# 我が国における能動的サイバー防御法制の動向「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及び同整備法」

株式会社KDDI総合研究所
シンクタンク部門

2026年2月9日　第1版
2026年3月10日　第2版
2026年3月12日　第3版

KDDI Research

# 目次(1)







KDDI Research

# 目次(2)







KDDI Research

# エグゼクティブサマリ(1)



## ■ 本報告の目的

- **本報告は、近年深刻化するサイバー攻撃の脅威に対処するために成立した能動的サイバー防御の法制度について、本法の成立背景及び内容を解説するものである。具体的には以下の項目があげられる：**
  - 令和4年(2022年)12月「国家安全保障戦略」で掲げられた課題
  - 有識者会議「サイバー安全保障分野での対応能力の向上に向けた提言」
  - 「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」及び「その整備法」

- **本報告は、特に強化法において本法の理解を必要とする事業者に向けて、今後どのような行動、準備、対策等が本法の下要請されるのか、求められると想定されるのかについて解説するものである。具体的には以下の事業者を想定している：**
  - 基幹インフラ事業者及び重要インフラ事業者
  - 電気通信事業者
  - ベンダー・サプライチェーン



KDDI Research

# エグゼクティブサマリ(2)



## ■ 本報告の目的

- 本報告書で取り扱う法制度の中核をなす「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」(以下、「強化法」とする。)は、国の安全保障や国民生活に重大な影響を及ぼす重要インフラ等をサイバー攻撃から守ることを目的とする。その実現のため、以下の3つの主要な枠組みのもと解説する:

1. **官民連携の強化**: 特定社会基盤事業者(＝基幹インフラ事業者)を対象に、重要電子計算機の導入に関する「届出」や、サイバー攻撃を認知した際の「インシデント報告」を義務付ける。これにより、政府は被害状況を迅速に把握し、官民一体での対処を目指す。
2. **通信情報の取得**及び限定的な利用: 政府(内閣総理大臣)が、事業者との「協定」に基づき、または脅威が深刻な場合には「協定なし」で、サイバー攻撃に関連する通信情報を限定的に取得・分析する。これにより、攻撃の予兆検知や分析能力の向上を図る。なお、取得した情報は通信の秘密を守るために、自動的な機械的フィルタリングにかけられ、本質的な通信内容は原則として分析対象外とされる。
3. **情報共有体制の整備**: 政府、関係行政機関、重要インフラ事業者、ベンダー等への情報共有体制の確立、及び当該事業者等が参加できる「協議会」の設置を通し、分析で得られた脅威情報や対策を共有。これにより、社会全体のサイバー防御能力の向上を促進を目指す。



KDDI Research

# 強化法及び整備法の成立背景
## ―「サイバー安全保障」に係る対策の必要性―

# 強化法及び整備法の成立背景―「サイバー安全保障」に係る対策の必要性―



## ■「国家安全保障戦略」とサイバー安全保障対策

### 1. 令和4年(2022年)(2022年)12月「国家安全保障戦略」の制定

- 日本を取り巻く現状の把握と政府の認識(以下、「国家安全保障戦略」抜粋)
  - 「我が国は戦後最も厳しく複雑な安全保障環境に直面している。」
  - 「有事と平時の境目はますます曖昧になってきている。」
  - 「国家安全保障の対象は、経済、技術等、これまで非軍事的とされてきた分野にまで拡大」
  - 「サイバー空間・海洋・宇宙空間・電磁波領域等におけるリスクが深刻化。」

- 環境の変化と新たなリスクの具体例(以下、「国家安全保障戦略」抜粋)
  - 「サイバー空間、海洋、宇宙空間、電磁波領域等において、自由なアクセスやその活用を妨げるリスクが深刻化している。特に、相対的に露見するリスクが低く、攻撃者側が優位にあるサイバー攻撃の脅威は急速に高まっている。サイバー攻撃による重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取等は、国家を背景とした形でも平素から行われている。」
  - 「サプライチェーンの脆弱性、重要インフラへの脅威の増大、先端技術をめぐる主導権争い等、従来必ずしも安全保障の対象と認識されていなかった課題への対応も、安全保障上の主要な課題」

[参考]:内閣官房「国家安全保障戦略」(2022年 12月)https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf



