃の脅威の抑止にもつながるものであり、我が国の総力を十全に活用する必要があるため、不正プログラムの解析等の高度なフォレンジック能力や攻撃者やサイバー攻撃の手口等を解明する高度情報分析能力等を有する警察と、武力攻撃事態等における高烈度なサイバー攻撃に対処するための高度なサイバー防衛能力等を有する防衛省・自衛隊が共同して対処する体制を構築する。

（略）

さらに、サイバー対処能力強化法に基づく新たな官民連携の枠組みと既存の取組を組み合わせ、高度な侵入・潜伏能力を備えた攻撃に関し、民間事業者等の情報ニーズを踏まえ、国からサイバー脅威情報等を積極的に情報提供する。これにより、民間事業者等が具体的な行動をとることが可能となり、サイバー攻撃による被害の防止にも寄与する。

以上のようなサイバー対処能力強化法等に基づく取組に加え、従前から行われているサーバ等の管理者と連携した任意のテイクダウン、パブリック・アトリビューション、攻撃手口の公表等も、極めて重要な措置である。**重大なサイバー攻撃の脅威の抑止、サイバー攻撃による被害の防止のためには、サイバー対処能力強化法等に基づく措置のみならず、あらゆる選択肢を、関係府省庁との緊密な連携を確保しつつ国家サイバー統括室の総合調整の下で検討し、実施していかなければならない**。

以上の能動的な防御・抑止の取組を行っていくため、関係府省庁等の間で共同訓練・演習を実施し、その結果を踏まえた知見や教訓の共有等を着実に進める。また、システムや資機材の整備・確保に当たっては、AIを始めとする先端技術の活用を積極的に検討するとともに、民間事業者が有する高い能力を最大限に引き出せるように努める。

あわせて、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や、高度化したサイバー攻撃に一国で対応することが困難であることを踏まえれば、サイバー分野における同盟国・同志国等との効果的な国際連携及び国際協調は極めて重要である。特に、アクセス・無害化措置やパブリック・アトリビューション等、能動的な防御・抑止に係る各種措置の検討、実施に際しては、同盟国・同志国等と必要な情報を共有し、共同して対応を図るなど適切に連携するとともに、国際的な枠組み・ルール形成等のための多国間の議論にも積極的に貢献する。

重要電子計算機の被害防止の観点から必要と認められる脆弱性及びその対応（例）

資料2-3

対象

- **重要電子計算機の被害防止の観点から内閣府への通知が必要と認められる脆弱性**とは、主に下記が考えられる。
  - **行政機関や基幹インフラ事業者等を狙う攻撃キャンペーンとの関連が疑われるもの**：
    既に悪用が確認されているもの、悪用の蓋然性が高いと考えられるもの　等
  - **悪用された場合に社会的な影響が大きいと疑われるもの**：
    基幹インフラ事業者の用いる電子計算機の脆弱性で悪用された場合にインフラ機能への影響が大きいと考えられるもの　等

対応（例）

- 種々の情報を踏まえた上で、**重要電子計算機の被害防止やサイバー安全保障上の観点からの総合的な判断の下で対応する**こととなるが、例えば、下記のような対応が考えらえる。

①　脆弱性情報の公表前段階からの基幹インフラ事業者等への個別情報提供

- 基幹インフラ事業者の電子計算機に関する**届出情報を基に**、脆弱性の悪用により基幹インフラ機能に大きな影響を及ぼす可能性が考えられる**基幹インフラ事業者**等に対して、**脆弱性情報が公表される前**から、強化法上の守秘義務の下で**情報提供**し、**監視強化、回避策の適用等の対応**を促す。

