情報セキュリティ早期警戒パートナーシップ ガイドライン改訂案について

2026年9月14日
独立行政法人情報処理推進機構
セキュリティセンター

1. 本資料の概要

- 情報セキュリティ早期警戒パートナーシップは、2004年の制度開始以降、「告示」という政府・官のルールと、脆弱性研究会という産学・民のルールである「ガイドライン」という２階層構造で運用がなされてきた。
- この度、内閣官房国家サイバー統括室及び経済産業省における検討等の結果として、2025年度脆弱性研究会の時点で想定していた「告示の新規制定・改正を行ったうえでガイドラインを見直す」という方針ではなく、「『内閣総理大臣からの要請』に対応するものとしてガイドラインを見直す」という形での方針となった。
- 以上を踏まえ、パートナーシップ制度の基本的性格を損なわないよう、どこまでの範囲を、どのようにガイドラインに記載するか整理を行った。

本資料の構成

1. 本資料の概要
2. 2025年度時点での検討の方向性について
3. パートナーシップの基本的な在り方について
4. サイバー対処能力強化法施行に伴う対応の必要性について
5. ガイドライン改訂案の基本方針について
6. ガイドライン改訂案の詳細について
    a. ガイドライン本体への追記事項について
    b. 付録7での記載事項について
    c. その他の改訂事項
    d. 施行・適用について

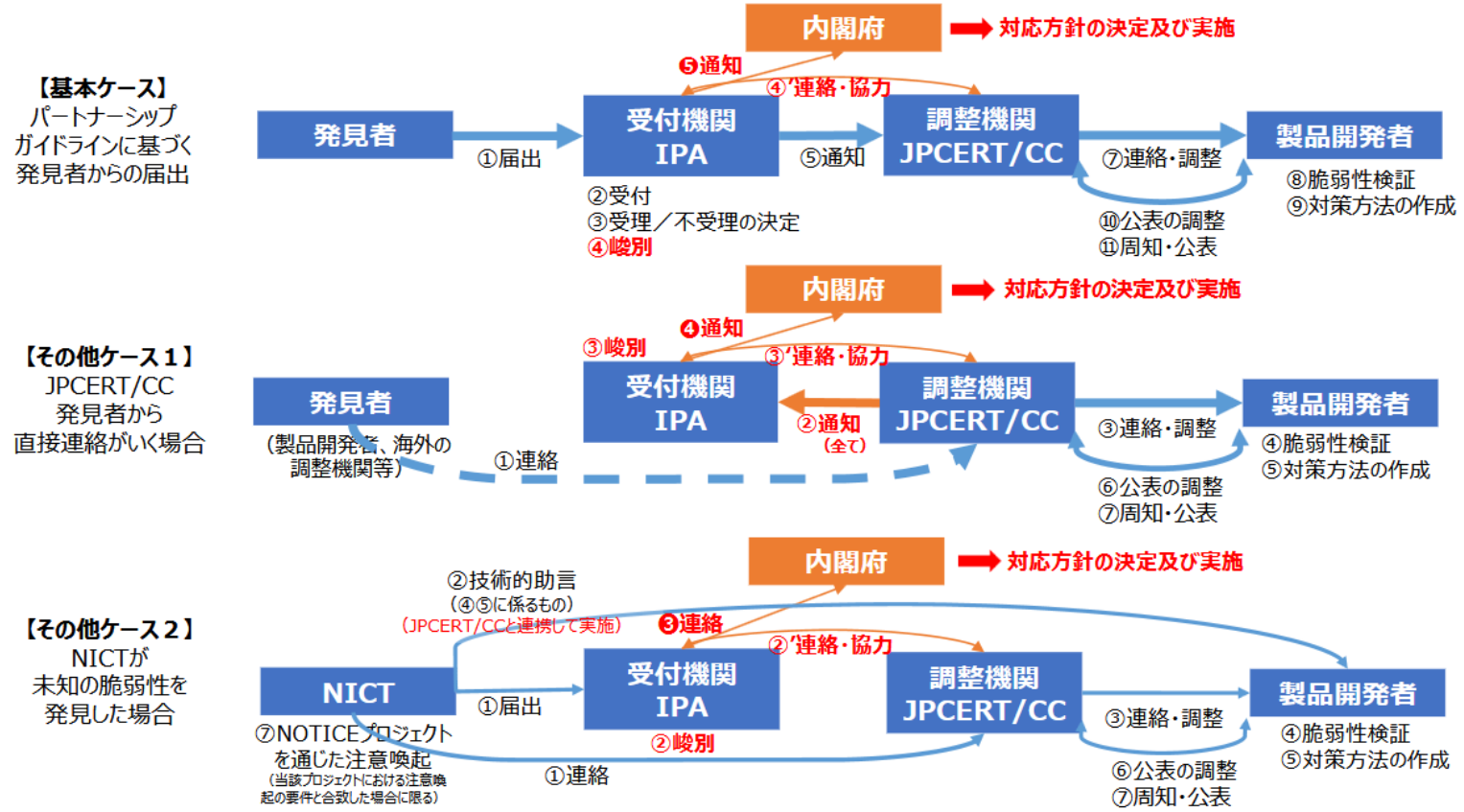
参考 関係条文

2-a. 2025年度時点での検討の方向性について

強化法施行後の脆弱性対応フロー（案）

資料2-3　7

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。**



※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。

引用：2025年度脆弱性研究会 第2回会合 資料2-3（抜粋）

2-b. 2025年度時点での検討の方向性について

告示・ガイドライン見直しの方向性（案）

資料2-3　9

- 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。

引用：2025年度脆弱性研究会 第2回会合 資料2-3（抜粋）

3-a. パートナーシップの基本的な在り方について

■ 情報セキュリティ早期警戒パートナーシップは、 2004年の制度開始以降、「告示」という政府・官のルールと、脆弱性研究会という産学・民のルールである「ガイドライン」という２階層構造で運用がなされてきた。
■ 2003年度研究会報告書においても、**公的ルールと民間ルールの双方で制度的担保**とすることとされている。

4.2.制度的担保の具体策
まず脆弱性関連情報の発見者に受付機関の存在を周知するとともに、関係者の適切な対応を促す目的を考慮すれば、**政府が公的なルールを制定**し、その目的や枠組みを広報するとともに、関連業界団体に対しても積極的に協力を呼びかけていくことが適当である。
また、**公的なルールと連動する形で**、受付機関や調整機関等の役割・機能を規定し、処理の流れを明確化する意図で、**民間側のガイドラインを別途策定することが適当**である。
したがって、公的ルールは、第三者が脆弱性関連情報を発見し、受付機関に届け出た際の、関係者間の必要最低限の推奨事項を明示するものとなる。また、民間ガイドラインは、第三者が脆弱性関連情報を発見し、IPA に届け出た際の、関係者間のなすべき事項を自ら宣言するものとなる。
それぞれの位置付けを、整理すると表4-1に示すところとなる。

■ 表4-1:制度的担保の位置付け

大項目	政府が定める公的ルール	民間ガイドライン
趣旨	第三者が脆弱性関連情報を発見し、受付機関に届け出た際の、関係者間の必要最低限の推奨事項を明示	第三者が脆弱性関連情報を発見し、IPA に届け出た際の、関係者間のなすべき事項を自ら宣言するもの
内容上の特徴等	● 受付機関の指定 ● 関係者に望まれる行動基準	● 発見者、製品開発者、ウェブサイト運営者それぞれに係わる法的関連事項の明示 ● 製品開発者の脆弱性関連情報公表に関する記載事項 ● ウェブサイト運営者の個人情報漏洩時の事実関係公表に関する記載事項