KDDI Research

# 強化法及び整備法の成立背景―「サイバー安全保障」に係る対策の必要性―



## ■「国家安全保障戦略」とサイバー安全保障対策

### 2. 令和4年(2022年)12月「国家安全保障戦略」で掲げる安全保障上の課題と戦略の方向性

- 対策の大枠(以下、「国家安全保障戦略」抜粋)
  - 「最悪の事態をも見据えた備え」を盤石なものとし」
  - 「外交力・防衛力・経済力・技術力・情報力を含む総合的な国力を最大限活用」
  - 「危機を未然に防ぎ、平和で安定した国際環境を能動的に創出」

- サイバー脅威に対する具体的な戦略の方向性(以下、「国家安全保障戦略」抜粋)
  - 「防衛力の抜本的強化を補完し、それと不可分一体のものとして、研究開発、公共インフラ整備、サイバー安全保障、我が国及び同志国の抑止力の向上等のための国際協力の四つの分野における取組を関係省庁の枠組みの下で推進」
  - 「サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、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。」
  - 「最新のサイバー脅威に常に対応できるよう、最新のサイバー脅威に常に対応できるようにするため、政府機関のシステムを常時評価し、政府機関等の脅威対策やシステムの脆弱性等を随時是正するための仕組みを構築する。」
  - 「武力攻撃に至らないものの、国、重要インフラ等に対する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、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入」

[参考]:内閣官房「国家安全保障戦略」(2022年 12月)https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf



KDDI Research

# 強化法及び整備法の成立背景―「サイバー安全保障」に係る対策の必要性―



## ■「国家安全保障戦略」は何を見据えていたのか？

- サイバー脅威に対する具体的な戦略の方向性（以下、「国家安全保障戦略」抜粋）

  - 能動的サイバー防御の実施のための体制を整備において、（ア）から（ウ）までを含む必要な措置の実現に向け検討を進める。

（ア）重要インフラ分野を含め、民間事業者等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対処調整、支援等の取組を強化するなどの取組を進める。

（イ）国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める。

（ウ）国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。

  - 以上の手段のために以下の具体的施策を進めるとする：
    - 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を設置
    - 法制度の整備、運用の強化
    - 経済安全保障、安全保障関連の技術力の向上等、サイバー安全保障の強化に資する他の政策との連携を強化
    - 同盟国・同志国等と連携した形での情報収集・分析の強化、攻撃者の特定とその公表、国際的な枠組み・ルールの形成

[参考]：内閣官房「国家安全保障戦略」（2022年　12月）https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf

# 強化法及び整備法の成立背景―「サイバー安全保障」に係る対策の必要性―



■「国家安全保障戦略」から何が見えるのか？

➡日本を取り巻く環境の変化により、様々な分野において安全保障の危機につながる。**守るべき対象が拡大**している。

➡**「平時」から何をすべきか検討する必要性**が強調されている。

サイバー攻撃が戦争に至る前段階から国家や重要インフラを脅かす現実を踏まえ、平時から**官民・通信・国境をまたいだ**脅威を把握し、**未然に検知・介入・無害化できる体制を構築するため**、組織改編と権限付与を含む**能動的サイバー防御を法制度として整備する必要がある**と判断したと評価できる。



KDDI Research

# 強化法及び整備法の成立背景―「サイバー安全保障」に係る対策の必要性―



■「国家安全保障戦略」をベースにした対策の内容に係る議論

- 令和4年(2022年)「国家安全保障戦略」を根拠にした有識者会議の設置及び開催(令和6年(2024年)6月～11月)

  「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」主な内容・中心の議論

  「能動的サイバー防御に関する法制の検討を進めていく」にあたり:

  ① 官民の情報共有の強化、民間に対する支援の強化

  ② 通信情報に関する情報を活用した攻撃者による悪用が疑われているサーバを検知

  ③ 重大なサイバー攻撃を未然に防ぐために政府に対する必要な権限の付与

[参考]:内閣府「『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』(第1回)議事要旨」(2024年 6月)https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai1/gijiyousi.pdf
[参考]:内閣府「『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』(第2回)議事要旨」(2024年 7月) https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai2/gijiyousi.pdf