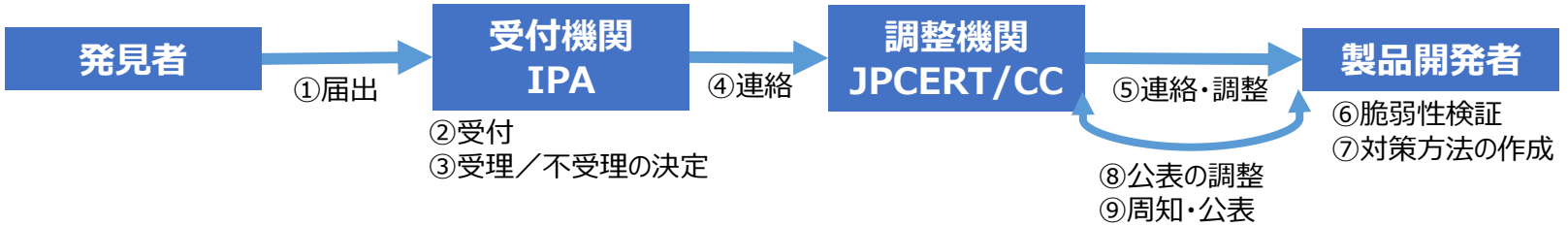
②　脆弱性情報の公表等より基幹インフラ事業者等の対応実施を優先

- 攻撃活動との関係性が確認されない等、すぐさま悪用される蓋然性が低いと考えられる脆弱性であって、悪用された場合に**基幹インフラ機能に多大な影響を及ぼすなど、社会影響が非常に大きいと考えられるもの**について、基幹インフラ事業者等に個別情報提供を行い、その**対応実施を優先した上で、脆弱性情報の公表を行う**。