引用：2003年度脆弱性研究会報告書（33-34頁）：下線・太字は本資料用に付加

3-b. 現行のガイドラインの構成

■ 現行の情報セキュリティ早期警戒パートナーシップガイドライン（2024年6月版）は以下のような構成となっている。

情報セキュリティ早期警戒パートナーシップガイドラインの目次

4-a. サイバー対処能力強化法施行に伴う対応の必要性について

■ サイバー対処能力強化法に基づく基本方針においても、脆弱性関連情報の取扱いについて、必要な見直しを実施することとされた。

(6) 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
[中略]
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。

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（令和７年12月23日閣議決定）
下線・太字は本資料用に付加

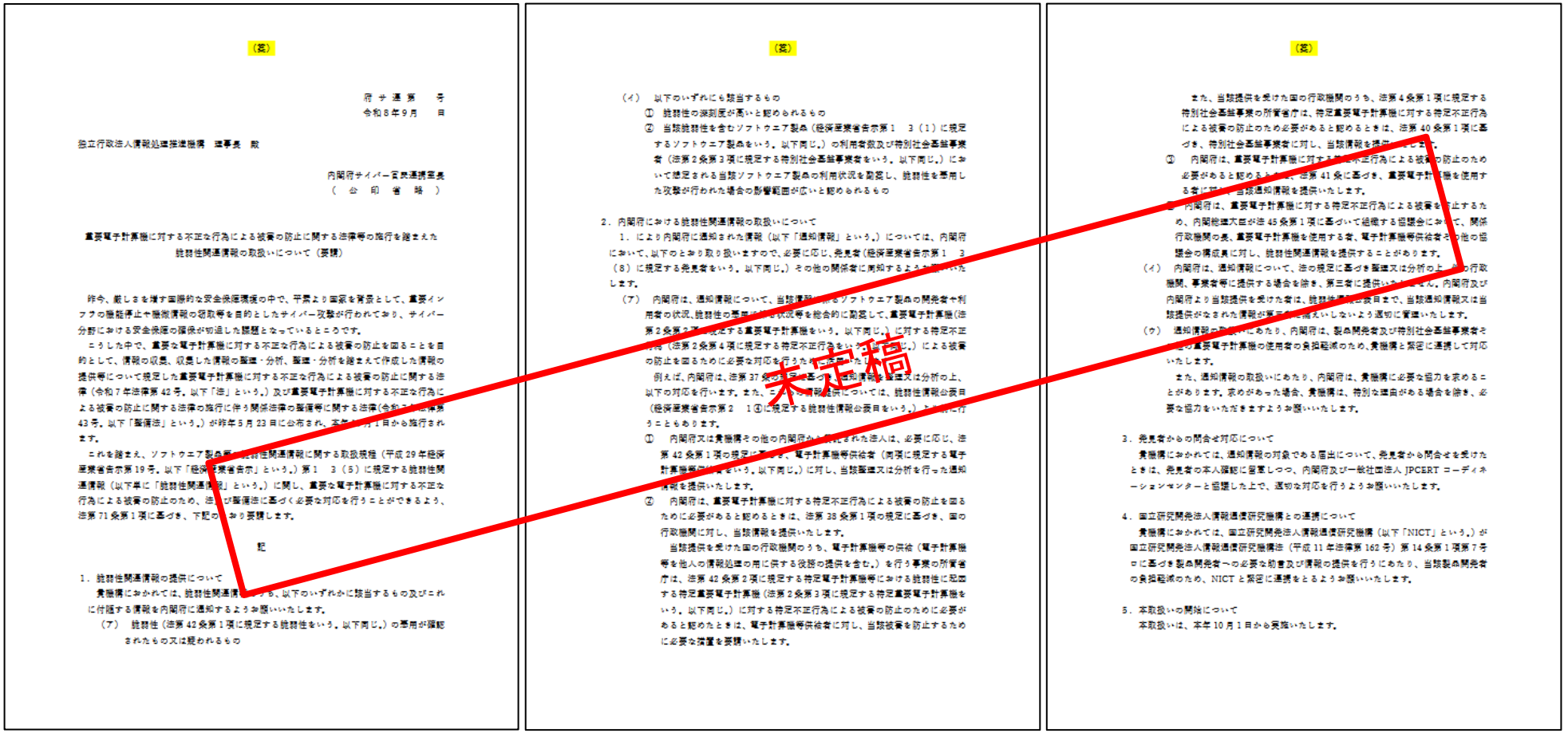
■ 2025年度脆弱性研究会での検討も踏まえ、内閣官房国家サイバー統括室及び経済産業省において告示新規制定・改定について検討・調整を行っていたが、告示での対応ではなく、**サイバー対処能力強化法に基づく内閣総理大臣の要請をIPA、JPCERT/CC宛に実施**し、また、**総務省からNICT宛に同様の通知を実施する**ことを前提に、**その要請等を踏まえたガイドライン改訂を行う**方針となった（要請（案）は次スライドに記載）。

（協力の要請等）
第71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**（委員会を除く。次項において同じ。）**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**（次条第一項及び第二項において「情報処理推進機構」という。）**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**。

引用：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）
下線・太字は本資料用に付加

4-b. サイバー対処能力強化法施行に伴う対応の必要性について

- 内閣総理大臣（文書名義上は内閣府）からの要請（案）として、IPAとJPCERT/CC宛に文書の発出が検討されている。また、総務省からNICT宛に通知の発出が検討されている。
- IPA宛としては以下のような案が検討されている。



（案）

府サ連第　号
令和８年９月　日

独立行政法人情報処理推進機構　理事長　殿

内閣府サイバー官民連携室長
（　公　印　省　略　）

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等の施行を踏まえた
脆弱性関連情報の取扱いについて（要請）

昨今、厳しさを増す国際的な安全保障環境の中で、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ところです。

こうした中で、重要な電子計算機に対する不正な行為による被害の防止を図ることを目的として、情報の収集、収集した情報の整理・分析、整理・分析を踏まえて作成した情報の提供等について規定した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「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。以下「整備法」という。）が昨年５月23日に公布され、本年９月１日から施行されます。

これを踏まえ、ソフトウエア製品の脆弱性関連情報に関する取扱規程（平成29年経済産業省告示第19号。以下「経済産業省告示」という。）第１　３（５）に規定する脆弱性関連情報（以下単に「脆弱性関連情報」という。）に関し、重要な電子計算機に対する不正な行為による被害の防止のため、法及び整備法に基づく必要な対応を行うことができるよう、法第71条第１項に基づき、下記のとおり要請します。

記

１．脆弱性関連情報の提供について
貴機構におかれては、脆弱性関連情報のうち、以下のいずれかに該当するもの及びこれに付随する情報を内閣府に通知するようお願いいたします。
（ア）　脆弱性（法第42条第１項に規定する脆弱性をいう。以下同じ。）の悪用が確認されたもの又は疑われるもの

（案）

（イ）　以下のいずれにも該当するもの
①　脆弱性の深刻度が高いと認められるもの
②　当該脆弱性を含むソフトウエア製品（経済産業省告示第１　３（１）に規定するソフトウエア製品をいう。以下同じ。）の利用者数及び特別社会基盤事業者（法第２条第３項に規定する特別社会基盤事業者をいう。以下同じ。）において想定される当該ソフトウエア製品の利用状況を勘案し、脆弱性を悪用した攻撃が行われた場合の影響範囲が広いと認められるもの