KDDI Research

# 強化法及び整備法の成立背景―「サイバー安全保障」に係る対策の必要性―



■「国家安全保障戦略」をベースにした対策の内容に係る議論

① 官民の情報共有の強化、民間に対する支援の強化について

- 「企業が情報セキュリティ事故にあった際の対応に関する情報の共有がなかなかされない。」
- 「官民連携による情報共有は、民間事業者の過度な負担を回避するとともに、…官民双方向なものとすべきである。」
- 「国家のレジリエンス強化という観点では、重要インフラの領域、そして価値創造をしている企業の領域を…中小企業を含めたレジリエンスを強化しない限り、日本のレジリエンスの強化にならない。」

➡テーマ別会合では、諸外国（主に米、英、豪）において情報提供を政府の役割として明確化していたことに触れ、政府の持つ情報及び事業者からの情報提供に係る枠組みが既に制度として確立されていることを検討していた。（＝日本におけるサイバーセキュリティ対策を欧米主要国と同等以上にすることを掲げるうえでの比較）

➡安全保障対策のステークホルダーの幅の広さに言及しつつ、その広さに対応できるような官民連携の重要性が指摘されていた。

# 強化法及び整備法の成立背景―「サイバー安全保障」に係る対策の必要性―



## ■「国家安全保障戦略」をベースにした対策の内容に係る議論

### ② 通信情報に関する情報を活用した攻撃者による悪用が疑われているサーバを検知

- 「サイバー安全保障において重要な点というのは、平時と有事が連続的につながっているということだ。この点をいかにこの有識者会議で議論できるかということが重要な課題」
- 「能動的サイバー防御に必要なデータとは何なのか、何が必要なもので何が不要なのか、具体的に明確にしていくべきではないか。」
- 「外内・内外通信をスコープとしてサイバーセキュリティの向上に活かす、としたことは大変重要」
- 「通信情報の利用においては、『対象とする通信対象』『対象とする通信内容』といった前提を明確にした上で、さらなる議論を進めるべきではないかと思う。また、今後電気通信事業者への『具体的な協力依頼内容』『攻撃対象となった場合の支援・補償』『必要となる設備の試算』などの現実的な検討も必要となる。」

**➡通信情報の内容がいかなるものなのか、またその取得において誰との連携が重要となるのかについて議論することの必要性が協調されていた。**

### ③ 重大なサイバー攻撃を未然に防ぐために政府に対する必要な権限の付与

- 「情報の取得・利用、関連する事業者に対する政府の権限行使について、目的達成に必要かつ合理的な実体的な要件、手続的規律を定めること。」
- 「具体的な組織法の議 論をする段階と考えている。組織の規模、体制、置き方、人材の配置、権限、権限行使の手続等の組織法の話を具体的に展開していくことが必要と考える。」

**➡重大な被害がおきる前の未然防止施策を実行するうえで、政府及び民間の企業がどのような権限をもとに行動すべきなのかを明確に示せるような枠組みの構築を検討すべきであるとされていた。**

[参考]：内閣府「『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』（第１回）議事要旨」（2024年 6月）https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai1/gijiyousi.pdf
[参考]：内閣府「『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』（第２回）議事要旨」（2024年 7月）https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai2/gijiyousi.pdf
[参考]：内閣府「『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』（第３回）議事要旨」（2024年 8月）https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai3/gijiyousi.pdf
[参考]：内閣府「『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』（第４回）議事要旨」（2024年 11月）https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai4/gijiyousi.pdf



KDDI Research

# 強化法及び整備法の成立背景―「サイバー安全保障」に係る対策の必要性―



## ■「国家安全保障戦略」をベースにした対策の内容に係る議論

### ● 有識者会議「サイバー安全保障分野での対応能力の向上に向けた提言」（令和6年（2024年）11月29日）

**実現すべき具体的な方向性として以下を上げる：**

- 「重要インフラの機能停止や破壊等を目的とした重大なサイバー攻撃は、国家を背景とした形でも日常的に行われているなど、安全保障上の大きな懸念となっており、官民ともに、 サイバーの世界は常に有事であるとの危機意識を持った対応が求められる。加えて、社会全体でデジタルトランスフォーメーションが進んだ結果、重要インフラ事業者等が自らのサイバーセキュリティを確保しようとすれば、そのサプライチェーン全体のセキュリティを確保することが必要となっている。」