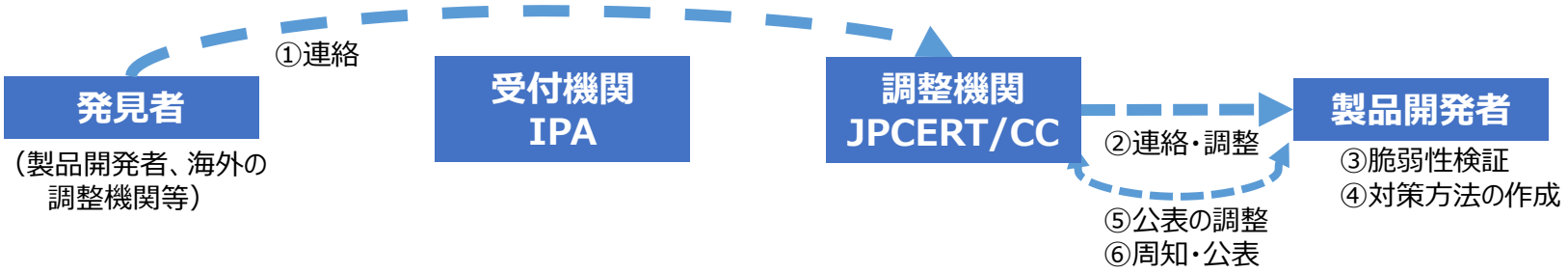
③　同盟国・同志国等の関係機関・関係団体との連携の中での対応

現行の脆弱性対応

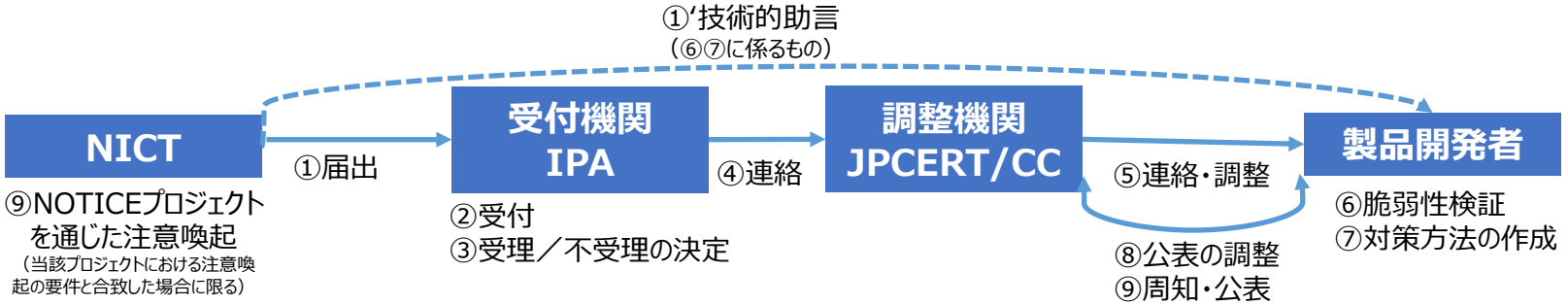
【基本ケース】
パートナーシップガイドラインに基づく発見者からの届出



【その他ケース１】
JPCERT/CCに発見者から直接連絡がいく場合



【その他ケース２】
NICTが未知の脆弱性を発見した場合

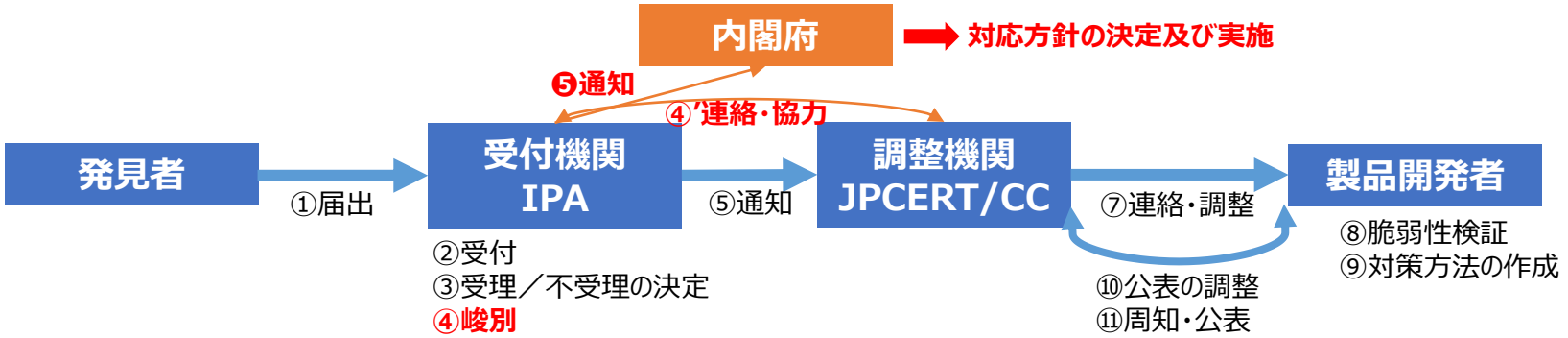


【見直しの方向性】
いずれのケースにおいても、**重要電子計算機の被害防止の観点から必要と認められる脆弱性が内閣府に通知されるよう見直す**。

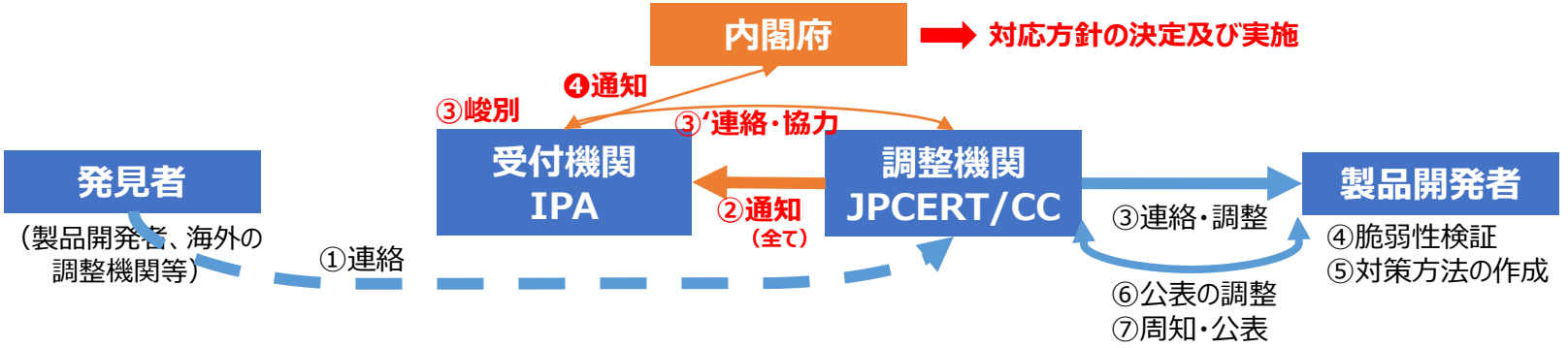
強化法施行後の脆弱性対応フロー（案）

受付機関IPAは、調整機関JPCERT/CCと必要な連絡・協力を行いつつ、認知した脆弱性のうち、**重要電子計算機の被害防止の観点から必要と認められるものに限って内閣府に通知する**。