２．内閣府における脆弱性関連情報の取扱いについて
１．により内閣府に通知された情報（以下「通知情報」という。）については、内閣府において、以下のとおり取り扱いますので、必要に応じ、発見者（経済産業省告示第１　３（８）に規定する発見者をいう。以下同じ。）その他の関係者に周知するようお願いいたします。
（ア）　内閣府は、通知情報について、当該脆弱性に係るソフトウエア製品の開発者や利用者の状況、脆弱性の悪用の有無や状況等を総合的に勘案して、重要電子計算機（法第２条第２項に規定する重要電子計算機をいう。以下同じ。）に対する特定不正行為（法第２条第４項に規定する特定不正行為をいう。以下同じ。）による被害の防止を図るために必要な対応を行うため、[illegible]
例えば、内閣府は、法第37条の規定に基づき通知情報の整理又は分析の上、以下の対応を行います。また、二の情報提供については、脆弱性情報公表日（経済産業省告示第２　１④に規定する脆弱性情報公表日をいう。）より前に行うこともあります。
①　内閣府又は貴機構その他の内閣府から委託された法人は、必要に応じ、法第42条第１項の規定に基づき、電子計算機等供給者（同項に規定する電子計算機等供給者をいう。以下同じ。）に対し、当該整理又は分析を行った通知情報を提供いたします。
②　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を図るために必要があると認めるときは、法第38条第１項の規定に基づき、国の行政機関に対し、当該情報を提供いたします。
当該提供を受けた国の行政機関のうち、電子計算機等の供給（電子計算機等を他人の情報処理の用に供する役務の提供を含む。）を行う事業の所管省庁は、法第42条第２項に規定する特定電子計算機等における脆弱性に起因する特定重要電子計算機（法第２条第３項に規定する特定重要電子計算機をいう。以下同じ。）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、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要請いたします。

（案）

また、当該提供を受けた国の行政機関のうち、法第４条第１項に規定する特別社会基盤事業の所管省庁は、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必要があると認めるときは、法第40条第１項に基づき、特別社会基盤事業者に対し、当該情報を提供いたします。
③　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のため必要があると認めるときは、法第41条に基づき、重要電子計算機を使用する者に対し、当該通知情報を提供いたします。
④　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を防止するため、内閣総理大臣が法45条第１項に基づいて組織する協議会において、関係行政機関の長、重要電子計算機を使用する者、電子計算機等供給者その他の協議会の構成員に対し、脆弱性関連情報を提供することがあります。
（イ）　内閣府は、通知情報について、法の規定に基づき整理又は分析の上、他の行政機関、事業者等に提供する場合を除き、第三者に提供いたしません。内閣府及び内閣府より当該提供を受けた者は、脆弱性情報公表日まで、当該通知情報又は当該提供がなされた情報が第三者に漏えいしないよう適切に管理いたします。
（ウ）　通知情報の取扱いにあたり、内閣府は、製品開発者及び特別社会基盤事業者その他の重要電子計算機の使用者の負担軽減のため、貴機構と緊密に連携して対応いたします。
また、通知情報の取扱いにあたり、内閣府は、貴機構に必要な協力を求めることがあります。求めがあった場合、貴機構は、特別な理由がある場合を除き、必要な協力をいただきますようお願いいたします。

３．発見者からの問合せ対応について
貴機構におかれては、通知情報の対象である届出について、発見者から問合せを受けたときは、発見者の本人確認に留意しつつ、内閣府及び一般社団法人 JPCERT コーディネーションセンターと協議した上で、適切な対応を行うようお願いいたします。

４．国立研究開発法人情報通信研究機構との連携について
貴機構におかれては、国立研究開発法人情報通信研究機構（以下「NICT」という。）が国立研究開発法人情報通信研究機構法（平成11年法律第162号）第14条第１項第７号ロに基づき製品開発者への必要な助言及び情報の提供を行うにあたり、当該製品開発者の負担軽減のため、NICT と緊密に連携をとるようお願いいたします。

５．本取扱いの開始について
本取扱いは、本年10月１日から実施いたします。

4-c-1. IPA宛の要請（案）の内容

■ IPA宛としては以下のような案が検討されている。

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等の施行を踏まえた脆弱性関連情報の取扱いについて（要請）

昨今、厳しさを増す国際的な安全保障環境の中で、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ところです。
こうした中で、重要な電子計算機に対する不正な行為による被害の防止を図ることを目的として、情報の収集、収集した情報の整理・分析、整理・分析を踏まえて作成した情報の提供等について規定した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「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。以下「整備法」という。）が昨年5月23日に公布され、本年10月1日から施行されます。
これを踏まえ、ソフトウエア製品等の脆弱性関連情報に関する取扱規程（平成29年経済産業省告示第19号。以下「経済産業省告示」という。）第1　3（5）に規定する脆弱性関連情報（以下単に「脆弱性関連情報」という。）に関し、重要な電子計算機に対する不正な行為による被害の防止のため、法及び整備法に基づく必要な対応を行うことができるよう、法第71条第1項に基づき、下記のとおり要請します。

記

1．脆弱性関連情報の提供について
貴機構におかれては、**脆弱性関連情報のうち、以下のいずれかに該当するもの**及びこれに付随する情報を**内閣府に通知する**ようお願いいたします。
（ア）　**脆弱性（法第42条第1項に規定する脆弱性をいう。以下同じ。）の悪用**が確認されたもの又は疑われるもの
（イ）　以下のいずれにも該当するもの
　① 脆弱性の**深刻度が高い**と認められるもの
　② 当該脆弱性を含むソフトウエア製品（経済産業省告示第1　3（1）に規定するソフトウエア製品をいう。以下同じ。）の**利用者数**及び**特別社会基盤事業者**（法第2条第3項に規定する特別社会基盤事業者をいう。以下同じ。）において想定される当該ソフトウエア製品の**利用状況**を勘案し、**脆弱性を悪用した攻撃が行われた場合の影響範囲**が広いと認められるもの

下線・太字は本資料用に付加

4-c-2. IPA宛の要請（案）の内容

■ IPA宛としては以下のような案が検討されている。

2. 内閣府における脆弱性関連情報の取扱いについて

1. により内閣府に通知された情報（以下「通知情報」という。）については、**内閣府において、以下のとおり取り扱います**ので、必要に応じ、発見者（経済産業省告示第1　3（8）に規定する発見者をいう。以下同じ。）その他の関係者に周知するようお願いいたします。

（ア）　**内閣府は、通知情報について、**当該情報に係るソフトウエア製品の開発者や利用者の状況、脆弱性の悪用に係る状況等を総合的に勘案して、**重要電子計算機**（法第2条第2項に規定する重要電子計算機をいう。以下同じ。）**に対する特定不正行為**（法第2条第4項に規定する特定不正行為をいう。以下同じ。）**による被害の防止を図るために必要な対応を行うために活用**いたします。

例えば、**内閣府は、**法第37条の規定に基づき、通知情報を整理又は分析の上、**以下の対応を行います**。また、これらの情報提供については、脆弱性情報公表日（経済産業省告示第2　1④に規定する脆弱性情報公表日をいう。）より前に行うこともあります。

① 内閣府又は貴機構その他の内閣府から委託された法人は、必要に応じ、法第42条第1項の規定に基づき、**電子計算機等供給者**（同項に規定する電子計算機等供給者をいう。以下同じ。）に対し、当該**整理又は分析を行った通知情報を提供**いたします。

② 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を図るために必要があると認めるときは、法第38条第1項の規定に基づき、**国の行政機関に対し、当該情報を提供**いたします。

当該提供を受けた国の行政機関のうち、**電子計算機等の供給**（電子計算機等を他人の情報処理の用に供する役務の提供を含む。）**を行う事業の所管省庁**は、法第42条第2項に規定する特定電子計算機等における脆弱性に起因する特定重要電子計算機（法第2条第3項に規定する特定重要電子計算機をいう。以下同じ。）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、**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要請**いたします。