  **➡以上を背景に、「高度な攻撃に対する支援・情報提供」「ソフトウェア等の脆弱性対応」「政府の情報提供・対処を支える制度」を具体的施策の在り方として挙げる。**

- 「今般実現されるべきき通信情報の利用は、 重大なサイバー攻撃による被害を未然に防ぐため、また、被害が生じようとしている場合に即時に対応するため、具体的な攻撃が顕在化する前、すなわち前提となる犯罪事実がない段階から行われる必要がある。したがって、通信情報を取得しようとする時点では、いかなる具体的態様でサイバー攻撃が発生するかを予測することはできず、あらかじめそのサイバー攻撃に関係する通信手段、内容等を特定することは通常は困難であるから、犯罪捜査とは異なる形で通信情報を取得し利用する必要があり、被害の防止と通信の秘密の保護という両方の目的を適切に果たすためには、これまで我が国では存在しない新たな制度による通信情報の利用が必要とされると考えられる。」

  **➡以上を背景に、「通信情報の利用の範囲及び方式」「通信の秘密との関係」「同意がある場合の通信情報の利用」「電気通信事業者の協力」「国民の理解を得るための方策とその他の検討課題等」を踏まえ、通信情報をいかにして利用すべきなのか、そしてその目的と手段を明らかにした施策を検討していく必要性を掲げる。**

[参考]：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「サイバー安全保障分野での対応能力の向上に向けた提言」（2024年 11月）
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf

# 強化法及び整備法の成立背景―「サイバー安全保障」に係る対策の必要性―



- 「現実空間における危険とは質的に異なり、実際にある危険が潜在化し認知しにくいということが挙げられる。また、潜伏の高度化等により、攻撃者の意図次第でいつでもサイバー攻撃が実行可能であるとともに、ネットワーク化の進展により、一旦攻撃が行われれば、被害が瞬時かつ広範に及ぶおそれがある。」
- 「武力攻撃事態に至らない状況下において、重大なサイバー攻撃による被害の未然防止・拡大防止を目的とした、攻撃者サーバ等へのアクセス・無害化を行う権限を政府に付与することは必要不可欠であり、我々が価値創造するための安全なサイバー空間を守る観点から極めて重要な取組と考えられる。」

**➡以上を背景に、法執行を含めた政府の機能を明確化し、サイバー攻撃からの未然の対策が迅速にとれるような法制度の仕組みを構築していくことも一つ重要な論点・課題であることに言及をしている。**

[参考]：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「サイバー安全保障分野での対応能力の向上に向けた提言」(2024年 11月)https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/koujou_teigen/teigen.pdf



KDDI Research

# 強化法及び整備法の概要

# 強化法及び整備法の概要（1）



■ 法律の構成及び施行の日程

- 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（以下、「強化法」とする。）は令和7年5月23日に公布（全八十六条）
- 施行日に関しては各条文毎に異なる

  ＝現時点（2026年2月9日）では：

  - 第一条（目的）、第二条（定義）、第二条の二（通信の秘密の尊重）
  - 第三条（基本方針）、第七十六～七十八条（雑則）、附則抄

  **のみ施行**。

➡具体的な能動的サイバー防御の**実施は令和8年秋頃、もしくは令和9年以降になる**とされる（本法附則抄（施行期日）第一条）

➡アクセス・無害化措置の実施に際するその他法令（以下、「整備法」とする。）の**改正及び施行日は、強化法の施行の日**とされる。

※現時点で強化法の一部は施行されているが、例えば整備法による警察官職務執行法第六条の二は未だ施行されていないことを踏まえると、強化法が全部施行される日に合わせると想定される。