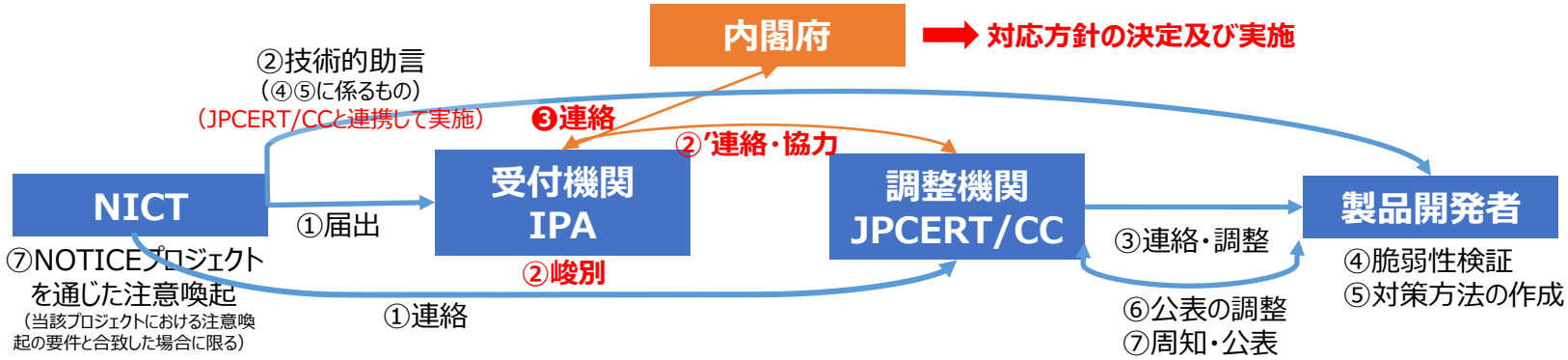
【基本ケース】
パートナーシップガイドラインに基づく発見者からの届出



【その他ケース１】
JPCERT/CC発見者から直接連絡がいく場合



【その他ケース２】
NICTが未知の脆弱性を発見した場合



※受付機関IPAは、重要電子計算機の被害防止の観点から内閣府への通知が必要と認められないと判断した場合にも、その後に取得した情報から、これに認められると判断する場合には**事後的に内閣府に通知する**こととする。また、JC-STARの申請審査又は運用課程において脆弱性を発見した場合にも、重要電子計算機の被害防止の観点から必要と認められるものを内閣府に通知する。

脆弱性情報の峻別・通知（案）

対象（再掲）

- **重要電子計算機の被害防止の観点から内閣府への通知が必要と認められる脆弱性**とは、主に下記が考えられる。
  - **行政機関や基幹インフラ事業者等を狙う攻撃キャンペーンとの関連が疑われるもの**：
    既に悪用が確認されているもの、悪用の蓋然性が高いと考えられるもの　等
  - **悪用された場合に社会的な影響が大きいと疑われるもの**：
    基幹インフラ事業者の用いる電子計算機の脆弱性で悪用された場合にインフラ機能への影響が大きいと考えられるもの　等

※届け出られた脆弱性情報を不受理又は処理を取りやめとする場合にも、その届け出られた脆弱性関連情報が上記に該当すると認められる場合には、受付機関IPAは内閣府に速やかに通知することとする。

受付機関・調整機関の取組

- **受付機関IPA**は、調整機関JPCERT/CCと必要な連絡・協力を行いつつ、認知した脆弱性に関して、**基幹インフラ事業者の電子計算機の届出情報との照合等を通じた分析**や**インシデント報告情報等との照合を通じた分析**、その他**IPAが有する脅威情報**等を踏まえて**峻別**を行い、重要電子計算機の被害防止の観点から必要と認められるものを**内閣府に速やかに通知する**。

  ※１　強化法第72条第１項に基づく情報の整理・分析の事務の委託として実施する。

  ※２　受付機関IPAは、重要電子計算機の被害防止の観点から内閣府への通知が必要と認められないと判断した場合にも、その後に取得した情報から、これに認められると判断する場合には**事後的に内閣府に通知する**。

- **調整機関JPCERT/CC**は、脆弱性の**悪用状況**や、脆弱性の**他製品（OEM製品等）への波及影響に関する分析**、その他JPCERT/CCが有する**技術的な知見**や**国際組織との連携を通じて得た情報**等を踏まえて、**受付機関IPA**が峻別するにあたって**必要な協力を行う**。

  ※強化法法第71条第２項の緊密な連絡・協力に係る規定に基づき実施する。

告示・ガイドライン見直しの方向性（案）

- 具体的には、**告示又はガイドラインに下記事項を新たに規定する**こととしてはどうか。

主な規定事項（案）

① **受付機関IPA**は、**調整機関JPCERT/CCと必要な連絡・協力**を行いつつ、認知した脆弱性のうち、**重要電子計算機の被害防止の観点から内閣府への通知が必要と認められるものを内閣府に速やかに通知する**。