また、当該提供を受けた国の行政機関のうち、法第4条第1項に規定する**特別社会基盤事業の所管省庁**は、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必要があると認めるときは、法第40条第1項に基づき、**特別社会基盤事業者に対し、当該情報を提供**いたします。

③ 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のため必要があると認めるときは、法第41条に基づき、**重要電子計算機を使用する者に対し、当該通知情報を提供**いたします。

④ 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を防止するため、内閣総理大臣が法45条第1項に基づいて組織する協議会において、関係行政機関の長、重要電子計算機を使用する者、電子計算機等供給者その他の**協議会の構成員に対し、脆弱性関連情報を提供**することがあります。

下線・太字は本資料用に付加

4-c-3. IPA宛の要請（案）の内容

■ IPA宛としては以下のような案が検討されている。

2. 内閣府における脆弱性関連情報の取扱いについて
1. により内閣府に通知された情報（以下「通知情報」という。）については、**内閣府において、以下のとおり取り扱います**ので、必要に応じ、発見者（経済産業省告示第1　3（8）に規定する発見者をいう。以下同じ。）その他の関係者に周知するようお願いいたします。
[略]
（イ） 内閣府は、通知情報について、法の規定に基づき整理又は分析の上、他の行政機関、事業者等に提供する場合を除き、第三者に提供いたしません。**内閣府及び内閣府より当該提供を受けた者**は、脆弱性情報公表日まで、**当該通知情報又は当該提供がなされた情報が第三者に漏えいしないよう適切に管理**いたします。
（ウ） 通知情報の取扱いにあたり、内閣府は、製品開発者及び特別社会基盤事業者その他の重要電子計算機の使用者の負担軽減のため、貴機構と緊密に連携して対応いたします。
　また、通知情報の取扱いにあたり、内閣府は、貴機構に必要な協力を求めることがあります。求めがあった場合、貴機構は、特別な理由がある場合を除き、必要な協力をいただきますようお願いいたします。

3. 発見者からの問合せ対応について
貴機構におかれては、通知情報の対象である届出について、発見者から問合せを受けたときは、発見者の本人確認に留意しつつ、内閣府及び一般社団法人JPCERTコーディネーションセンターと協議した上で、**適切な対応を行う**ようお願いいたします。

4. 国立研究開発法人情報通信研究機構との連携について
貴機構におかれては、国立研究開発法人情報通信研究機構（以下「NICT」という。）が国立研究開発法人情報通信研究機構法（平成11年法律第162号）第14条第1項第7号ロに基づき製品開発者への必要な助言及び情報の提供を行うにあたり、当該製品開発者の負担軽減のため、NICTと緊密に連携をとるようお願いいたします。

5. 本取扱いの開始について
本取扱いは、本年10月1日から実施いたします。

下線・太字は本資料用に付加

5. ガイドライン改訂案の基本方針について

■ 基本方針の考え方

① ガイドラインは本来、**「告示」に対応**する**任意・協力・推奨を基本的性格とするルール**を記載するものである。

② **内閣府への通知以降の対応**は、**推奨行為というより法令に基づく対応**であり、既存のガイドラインに規定されるIPAやJPCERT/CC、ソフトウエア製品開発者等の推奨行為とは、法的位置づけ上の性格が異なる。

③ 内閣府への通知等の対応自体は**法令及び法令に規定のある要請に根拠をもつ**ため、告示・ガイドラインにおける、**脆弱性情報の第三者開示の禁止の例外である「正当な理由」に該当**する。経済産業省告示の「受付機関は、**正当な理由がない限り**、第三者に脆弱性関連情報を開示しないこと」の「正当な理由」を具体化するものとして、告示の改正を要さずともガイドラインのみの改訂による対応をすることができる。

④ 内閣府の行為をガイドライン（本体）に規定してしまうと、告示なしに**民間ガイドライン側で政府の行動を規律すること**となる。**公的ルールと民間ルールで双方規定するという制度の骨格整理と不整合**が生じる。

⑤ また、ガイドラインは民間ルールであり、「自らなすべき事項を宣言」するものであるため、**ガイドラインに署名しない内閣府の行為を記載すると、ガイドラインは「自らなすべき事項を宣言」するものとは言えなくなる。**

⑥ そのため、内閣府への通知等に関する対応については、ガイドライン本体に関連規定を置くのではなく、**ガイドライン付録において、対応フロー等の説明記載を設ける**こととしたい。

⑦ なお、NICTの対応（NICTとJPCERT/CCの協力対応）については、**内閣府への通知対応だけでなく、通常の届出対応でも生じる**ため、上述の整理の例外として、**ガイドライン本体に必要な条項を新設**するものとしたい。

■ 基本方針を踏まえたガイドラインの既存事項・改訂事項の整理

項目		根拠	ガイドラインでの扱い
既存	従来の届出受付、公表調整等	経産省告示＋ガイドライン	ガイドライン本体で規定（継続）
●新設	IPAから内閣府への通知・JPCERT/CCの協力対応	要請に基づく対応	付録で説明
●新設	内閣府・関係省庁の対応	強化法に基づく対応	付録で説明
●新設	NICTとJPCERT/CC間の協力（内閣府通知届出だけでなく通常の届出対応を含む協力体制）	要請に基づく対応 総務省通知に基づく対応	ガイドライン本体で規定（新規） NICTによるガイドライン署名（連名）

【参考】2003年度脆弱性研究会報告書におけるガイドラインの位置付けの説明（35頁）

4.4.1.脆弱性関連情報取扱に係わる文書の法的位置付け
(2) 民間ガイドラインの位置付け
本ガイドラインは、関係者の連名で発行されることを想定しており、法的強制力は無い。基本的には、政府の公的ルールの存在を前提としており、政府の公的ルールが関係者への推奨事項を前提とした文書であるため、本ガイドラインも同一の前提を有している。内容は、関係者向けに行動の基準を平易に解説したものとなっている。

6. ガイドライン改訂案の詳細について

■ ガイドライン改訂案の改訂概要は以下のとおり。

項目	改訂案の内容
はじめに	• 従来の「告示を踏まえ」という記述は維持 • 要請を踏まえた対応が加わることを説明 • NICTに関する行為についても規定することを説明
発見者の対応	• 発見者がNICTである場合の対応について記載
IPA（受付機関）の対応	• 内閣府通知等について付録に基づく対応をする旨の条項を新設
JPCERT/CC（調整機関）の対応	• 内閣府通知にあたっての協力等について付録に基づく対応をする旨の条項を新設 • 発見者からJPCERT/CCへ直接報告された脆弱性をIPAに通知する規定を追加（IPAを経由して内閣府に通知するため） • JPCERT/CCがNICTと緊密に連携して対応することを説明する規定を追加
【新設】付録7	• 「情報セキュリティ早期警戒パートナーシップと内閣府の対応について」を新設し、内閣府への通知や、その後の内閣府・関係行政機関の対応について説明する記載を追加

6-a-1. ガイドライン本体への追記事項について

■ 「はじめに」において、内閣総理大臣からの要請を踏まえた対応をIPA及びJPCERT/CCで実施すること、及び、実施内容について付録で説明を行うこと、NICTの連携対応について記載があることを追記する。