[参考]：内閣府「法律概要説明資料」https://www.cao.go.jp/cybersecurity/pdf/01sanko01.pdf

# 強化法及び整備法の概要（2）



## 法律の構成及び施行の日程

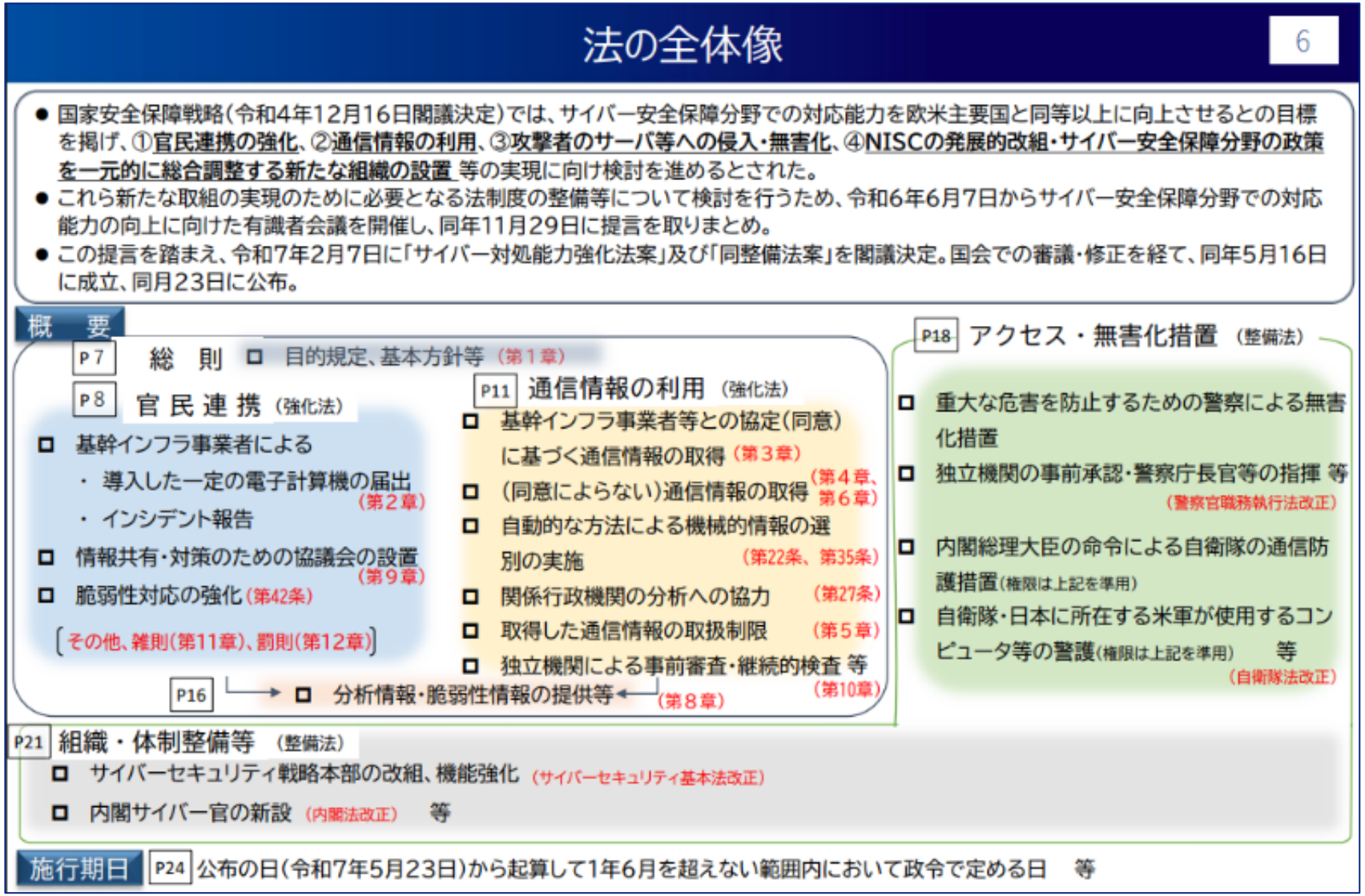
| | |
|---|---|
| サイバー脅威に対する防御・抑止 | ● 「官民連携」部分の下位法令の整備（2026年春頃）<br>● 「官民連携」、「アクセス・無害化措置」部分に係る制度施行（2026年10月1日想定）<br>● 「通信情報の利用」部分に係る下位法令の整備<br>● 「通信情報の利用」部分に係る制度施行（2027年11月まで）<br><br>● 新たな官民協議会の立ち上げ（2026年10月1日想定）<br>● 脅威ハンティングの普及促進・実施等に関する基本方針の策定（2026年夏） |
| 社会全体のサイバーセキュリティ・レジリエンスの向上 | ● 政府機関における機密性の高い情報の保全を前提としたクラウド技術の活用の在り方の検討（2026年度）<br>● 重要インフラ統一基準の新規策定、行動計画の一部見直し（2026年度）<br>● サプライチェーン強化に向けたセキュリティ対策評価制度の開始（2026年度末） |
| 人材・技術に係るエコシステム形成 | ● 人材フレームワークの策定（2025年度）<br>● 2035年までを目処とする政府機関等における耐量子計算機暗号（PQC）への円滑な移行に係る工程表の策定（2026年度） |