② 内閣府は、受付機関IPAから通知を受けた脆弱性について、**重要電子計算機の被害防止やサイバー安全保障の観点からの総合的な判断の下で対応する**。その際、

- 内閣府は、必要に応じて、受付機関IPA及び調整機関JPCERT/CCに対して指示を行い、受付機関IPA及び調整機関JPCERT/CCは、正当な理由がある場合を除き、これに従うこととする。
- 内閣府は、強化法の規定に基づき、重要電子計算機に関する脆弱性について、**製品開発者への脆弱性情報の提供・調整や脆弱性への対応方法等の周知等を委託できる**。
- 内閣府は、重要電子計算機に関する脆弱性について、必要に応じて、関係する製品開発者の所管省庁※に情報提供を行い、内閣府から情報提供を受けた**所管省庁**は、強化法の規定に基づき、特定重要電子計算機の被害防止のために必要があると認めたときは、**製品開発者に対し、被害防止のために必要な措置を講ずるよう要請することができる**。 ※主に経済産業省
- 内閣府は、**他の行政機関や特定の基幹インフラ事業者など、対応にあたって必要な者に対する情報提供を行う際**には、強化法上の守秘義務の下でこれを行う等、**適切な管理の下で情報提供を行う**。
- 内閣府は、**対応が終了した際には、この旨を受付機関IPAに通知する**。この旨の通知を受けた**受付機関IPAは、この旨を速やかに発見者に通知する**。また、 受付機関IPAは、発見者から問合せを受けたときは、内閣府と協議した上で、適切な情報を提供する。

③ 調整機関JPCERT/CCは、発見者から脆弱性情報を入手した場合、IPAに対してこれを速やかに通知する。また、受付機関IPAが、重要電子計算機の被害防止の観点から内閣府への通知が必要と認められるものを峻別するにあたって必要な協力を行う。

④ NICTが未知の脆弱性を発見した場合、NICTは受付機関IPAに届け出るとともに、調整機関JPCERT/CCに連絡し製品開発者の負担軽減のため個別ではなくNICTとJPCERT/CCが連携を取りつつ製品開発者への技術的助言を行う。また、製品開発者による対応方法の作成後には、NOTICEプロジェクトを通じた注意喚起※を行う。 ※当該プロジェクトにおける注意喚起の要件に合致した場合に限る。

※IPAがIoT製品ラベリング制度（JC-STAR）の申請審査又は運用課程において脆弱性を発見した場合、製品開発者との調整を行うこととなるが、その際、必要性に鑑みて、早期警戒パートナーシップ及び本運用との連携を図るべく、調整中。

【参考】強化法に基づく事務の委託

サイバー対処能力強化法に基づく基本方針（案）より引用

事務	想定される事務の内容	想定される委託先
第37条に規定する事務 報告等情報、選別後通信情報（略）、提供用選別後情報、協議会を通じて得た情報その他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、当該**情報の整理及び分析**を行う ※選別後通信情報を取り扱うものを除く	● 特定重要電子計算機の届出情報や特定侵害事象等の内容の整理・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	**IPA**
	➢ NICTが有する分析能力や観測網等のリソースを活用した上記業務の高度化	**NICT**
第41条に規定する事務 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必要があると認めるときは、重要電子計算機を使用する者、重要電子計算機に対する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その他の者**に対し、**周知等用総合整理分析情報**を**提供**し、又はこれを**公表**その他の適切な方法により**周知**する	➢ インシデント情報に係る注意喚起　等	**IPA** **JPCERT/CC**
第42条第1項に規定する事務 総合整理分析情報その他の情報により電子計算機等における脆弱性（略）を認知したときは、必要に応じ、当該電子計算機等に係る**電子計算機等供給者**（略）に対し当該電子計算機等における**脆弱性に関する周知等用総合整理分析情報その他の情報**（略）を**提供**するとともに、**当該情報又は当該脆弱性への対応方法**について、**公表**その他の適切な方法により**周知**する	➢ 電子計算機等供給者への脆弱性情報の提供・調整 ➢ 脆弱性への対応方法等の周知　等	**IPA** **JPCERT/CC** **NICT**

※上記の事務の委託に限らず、強化法の施行にあたって、内閣府、国の行政機関、IPA、NICT、JPCERT/CC等の関係機関は、重要電子計算機の被害防止に関する事項について、相互に緊密に連絡・協力する