現行ガイドライン	ガイドライン改訂案
I.　はじめに [略] 本ガイドラインは、上記告示を踏まえ、脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルス等による被害発生を抑制するために、関係者に推奨する行為をとりまとめたものです。さらに、本ガイドラインに基づく取組みがより効果的に社会貢献できるように、影響の大きい届出（脆弱性の深刻度の大きさや影響範囲の広さで判断、詳細は付録４を参照）を優先して取り扱うことや、発見者と製品開発者または、ウェブサイト運営者との調整において自律的な進展が困難な場合の打開を促すことにも取り組みます。 具体的には、独立行政法人情報処理推進機構（以下、「IPA」とする）が受付機関、一般社団法人JPCERTコーディネーションセンター（以下、「JPCERT/CC」とする）が調整機関という役割を担い、発見者、製品開発者、ウェブサイト運営者と協力をしながら脆弱性関連情報に対処するための、その発見から公表に至るプロセスを詳述しています。 関係者の方々は、脆弱性関連情報の取扱いに際し、本ガイドラインを基本としてご対応くださいますようお願い申し上げます。	I.　はじめに [略] 本ガイドラインは、上記告示を踏まえ、脆弱性関連情報の適切な流通により、コンピュータ不正アクセス、コンピュータウイルス等による被害発生を抑制するために、関係者に推奨する行為をとりまとめたものです。さらに、本ガイドラインに基づく取組みがより効果的に社会貢献できるように、影響の大きい届出（脆弱性の深刻度の大きさや影響範囲の広さで判断、詳細は付録４を参照）を優先して取り扱うことや、発見者と製品開発者または、ウェブサイト運営者との調整において自律的な進展が困難な場合の打開を促すことにも取り組みます。 具体的には、独立行政法人情報処理推進機構（以下、「IPA」とする）が受付機関、一般社団法人JPCERTコーディネーションセンター（以下、「JPCERT/CC」とする）が調整機関という役割を担い、発見者、製品開発者、ウェブサイト運営者と協力をしながら脆弱性関連情報に対処するための、その発見から公表に至るプロセスを詳述しています。 また、2026年から、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」とする。）の施行に伴い、内閣府からの要請を受け、IPAおよびJPCERT/CC において内閣府と連携する対応も実施することとなったため、付録においてその概要を説明しています。あわせて、国立研究開発法人情報通信研究機構（以下、「NICT」とする）が製品開発者に必要な助言および情報の提供を行う場合には、内閣府からの要請および総務省からの通知に基づき、NICTおよび調整機関であるJPCERT/CCが当該製品開発者の負担軽減のため緊密に連携することを記載しています。 関係者の方々は、脆弱性関連情報の取扱いに際し、本ガイドラインを基本としてご対応くださいますようお願い申し上げます。

6-a-2. ガイドライン本体への追記事項について

■ 「発見者の対応」において、発見者がNICTの場合におけるJPCERT/CCとの緊密連携対応について明記する。

現行ガイドライン	ガイドライン改訂案
II.　発見者の対応 [略] 3) 脆弱性関連情報の届出 発見者は、発見した脆弱性関連情報をIPAに届け出てください 。 ただし、発見者から直接の届出を受け入れる旨を承諾している製品開発者 の場合、直接届け出ることも可能です。 その際、IPAと製品開発者の両方に届け出る場合には、関係者間の調整が混乱しないように、脆弱性の解消に向けた製品開発者との調整を自ら行うか、IPAに任せるかを届出の際に、明確にしてください。さらに、以降の調整をIPAに任せる場合は、製品開発者へその旨を通知するとともに、その通知を行った旨を届出に明記してください。	II.　発見者の対応 [略] 3) 脆弱性関連情報の届出 発見者は、発見した脆弱性関連情報をIPAに届け出てください 。 ただし、発見者から直接の届出を受け入れる旨を承諾している製品開発者 の場合、直接届け出ることも可能です。 その際、IPAと製品開発者の両方に届け出る場合には、関係者間の調整が混乱しないように、脆弱性の解消に向けた製品開発者との調整を自ら行うか、IPAに任せるかを届出の際に、明確にしてください。さらに、以降の調整をIPAに任せる場合は、製品開発者へその旨を通知するとともに、その通知を行った旨を届出に明記してください。 なお、発見者がNICTである場合であって、国立研究開発法人情報通信研究機構法（平成11年法律第162号）第14条第１項第７号ロに基づき製品開発者に必要な助言および情報の提供を行うときは、NICTはあらかじめJPCERT/CCに連絡するなど、製品開発者の負担軽減のため、JPCERT/CCと緊密に連携して対応します。

6-a-3. ガイドライン本体への追記事項について

■ 「IPA（受付機関）の対応」において、脆弱性の第三者への開示の正当な理由の一種として、内閣府への通知対応が位置づけられることを明示する。

現行ガイドライン	ガイドライン改訂案
IV.　ソフトウエア製品に係る脆弱性関連情報取扱 3. IPA（受付機関）の対応 (1)脆弱性関連情報の届出受付と取扱いについて [略] 5) 脆弱性関連情報の取扱い IPAは、脆弱性関連情報に関して、正当な理由がない限り発見者・JPCERT/CC・当該製品開発者以外の第三者に開示しません。ただし、以下のような正当な理由がある場合、IPAは第三者に情報を開示することがあります。なお、技術的分析を依頼する場合、IPAは秘密保持契約を結びます。 (ア) 脆弱性を有するソフトウエア製品が、他のソフトウエアやウェブサイトで利用されている場合に、それらの製品開発者やウェブサイト運営者に連絡する場合 (イ) 脆弱性が再現する状況を特定できない等の場合に、国立研究開発法人産業技術総合研究所や技術研究組合制御システムセキュリティセンター等の外部機関に脆弱性関連情報に関する技術的分析を依頼する場合 この場合、関係者の許諾を得た上で、JPCERT/CCと連携し、脆弱性の再現に必要な情報を製品開発者に開示することがあります。 また、IPAは、脆弱性関連情報に関して、それに関する脆弱性情報が一般に公表されるまでの間は、発見者・JPCERT/CC・当該製品開発者以外の第三者に漏えいしないように適切に管理します。	IV.　ソフトウエア製品に係る脆弱性関連情報取扱 3. IPA（受付機関）の対応 (1)脆弱性関連情報の届出受付と取扱いについて [略] 5) 脆弱性関連情報の取扱い IPAは、脆弱性関連情報に関して、正当な理由がない限り発見者・JPCERT/CC・当該製品開発者以外の第三者に開示しません。ただし、以下のような正当な理由がある場合、IPAは第三者に情報を開示することがあります。なお、技術的分析を依頼する場合、IPAは秘密保持契約を結びます。 さらに、下記12)および15)に関しては例外とします。 (ア) 脆弱性を有するソフトウエア製品が、他のソフトウエアやウェブサイトで利用されている場合に、それらの製品開発者やウェブサイト運営者に連絡する場合 (イ) 脆弱性が再現する状況を特定できない等の場合に、国立研究開発法人産業技術総合研究所や技術研究組合制御システムセキュリティセンター等の外部機関に脆弱性関連情報に関する技術的分析を依頼する場合 この場合、関係者の許諾を得た上で、JPCERT/CCと連携し、脆弱性の再現に必要な情報を製品開発者に開示することがあります。 また、IPAは、脆弱性関連情報に関して、それに関する脆弱性情報が一般に公表されるまでの間は、発見者・JPCERT/CC・当該製品開発者以外の第三者に漏えいしないように適切に管理します。