[出展]：国家サイバー統括室「サイバーセキュリティ専門家会議　参考資料1-1」（2026年　2月）https://www.cyber.go.jp/pdf/council/cs/cs_expert/04/04reference1-1.pdf

# 強化法及び整備法の概要（3）



## 法律の構造




[出展]：内閣府「法律概要説明資料」https://www.cao.go.jp/cybersecurity/pdf/01sanko01.pdf

# 強化法及び整備法の概要（5）



## ■ 第1条（目的）

この法律は、インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用の進展、国際情勢の複雑化等に伴い、そのサイバーセキュリティが害された場合に国家及び国民の安全を害し、又は国民生活若しくは経済活動に多大な影響を及ぼすおそれのある国等の重要な電子計算機のサイバーセキュリティを確保する重要性が増大していることに鑑み、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の策定、特別社会基盤事業者による特定侵害事象等の報告の制度、重要電子計算機に対する国外通信特定不正行為による被害の防止のための通信情報の取得、当該通信情報の取扱いに関するサイバー通信情報監理委員会による審査及び検査、当該通信情報等を分析した結果の提供等について定めることにより、重要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する。

# 強化法及び整備法の概要 （5）



■ **第2条(定義)**
この法律において「サイバーセキュリティ」とは、サイバーセキュリティ基本法(平成二十六年法律第百四号)第二条に規定するサイバーセキュリティをいう。

● サイバーセキュリティ基本法(平成26年)

第二条(定義)
この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式(以下この条において「電磁的方式」という。)により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置(情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体(以下「電磁的記録媒体」という。)を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。)が講じられ、その状態が適切に維持管理されていることをいう。

「ハンドブック」では:
「保護すべき客体(措置対象)に着目して整理すると、**①情報、②情報システム、③情報通信ネットワークについて必要な措置が講じられ、それが適切に維持管理されていること**、ということができる。」とされる。

[参考]:内閣官房内閣サイバーセキュリティセンター「サイバーセキュリティ関係法令Q&A　ハンドブック Ver 2.0」（2023年　9月）https://security-portal.cyber.go.jp/guidance/pdf/law_handbook/law_handbook_2.pdf

# 強化法の具体的内容①
# ―届出・インシデント報告・罰則―

# 強化法の具体的内容①　―届出・インシデント報告・罰則―



■　第4条（特定重要電子計算機の届出）

特別社会基盤事業者は、特定重要電子計算機を導入したときは、主務省令で定めるところにより、特定重要電子計算機の製品名及び製造者名その他の主務省令で定める事項を特別社会基盤事業（特別社会基盤事業者が行う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第五十条第一項に規定する特定社会基盤事業をいう。）を所管する大臣（以下「特別社会基盤事業所管大臣」という。）に届け出なければならない。

２　特別社会基盤事業所管大臣は、前項の規定による届出を受けたときは、速やかに、当該届出に係る事項を内閣総理大臣に通知するものとする。

３　特別社会基盤事業者は、第一項の規定により届け出た事項に変更があったときは、主務省令で定めるところにより、その旨を特別社会基盤事業所管大臣に届け出なければならない。ただし、その変更が主務省令で定める軽微なものであるときは、この限りでない。

４　第二項の規定は、前項の規定による届出について準用する。

➡　特別社会基盤事業者（強化法第2条3項）が、省令で定める範囲に該当するとされる電子計算機を導入していた・これからする場合、事業者を所管する大臣へ届出を行わなければならない。



KDDI Research

# 強化法の具体的内容①　―届出・インシデント報告・罰則―



■ 第4条の具体的内容

● 重要電子計算機の届け出を出す者：特別社会基盤事業者とは？

→強化法第2条第3項：「特別社会基盤事業者」とは、①特定社会基盤事業者のうち、前項第二号に該当する②重要電子計算機（以下「特定重要電子計算機」という。）を使用するものをいう。

①「特定社会基盤事業者」…強化法第2条第2項第2号では、特定社会基盤事業者（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（令和四年法律第四十三号）第五十条第一項に規定する特定社会基盤事業者をいう。次項において同じ。）とする。