想定スケジュール（案）

2025年度

９／10（水）【済】	第１回　研究会：強化法及び同整備法の概要
12／９（火）【本日】	第２回　研究会：見直しの方向性（案）
１月下旬Ｐ	第３回　研究会：告示見直し（案）
２月Ｐ	告示見直し（案）のパブコメ
３月末目途	新告示の公布

2026年度

４月以降	研究会：ガイドライン改訂（案）の議論
秋頃	強化法の制度施行（官民連携に係る部分）
	見直し後の告示・ガイドラインの施行

【参考】サイバー対処能力強化法及び同整備法の全体像

2025年度 第１回研究会配布資料

- 国家安全保障戦略（令和4年12月16日閣議決定）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との目標を掲げ、①**官民連携の強化**、②**通信情報の利用**、③**攻撃者のサーバ等への侵入・無害化**、④**NISCの発展的改組・サイバー安全保障分野の政策を一元的に総合調整する新たな組織の設置** 等の実現に向け検討を進めるとされた。
- これら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、令和6年6月7日から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を開催し、同年11月29日に提言を取りまとめ。
- この提言を踏まえ、令和7年2月7日に「サイバー対処能力強化法案」及び「同整備法案」を閣議決定。国会での審議・修正を経て、同年5月16日に成立、同月23日に公布。

概　要

P7 総　則

- 目的規定、基本方針等（第１章）

P8 官民連携（強化法）

- 基幹インフラ事業者による
  - 導入した一定の電子計算機の届出
  - インシデント報告

（第２章）

- 情報共有・対策のための協議会の設置（第９章）
- 脆弱性対応の強化（第42条）

（その他、雑則（第11章）、罰則（第12章））

P11 通信情報の利用（強化法）

- 基幹インフラ事業者等との協定（同意）に基づく通信情報の取得（第３章）
- （同意によらない）通信情報の取得（第４章、第６章）
- 自動的な方法による機械的情報の選別の実施（第22条、第35条）
- 関係行政機関の分析への協力（第27条）
- 取得した通信情報の取扱制限（第５章）
- 独立機関による事前審査・継続的検査 等（第10章）

P16 → 分析情報・脆弱性情報の提供等（第８章）

P18 アクセス・無害化措置（整備法）

- 重大な危害を防止するための警察による無害化措置
- 独立機関の事前承認・警察庁長官等の指揮 等（警察官職務執行法改正）
- 内閣総理大臣の命令による自衛隊の通信防護措置（権限は上記を準用）
- 自衛隊・日本に所在する米軍が使用するコンピュータ等の警護（権限は上記を準用） 等（自衛隊法改正）

P21 組織・体制整備等（整備法）

- サイバーセキュリティ戦略本部の改組、機能強化（サイバーセキュリティ基本法改正）
- 内閣サイバー官の新設（内閣法改正） 等

施行期日

P24 公布の日（令和7年5月23日）から起算して1年6月を超えない範囲内において政令で定める日　等

2025年度 第１回研究会配布資料

【参考】強化法:官民連携の強化

基幹インフラ事業者が**サイバー攻撃を受けた場合等の政府への情報共有**や、**政府から民間事業者等への情報共有、対処支援等の取組を強化**

基幹インフラ事業者によるインシデント報告等

（強化法第２章関係）

- 基幹インフラ事業者は、特定重要電子計算機を導入したときは、その製品名等を事業所管大臣に届出（当該事業所管大臣は当該届出に係る事項を内閣総理大臣に通知）
- 基幹インフラ事業者は、特定重要電子計算機のインシデント情報やその原因となり得る事象を認知したときは、事業所管大臣及び内閣総理大臣に報告

情報共有・対策のための協議会の設置

（強化法第９章関係）

- 内閣総理大臣は、サイバー攻撃による被害の防止のため、関係行政機関の長により構成される「情報共有及び対策に関する協議会」を設置
- 協議会には、基幹インフラ事業者、電子計算機等のベンダー等をその同意を得て構成員として加える
- 構成員に対しては、守秘義務を伴う被害防止に関する情報を共有するとともに、必要な情報共有を求めることが可能

脆弱性対応の強化

（強化法第８章第42条, サイバーセキュリティ基本法第７条関係）

- 内閣総理大臣・事業所管大臣（※）が重要電子計算機に用いられる電子計算機等の脆弱性を認知
  → 電子計算機等のベンダー等に対して情報提供、対応方法の公表・周知
- 基幹インフラ事業者が使用する特定重要電子計算機に用いられる電子計算機等に関連する脆弱性の場合
  → 事業所管大臣（※）は、その電子計算機等のベンダー等に対し、必要な措置を講ずるよう要請　　等