6-a-4. ガイドライン本体への追記事項について

■ 「IPA（受付機関）の対応」において、内閣府への通知等を行うこと、及び、付録で説明をしていることについて説明する規定を新設する。

現行ガイドライン	ガイドライン改訂案
IV.　ソフトウエア製品に係る脆弱性関連情報取扱 3. IPA（受付機関）の対応 (1)脆弱性関連情報の届出受付と取扱いについて [略] 15) 統計情報の集計と公表 IPAは、脆弱性に係る実態を周知徹底し危機意識の向上を図り、その結果としての被害の予防のために、受け付けた脆弱性関連情報を集計し、統計情報としてインターネット上等で原則、四半期ごとに公表します。統計情報には、届出件数の時間的推移等が含まれます。	IV.　ソフトウエア製品に係る脆弱性関連情報取扱 3. IPA（受付機関）の対応 (1)脆弱性関連情報の届出受付と取扱いについて [略] 15) 内閣府への通知等に関する対応 IPAは、一定の脆弱性関連情報について、内閣府からの要請に基づき、内閣府への連携等の対応を実施します。対応の概要については、付録７に記載しています。 16) 統計情報の集計と公表 IPAは、脆弱性に係る実態を周知徹底し危機意識の向上を図り、その結果としての被害の予防のために、受け付けた脆弱性関連情報を集計し、統計情報としてインターネット上等で原則、四半期ごとに公表します。統計情報には、届出件数の時間的推移等が含まれます。

6-a-5. ガイドライン本体への追記事項について

■ 「JPCERT/CC（調整機関）の対応」において、NICTと緊密に連携して対応することを説明する記載を追加する。

現行ガイドライン	ガイドライン改訂案
IV.　ソフトウエア製品に係る脆弱性関連情報取扱 4. JPCERT/CC（調整機関）の対応 [略] 2) 製品開発者への連絡 JPCERT/CCは、届け出られた脆弱性関連情報のIPAからの通知を受け、製品開発者リストの活用や脆弱性関連情報を分析することにより、速やかに製品開発者を特定し、必要に応じて製品開発者リストに当該製品開発者を追加した上で、その製品開発者に連絡を行います。その際に、各製品開発者に対して、脆弱性検証を行い、その結果を報告することを求めます。 [略] さらに、製品開発者が申告した連絡先情報や製品に添えられた宛先情報等をもとに電子メールや郵便、電話、FAX等いずれの手段で製品開発者に連絡を試みても一定期間にわたりまったく応答がない場合には、「連絡が取れない」と判断します。その場合、JPCERT/CCは、該当する製品開発者を「連絡不能開発者」と位置づけて公表し、連絡を呼びかけます（連絡不能開発者一覧の公表については、付録５を参照）。それでも連絡が取れない場合には、JPCERT/CCは、対象製品（製品名およびバージョン）を公表し、広く一般に情報提供を呼びかけることがあります（対象製品情報の公表と関係者へのお願いについては、付録５を参照）。	IV.　ソフトウエア製品に係る脆弱性関連情報取扱 4. JPCERT/CC（調整機関）の対応 [略] 2) 製品開発者への連絡 JPCERT/CCは、届け出られた脆弱性関連情報のIPAからの通知を受け、製品開発者リストの活用や脆弱性関連情報を分析することにより、速やかに製品開発者を特定し、必要に応じて製品開発者リストに当該製品開発者を追加した上で、その製品開発者に連絡を行います。その際に、各製品開発者に対して、脆弱性検証を行い、その結果を報告することを求めます。 [略] さらに、製品開発者が申告した連絡先情報や製品に添えられた宛先情報等をもとに電子メールや郵便、電話、FAX等いずれの手段で製品開発者に連絡を試みても一定期間にわたりまったく応答がない場合には、「連絡が取れない」と判断します。その場合、JPCERT/CCは、該当する製品開発者を「連絡不能開発者」と位置づけて公表し、連絡を呼びかけます（連絡不能開発者一覧の公表については、付録５を参照）。それでも連絡が取れない場合には、JPCERT/CCは、対象製品（製品名およびバージョン）を公表し、広く一般に情報提供を呼びかけることがあります（対象製品情報の公表と関係者へのお願いについては、付録５を参照）。 なお、NICTが２．３)の必要な助言又は情報提供を行うにあたり、当該製品開発者の負担軽減のため、JPCERT/CCは、NICTと緊密に連携して対応します。

6-a-6. ガイドライン本体への追記事項について

- 「JPCERT/CC（調整機関）の対応」において、JPCERT/CCに発見者から直接報告された脆弱性について、IPAに通知することの規定を新設する。
- また、内閣府への通知にあたっての協力等を行うこと、及び、付録で説明をしていることについて説明する規定を新設する。

現行ガイドライン	ガイドライン改訂案
IV.　ソフトウエア製品に係る脆弱性関連情報取扱 4. JPCERT/CC（調整機関）の対応 [略] （新設）	IV.　ソフトウエア製品に係る脆弱性関連情報取扱 4. JPCERT/CC（調整機関）の対応 [略] 11) JPCERT/CCに発見者から直接に連絡がなされた脆弱性関連情報に係る対応 JPCERT/CCは、IPAを経由せず、発見者から脆弱性関連情報を受領したときは、当該脆弱性関連情報と発見者に係る情報を速やかにIPAに通知します。 12) 内閣府への通知に伴う協力等に関する対応 JPCERT/CCは、一定の脆弱性関連情報について、内閣府からの要請に基づき、内閣府への協力等の対応を実施します。対応の概要については、付録７に記載しています。

6-b. 付録7での記載事項について

■ 「付録7 情報セキュリティ早期警戒パートナーシップと内閣府の対応について」を追加し、要請等を踏まえたIPA及びJPCERT/CCの対応、サイバー対処能力強化法に基づく内閣府や内閣府からの通知先となる関係機関・組織の対応について、説明する記載を置く。

項目	内容
１．内閣府へ通知する脆弱性関連情報	• IPAから内閣府に通知する脆弱性の範囲について、CVSS等の業界標準基準を参考に決定すること
２．関係者の対応	• IPAから内閣府への通知、JPCERT/CCの協力 • 内閣府での対応、内閣府からIPA・JPCERT/CCへの協力依頼 • 内閣府から製品開発者への情報提供 • 内閣府から行政機関等への情報提供 • 内閣府から利用者への情報提供 • 内閣府から協議会への情報提供
３．関係者の情報管理体制	• 内閣府や提供先組織での脆弱性情報の管理
４．発見者からの問い合わせ対応	• 発見者からの問い合わせに対する対応

ガイドライン改訂案

付録７　情報セキュリティ早期警戒パートナーシップと内閣府の対応について

内閣府では、サイバー対処能力強化法に基づき、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、サイバー安全保障の観点から、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を実施しています。
サイバー対処能力強化法および同法に基づく内閣府からの要請を踏まえ、IPA、JPCERT/CCおよび内閣府は重要な電子計算機に対する不正な行為による被害の防止を図ることを目的として、第三者へ脆弱性関連情報を提供する場合における「正当な理由」に該当するものとして、脆弱性関連情報の内閣府への通知等を実施します。IPA、JPCERT/CCおよび内閣府の対応の概要は以下の通りです。
なお、以下の対応は、IV. ソフトウエア製品に係る脆弱性関連情報取扱に定める通常の届出の対応フローと並行して実施するものです。JPCERT/CCによる製品開発者との調整対応やJVNを通じた一般への情報の公表等は内閣府への通知を行う脆弱性についても原則として実施されます。

6-b-1. 内閣府へ通知する脆弱性関連情報

- 内閣府へ通知される脆弱性の範囲として、悪用可能性のあるものと、深刻度が高く基幹インフラ事業者等への影響が大きいものを対象とする旨の記載を設ける。
- CVSSスコアを参照する記載とするが、CVSSのバージョン（v3.1、v4.0）を明記したり、CVSS のみを基準としてしまうと、CVSSスコア以外の脆弱性評価基準が普及した際の対応に困難が生じる可能性があることから、「業界標準となる深刻度指標を用いて評価」という限定しない記載とすることとしたい。