**事業所管省庁によって指定を受けている事業者のこと**

基幹インフラ制度の対象事業（特定社会基盤事業）　（計２５７者）

| | | |
|---|---|---|
| ①電気（４８者） | ②ガス（２５者） | ③石油（１８者） |
| ④水道（２３者） | ⑤鉄道（５者） | ⑥貨物自動車運送（５者） |
| ⑦外航海運（３者） | ⑧港湾（３２者） | ⑨航空（２者） |
| ⑩空港（６者） | ⑪電気通信（１０者） | ⑫放送（６者） |
| ⑬郵便（１者） | ⑭金融（６４者） | ⑮クレジットカード（９者） |

※ 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）
※ 内閣府「特定社会基盤事業者として指定した者（令和７年７月31日時点）」から作成
※ サイバーセキュリティ基本法の「重要社会基盤事業者（重要インフラ）」とは別概念

[出展]：国家サイバー統括室「サイバー対処能力強化法及び同整備法について」（2025年　9月）https://www.cao.go.jp/cybersecurity/pdf/setsumei.pdf
[参考]：内閣府「特定社会基盤事業者として指定した者」（2025年　7月）https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_jigyousya.pdf

# 強化法の具体的内容①　―届出・インシデント報告・罰則―



■ 第4条の具体的内容

● 特別社会基盤事業者が求められる届出提出の対象とは？

→強化法第2条第3項：「**特別社会基盤事業者**」とは、①特定社会基盤事業者のうち、前項第二号に該当する②重要電子計算機（以下「特定重要電子計算機」という。）を使用するものをいう。

② 「重要電子計算機」（**強化法第2条第2項**：法律上の「重要電子計算機」の定義）

この法律において「重要電子計算機」とは、**次の各号のいずれかに該当する電子計算機**（**当該電子計算機に組み込まれたプログラム（電子計算機に対する指令であって、一の結果を得ることができるように組み合わされたものをいう。**第四十二条第一項及び第二項において同じ。）を含む。以下同じ。）をいう。・以上の政令案（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施行令（令和8年政令第　号））

第2条第2項第2号：

**特定社会基盤事業者**（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（令和四年法律第四十三号）第五十条第一項に規定する特定社会基盤事業者をいう。次項において同じ。）**が使用する電子計算機のうち、そのサイバーセキュリティが害された場合において、**同条第一項に規定する**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ものとして政令で定めるもの**（当該特定重要設備の一部を構成するものを含む。）

# 強化法の具体的内容①　―届出・インシデント報告・罰則―



- **政令案の内容（2026年　1月）**

・政令第1条第3項第1号：
特定重要設備である電子計算機又は特定重要設備の一部を構成する電子計算機

・政令第1条第3項第2号：
特定重要設備と電気通信回線で直接又は間接に接続されている電子計算機であって、当該重要設備に対し、当該重要設備の機能に影響を与える電磁的記録（強化法第2条第8項）を送信する機能を有するものとして主務省令で定めるもの

・政令第1条第3項第3号：
第1号に掲げる電子計算機による情報処理のように供される電磁的記録を作成するために用いられる電子計算機のうち、当該電磁的記録が一定の期間毎にに当該1号電子計算機に入力される者であって、道外電磁的記録が問うが一定の期間ごとに当該1号電子計算機に入力されなくなった場合には当該1号電子計算機に係る特定重要設備の機能が停止し、又は低下することとなるものとして主務省令で定めるもの

[参考] 内閣府政策統括官「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施行令案」https://public-comment.e-gov.go.jp/contents/about-public-comment/ (2026 年1月)

# 強化法の具体的内容①　―届出・インシデント報告・罰則―



- 強化法及び政令から考えられる届出の対象となる資産例：

① **特定重要設備そのもの又はその一部を構成する電子計算機**

**特定重要設備**とは、「**特定社会基盤事業の用に供される設備、機器、装置又はプログラム**のうち、特定社会基盤役務を安定的に提供するために重要であり、かつ、我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為の手段として使用されるおそれがあるものとして**主務省令**で定めるもの」

・総務省の省令*（例）：
第一種指定電気通信設備（電気通信事業法第三十三条第二項）のうち交換機能を有する電気通信設備等

＝これは、「経済安全保障推進法」を根拠に基幹インフラ事業者へ当該事業者を所管する省庁へ届出を行っているもの
※主務省令は本報告書「参考資料」に一覧として掲載。
＝経済安全保障推進法の規定に基づく導入の届出を行っている場合には、**当該届出の内容について政府内で連携することで、事業者の負担軽減に繋げられないか検討中**。