（※）電子計算機やそれに組み込まれるプログラムの供給を行う事業を所管する大臣

【参考】強化法：官民連携の強化（詳細）

2025年度 第１回研究会配布資料

基幹インフラ事業者によるインシデント報告等（強化法第２章）

○　基幹インフラ事業者は、特定重要電子計算機（☆）を導入したときは、その製品名等を事業所管大臣に届け出なければならないこととするとともに、当該事業所管大臣は当該届出に係る事項を内閣総理大臣に通知することとする（資産届出）。（第４条）

○　基幹インフラ事業者は、不正アクセス行為等により特定重要電子計算機（☆）のサイバーセキュリティが害されたこと又はその原因となり得る一定の事象を認知したときは、その旨及び一定の事項を事業所管大臣及び内閣総理大臣に報告しなければならないこととする。（第５条）

☆　そのサイバーセキュリティが害された場合に、特定重要設備の機能が停止し、又は低下するおそれがある一定の電子計算機。

情報共有・対策のための協議会の設置（強化法第９章）

○　内閣総理大臣は、サイバー攻撃による被害の防止のため、重要電子計算機を使用する者等（あらかじめ同意を得た者に限る。）を構成員とする協議会を設置し、構成員に対し、守秘義務を伴う被害防止に資する情報を共有するとともに、必要な資料提出等を求めることができることとする（サイバーセキュリティ協議会を廃止し、強化・新設）。（第45条）

電子計算機の使用者に対する情報共有（強化法第８章第41条）

○　内閣総理大臣は、サイバー攻撃による被害の防止に必要な情報を公表・周知する。（第41条）

【参考】強化法:分析情報・脆弱性情報の提供等

2025年度 第１回研究会配布資料

基幹インフラ事業者から届出された**電子計算機の情報**
（第２章）

〃 報告された**インシデント情報**
（第２章）

選別した後の**通信情報**※
（第５章、第７章）

協議会を通じて得た情報
（第９章）

その他の情報
（外国政府から提供された情報等）

情報の整理・分析
（第37条）

通信情報や秘密を含み得る

総合整理分析情報
国の行政機関 等
（第38条）

通信情報は含まないが秘密は含み得る

提供用総合整理分析情報
協議会の構成員 等（※）
（第45条）

通信情報や秘密は含まず

周知等用総合整理分析情報
基幹インフラ事業者
電子計算機等の供給者
公表・周知 等
（第40条～第42条）

※　外国政府等に対しても、必要に応じ提供可能。
（第28条、第39条）

【参考】強化法：分析情報・脆弱性情報の提供等（詳細）

2025年度 第１回研究会配布資料

分析情報の提供等（強化法第８章）

○　内閣総理大臣は、基幹インフラ事業者によるインシデント報告等に係る情報を含め、取得した情報を整理・分析し、その情報を、サイバーセキュリティ確保のため、アクセス・無害化を行う行政機関その他関係行政機関に提供するものとする。また、内閣総理大臣は、必要がある場合には、外国の政府等に対し、分析情報を提供することができることとするほか、事業所管大臣も、必要がある場合にはその情報を基幹インフラの事業者に提供することができることとする。（第37条～第40条）

（再掲）　内閣総理大臣は、サイバー攻撃による被害の防止に必要な情報を公表・周知する。（第41条）

（再掲）　内閣総理大臣及び電子計算機等供給事業所管大臣（☆１）は、重要電子計算機として用いられる電子計算機やプログラムにおける脆弱性を認知したときには、当該電子計算機等の供給者（☆２）に対し情報を提供することができることとする。（第42条第１項）

（再掲）　内閣総理大臣は、サイバー攻撃による被害の防止のため、重要電子計算機を使用する者等（あらかじめ同意を得た者に限る。）を構成員とする協議会を設置し、構成員に対し、守秘義務を伴う被害防止に資する情報を共有するとともに、必要な資料提出等を求めることができることとする（サイバーセキュリティ協議会を廃止し、強化・新設）。（第45条）