ガイドライン改訂案

１． 内閣府へ通知する脆弱性関連情報
以下のいずれかに該当するものを内閣府へ通知する脆弱性(*)とします。
(ア) 悪用が確認された、または、悪用が疑われる脆弱性
(イ) 一定の深刻度のある脆弱性であって、悪用された場合に影響範囲が大きいもの
・深刻度については、CVSS スコアなど業界標準となる深刻度指標を用いて評価します。
・影響範囲については、脆弱性の対象となるソフトウエア製品の利用者数や基幹インフラ事業者(**)での利用状況などの要素を勘案します。

(*)付録７における脆弱性は、サイバー対処能力強化法における脆弱性（電子計算機のサイバーセキュリティを害するおそれがある電子計算機又は電子計算機に組み込まれるプログラムに含まれる要因（当該電子計算機の通常予見される使用形態によらないことにより生ずるものを除く。））を指します。
(**)サイバー対処能力強化法第２条第３項に規定する特別社会基盤事業者を指します。

6-b-2. 関係者の対応①

■ IPAから内閣府への通知や、通知以降のサイバー対処能力強化法に基づく内閣府等での対応について説明する記載を設ける。

ガイドライン改訂案

２．関係者の対応
1）内閣府への通知
IPAは、脆弱性関連情報が１.に掲げる各号のいずれかに該当すると判断した場合には、当該脆弱性関連情報およびこれに付随する情報（以下「通知情報」という）を内閣府に速やかに通知します。内閣府への通知を行うにあたり、IPAは、この通知情報の峻別の適切な実施のため、速やかに、JPCERT/CCに必要な連絡を行い、または必要な協力を依頼します。JPCERT/CC は当該連絡を受け、必要となる協力を行います。なお、IPAは、発見者から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であっても、その届け出られた脆弱性関連情報が１． に掲げる各号のいずれかに該当すると判断した場合は、内閣府に速やかに通知します。

2）内閣府での対応
内閣府は、通知情報について、製品開発者や製品利用者の状況、脆弱性の悪用に係る状況等を総合的に勘案して、重要電子計算機(*)に対する特定不正行為(**)による被害の防止を図るために必要な対応を行います。例えば、内閣府は、サイバー対処能力強化法第37条第１項の規定に基づき、通知情報を整理または分析の上、3)～6)のとおり情報提供を行います。なお、これらの情報提供については、IPAおよびJPCERT/CCがⅣ． ３．(1)14)およびⅣ． ４．9)により脆弱性情報等を一般に公表する日より前に行うこともあります。
これらの情報提供にあたり、内閣府は、製品開発者および基幹インフラ事業者その他の重要電子計算機の利用者の負担軽減のため、IPAおよびJPCERTと緊密に連携して対応いたします。
また、この際、内閣府は、IPAまたはJPCERT/CCに必要な協力を求めることがあります。求めがあった場合、IPAおよびJPCERT/CCは、特別な理由がある場合を除き、それぞれ必要な協力を行います。

(*)国や地方公共団体、独立行政法人、地方独立行政法人、政令で定める特殊法人、基幹インフラ事業者、重要情報を保有する事業者が使用する重要な電子計算機。正確な定義はサイバー対処能力強化法や関係する政省令などの規定を参照してください。
(**)マルウェアの供用や不正アクセス等。正確な定義はサイバー対処能力強化法や関係する政省令などの規定を参照してください。

[後略：次スライドに続く]

6-b-2. 関係者の対応②

- 内閣府や行政機関等での対応について説明する記載を設ける。
- サイバー対処能力強化法の事務委託（第72条）として、内閣府の代わりにIPAその他の委託先となる法人（政令上、JPCERT/CCが指定）が対応する可能性があることも記載する。

ガイドライン改訂案

２．関係者の対応
[略]
3）内閣府から製品開発者への情報提供
内閣府またはIPAその他の内閣府から委託された法人は、必要がある場合には、サイバー対処能力強化法第42条第1項の規定に基づき、製品開発者に対し、脆弱性関連情報を提供します。
この場合において、Ⅳ．２．3)の必要な助言又は情報提供を行うときは、NICTは、製品開発者の負担軽減のため、内閣府と緊密に連携して対応します。

4）内閣府から行政機関等への情報提供
内閣府は、必要がある場合には、サイバー対処能力強化法第38条第１項の規定に基づき、関係する国の行政機関に対し、脆弱性関連情報を提供します。電子計算機供給事業を所管する行政機関の場合、当該行政機関は、必要に応じ、サイバー対処能力強化法第42条第2項の規定に基づき、製品開発者に対し、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します。また、基幹インフラ分野を所管する行政機関の場合、当該行政機関は、必要がある場合には、サイバー対処能力強化法第40条第１項の規定に基づき、基幹インフラ事業者に脆弱性関連情報を提供します。

5）内閣府から利用者への情報提供
内閣府またはIPAその他の内閣府から委託された法人は、必要がある場合には、サイバー対処能力強化法第41条に基づき、重要電子計算機の利用者に脆弱性関連情報を提供します。

6）内閣府から協議会構成員への情報提供
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のため、内閣府がサイバー対処能力強化法45条第１項に基づいて組織した協議会において、関係行政機関の長、重要電子計算機の利用者、製品開発者その他の協議会の構成員に脆弱性関連情報を提供することがあります。

6-b-3. 関係者の情報管理体制

■ 内閣府や内閣府からの提供先となる関係機関・組織での脆弱性情報の秘密管理に関する対応について、説明する記載を設ける。

ガイドライン改訂案

３．関係者の情報管理体制
内閣府は、２.に掲げるように、サイバー対処能力強化法の規定に基づき、他の行政機関や事業者等に脆弱性関連情報を提供する場合を除き、第三者に脆弱性関連情報を開示しません。また、内閣府および脆弱性関連情報の提供を受けた他の行政機関や事業者等は、IPAおよびJPCERT/CCが３．(1)14)および４．9)により脆弱性情報等を一般に公表する日まで、脆弱性関連情報が第三者に漏えいしないよう適切に管理します。

6-b-4. 発見者からの問い合わせ対応

■ 発見者から問い合わせを受けた場合に、IPAが、内閣府とJPCERT/CCと協議し、適切な対応を行うことを記載する。

ガイドライン改訂案

４．発見者からの問い合わせ対応
IPAは、通知情報の対象である届出について、発見者から問い合わせを受けたときは、発見者の本人確認に留意しつつ、内閣府およびJPCERT/CCと協議した上で、適切に対応します。なお、付録７の冒頭に記載したとおり、内閣府ではサイバー安全保障の観点から脆弱性関連情報を収集していることから、IPAから内閣府への通知の有無、内閣府における対応状況等については、お答えできない場合があります。

6-c. その他の改訂事項

■ 所要の改訂として表紙や目次等の修正を行うほか、ガイドラインで引用・参照する文書・組織名の名称変更等を反映する。

項目	内容
ガイドライン署名	• NICTを追加（IPA、JPCERT/CC、JEITA、SAJ、JISA、JNSAの6組織連名から、NICTを含めた7組織連名の文書に変更する）
表紙・奥付	• 発行日、版数について修正する
目次・項番修正	• 付録7の新設に伴い、項番の繰り下げと目次の更新を行う
組織名・文書名等の変更の反映	• 内閣サイバーセキュリティセンターから国家サイバー統括室への組織改組による名称変更を反映する • 重要インフラ分野・重要インフラ事業者等を規定する文書が「重要インフラのサイバーセキュリティに係る行動計画」から「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」に変更されることを反映する • 個人情報保護法の改正に伴う条名（条文番号）の変更を反映する
IPAロゴマークの変更の反映	• IPAのロゴマークが変更となったため、裏表紙のパートナーシップの体制図を更新する