罰則の整備（強化法第12章）

・行政職員及び協議会構成員等による秘密の不正な利用・漏えいの行為
　⇨　２年以下の拘禁刑又は100万円以下の罰金（第82条）

【参考】強化法の規定：情報の整理及び分析、周知等

■ サイバー対処能力強化法

第八章　総合整理分析情報等の提供

（内閣総理大臣による情報の整理及び分析）

第三十七条 内閣総理大臣は、報告等情報、選別後通信情報（略）、提供用選別後情報、協議会を通じて得た情報その他の情報が**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、当該**情報の整理及び分析を行う**ものとする。（略）

（電子計算機を使用する者に対する周知等）

第四十一条　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必要があると認めるときは、**重要電子計算機を使用する者、重要電子計算機に対する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その他の者**に対し、**周知等用総合整理分析情報を提供し、又はこれを公表その他の適切な方法により周知する**ことができる。

（電子計算機等供給者に対する情報提供等）

第四十二条　内閣総理大臣又は**重要電子計算機として用いられる電子計算機若しくは当該電子計算機に組み込まれるプログラム**（以下この条において「電子計算機等」という。）の供給（略）を行う事業を所管する大臣（略）は、総合整理分析情報その他の情報により電子計算機等における脆弱性（略）を認知したときは、**必要に応じ**、当該電子計算機等に係る**電子計算機等供給者（略）に対し当該電子計算機等における脆弱性に関する周知等用総合整理分析情報その他の情報（略）を提供する**とともに、**当該情報又は当該脆弱性への対応方法について、公表その他の適切な方法により周知する**ことができる。

2　電子計算機等供給事業所管大臣は、総合整理分析情報その他の情報により**特定重要電子計算機として用いられる電子計算機又は当該電子計算機に組み込まれるプログラム（略）における脆弱性を認知した場合**であって、当該脆弱性に起因する**特定重要電子計算機**に対する特定不正行為による被害の防止のために**必要があると認めたとき**は、当該特定電子計算機等に係る**電子計算機等供給者に対し、当該被害を防止するために必要な措置を講ずるよう要請する**ことができる。

3～6　（略）

【参考】強化法の規定：協力の要請等、事務の委託

■ サイバー対処能力強化法

（協力の要請等）
第七十一条内閣総理大臣は、この法律の規定を施行するために必要があると認めるときは、行政機関の長その他の関係者（略）に対し、資料又は情報の提供、説明、意見の表明その他必要な協力を求めることができる。

2 前項に定めるもののほか、**内閣総理大臣、国の行政機関の長、独立行政法人情報処理推進機構（略）の長、国立研究開発法人情報通信研究機構の長その他の関係者は、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、相互に緊密に連絡し、及び協力しなければならない**。

（事務の委託）
第七十二条　内閣総理大臣は、**第三十七条に規定する事務**（選別後通信情報を取り扱うものを除く。）又は**第四十一条に規定する事務**の一部を、**情報処理推進機構**その他当該事務について十分な技術的能力及び門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして**政令で定める法人**に**委託することができる**。

2　内閣総理大臣又は電子計算機等供給事業所管大臣は、**第四十二条第一項に規定する事務**の一部を、**情報処理推進機構**その他当該事務について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして**政令で定める法人**に**委託することができる**。

3　内閣総理大臣又は電子計算機等供給事業所管大臣は、前二項の規定による委託を受けた者（以下この条及び次条において「受託者」という。）からの求めに応じて、当該委託に係る事務を実施するために必要な提供用総合整理分析情報その他の情報及び資料（選別後通信情報を含むものを除く。）の提供を行うことができる。

4　受託者の役員若しくは職員又はこれらの職にあった者は、正当な理由がなく、当該委託に係る事務に関して知り得た秘密を漏らし、又は盗用してはならない。

5　受託者の役員又は職員であって当該委託に係る事務に従事するものは、刑法その他の罰則の適用については、法令により公務に従事する職員とみなす。

【参考】サイバー空間の安全確保　― NOTICEプロジェクト

資料2-3

取組　電気通信事業者（ISP）との連携による悪意あるプログラムに感染したIoT機器等の対処

- NICTがインターネットを観測・調査し、**悪意あるプログラム（マルウェア）に感染したIoT機器や、今後感染する危険性が高い脆弱なIoT機器を発見**
- 電気通信事業者（ISP）と連携し、当該機器等の**管理者に注意喚起※・意識啓発**を行い対応を促すことで、**IoTボットネットによるサイバー攻撃（DDoS攻撃）の発生と被害を軽減**

※IoT機器の管理者への注意喚起は本プロジェクトにおける注意喚起の要件と合致した場合に限る