6-d. 施行・適用について

- 改訂版ガイドラインの施行・適用については、以下のように対応する。
  - 要請に従った対応が2026年10月1日から求められるため、ガイドラインも追従し、本改訂（コメント募集の結果を踏まえた反映を含む）を反映したガイドラインは、**2026年10月1日から公開し、同日施行**する。
  - ただし、過去に受付した届出までさかのぼって内閣府への通知対象とすることは、発見者等の関係者にとっても（その届出時点においては）予想されなかった対応であることを踏まえ、付録7に従った内閣府への通知対応については、**2026年9月30日までにIPAが受付した届出案件には適用せず、従来通りの対応**を行うものとする。

参考 関係条文①（サイバー対処能力強化法）

第37条　（内閣総理大臣による情報の整理及び分析）
内閣総理大臣は、報告等情報、選別後通信情報（前条の規定により選別後通信情報とみなされるものを含む。以下同じ。）、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。この場合において、選別後通信情報については、特定被害防止目的の達成のために必要があると認める場合に限り、当該整理及び分析を行うことができる。

第38条　（行政機関等に対する情報提供）
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、国の行政機関に対し、前条の規定により整理又は分析した情報（以下「総合整理分析情報」という。）を提供するものとする。
2　前項に規定するもののほか、内閣総理大臣は、総合整理分析情報が第31条第2項に規定する事務に資すると認めるときは、警察庁及び防衛省に対し、これを提供するものとする。
3　前二項の場合において、内閣総理大臣は、総合整理分析情報に選別後通信情報が含まれるときは、特定被害防止目的の達成のために必要があると認める場合（当該選別後通信情報が選別後当事者通信情報である場合にあっては、あらかじめ当該選別後当事者通信情報に係る協定当事者の同意を得た場合に限る。）に限り、前二項の規定による提供をすることができる。
4　第1項の規定により総合整理分析情報の提供を受けた総務大臣は、当該総合整理分析情報により、重要電子計算機に対する国外通信特定不正行為に関係する電気通信が電気通信事業者若しくはその利用者（電気通信事業法第2条第7号に規定する利用者をいう。）の電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信元又は送信先とするものであると疑うに足りる状況がある場合であって、当該国外通信特定不正行為のおそれへの対処を求めるため特に必要があると認めるときは、当該対処に必要な範囲内において、当該電気通信事業者に対して、当該総合整理分析情報の全部又は一部を提供することができる。この場合において、当該電気通信事業者が選別後通信情報の保護に関し必要な措置を講じていると総務大臣が認めるときは、その提供する総合整理分析情報には選別後通信情報を含めることができる。

第40条　（特別社会基盤事業者に対する情報提供）
第38条第1項の規定により総合整理分析情報の提供を受けた特別社会基盤事業所管大臣は、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必要があると認めるときは、特別社会基盤事業者に対し、周知等用総合整理分析情報（提供用総合整理分析情報であって秘密を含まないものをいう。以下同じ。）を提供することができる。
2　前項の規定により周知等用総合整理分析情報の提供を受けた特別社会基盤事業者は、当該周知等用総合整理分析情報を活用して、特定重要電子計算機に対する特定不正行為による被害を防止するために必要な措置を講ずるよう努めなければならない。

参考 関係条文②（サイバー対処能力強化法）

第41条 （電子計算機を使用する者に対する周知等）
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。

第42条 （電子計算機等供給者に対する情報提供等）
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（電子計算機等を他人の情報処理の用に供する役務の提供を含む。以下この条において同じ。）を行う事業を所管する大臣（以下「電子計算機等供給事業所管大臣」という。）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（電子計算機のサイバーセキュリティを害するおそれがある電子計算機又は電子計算機に組み込まれるプログラムに含まれる要因（当該電子計算機の通常予見される使用形態によらないことにより生ずるものを除く。）をいう。以下この条において同じ。）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（電子計算機等の供給を行う者をいう。以下この条及び第45条第2項において同じ。）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（選別後通信情報又は秘密を含むものを除く。）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（以下この項及び次項において「特定電子計算機等」という。）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　内閣総理大臣又は特別社会基盤事業所管大臣は、総合整理分析情報その他の情報により特定電子計算機等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を図るため必要があると認めるときは、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前項の要請を行うよう、電子計算機等供給事業所管大臣に対し意見を述べることができる。この場合において、当該被害を防止するため緊急の必要があると認めるときは、自ら当該電子計算機等供給者に対し、当該意見を述べた旨を通知することができる。
4　内閣総理大臣又は電子計算機等供給事業所管大臣は、前三項の規定の施行に必要な限度において、電子計算機等供給者に対し、その供給を行った電子計算機等に関し報告又は資料の提出を求めることができる。
5　前項の規定により報告又は資料の提出の求めを受けた電子計算機等供給者は、その求めに応じるよう努めなければならない。
6　前各項の規定は、国外に所在する電子計算機等供給者が、国内に所在する者に対し電子計算機等の供給を行った場合についても、適用する。

参考 関係条文③（サイバー対処能力強化法）

第9章　協議会
第45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を防止するため、内閣総理大臣及び関係行政機関の長により構成される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情報共有及び対策に関する協議会（以下この条において「協議会」という。）を組織するものとする。
２　内閣総理大臣は、必要と認めるときは、協議会に、重要電子計算機を使用する者、電子計算機等供給者その他の内閣総理大臣が必要と認める者をその同意を得て構成員として加えることができる。
３　協議会は、第1項の目的を達成するため、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提供用総合整理分析情報その他の情報（選別後通信情報を含むものを除く。第2号及び次項において「被害防止情報」という。）を共有するとともに、次に掲げる事項について協議を行うものとする。
一　当該被害の防止のための対策に関する事項
二　被害防止情報を適正に管理するために必要な措置に関する事項
三　前二号に掲げるもののほか、当該被害の防止のために必要な事項
４　協議会の構成員は、前項の協議の結果に基づき、協議会で知り得た被害防止情報の適正な管理その他の必要な取組を行うものとする。
５　協議会は、第三項の協議を行うため必要があると認めるときは、その構成員に対し、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情報に関する資料の提出、意見の開陳、説明その他の協力を求めることができる。この場合において、当該構成員は、正当な理由がある場合を除き、その求めに応じなければならない。
６　構成員は、前項前段の規定による協議会の求めに応じて資料を提出するときは、当該資料の取扱いに関し意見を付すことができるものとし、意見を付した構成員以外の構成員は、その意見に配慮しなければならない。ただし、重要電子計算機に対する特定不正行為による被害を防止するため特に必要があると認めるときは、この限りでない。
７　協議会の事務に従事する者又は従事していた者は、正当な理由がなく、当該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。
８　前各項に定めるもののほか、協議会の組織及び運営に関し必要な事項は、協議会が定める。

参考 関係条文④（サイバー対処能力強化法）

第71条　（協力の要請等）
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（委員会を除く。次項において同じ。）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（次条第1項及び第2項において「情報処理推進機構」という。）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。

第72条　（事務の委託）
内閣総理大臣は、第37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41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。
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42条第1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 関係条文⑤（サイバー対処能力強化法施行令）

第2条 （情報の整理及び分析等の事務を委託することができる法人）
法第72条第1項の政令で定める法人は、次の各号に掲げる委託を行う事務の区分に応じ、当該各号に定める法人とする。
一　法第37条に規定する事務（同条に規定する選別後通信情報を取り扱うものを除く。） 国立研究開発法人情報通信研究機構
二　法第41条に規定する事務　一般社団法人JPCERTコーディネーションセンター（平成15年3月18日に有限責任中間法人JPCERTコーディネーションセンターという名称で設立された法人をいう。）
2　法第72条第2項の政令で定める法人は、前項各号に定める法人とする。