② **特定重要設備と直接又は間接につながっていて、その設備の機能に影響を与える電磁的記録を送信する機能を持つもの**　※主務省令で具体化を検討中

③ **特定重要設備で用いる電磁的記録を作る機器のうち、その電磁的記録が一定期間ごとに入らなくなると当該特定重要設備の機能が止まる・下がるもの**　※主務省令で具体化を検討中

[参考]：内閣府「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について」（2025年　8月）https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_gaiyou.pdf
[参考]：総務省「経済安全保障推進法」https://www.soumu.go.jp/menu_seisaku/kokumin/keizaianzenhosho/index_00001.html
*総務省関係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に基づく特定社会基盤事業者等に関する省令 第1条第1項イ

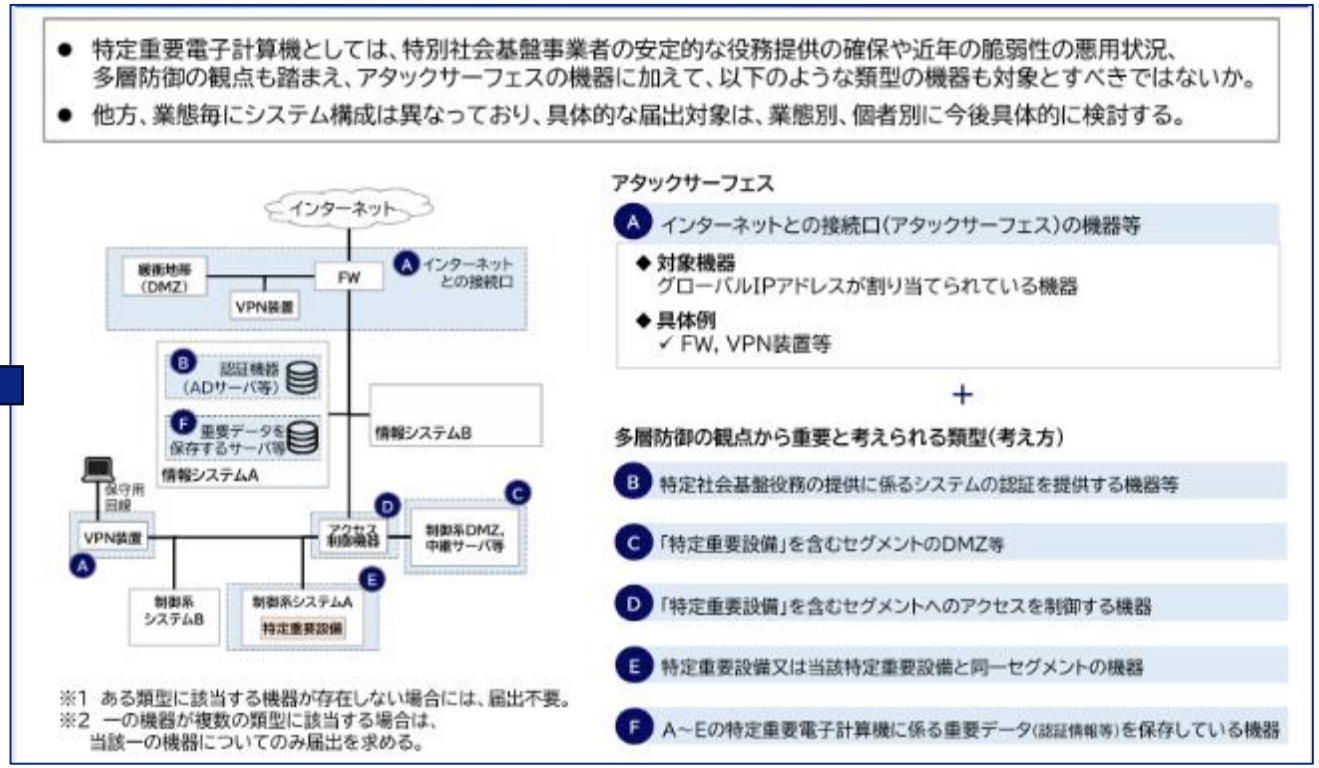
# 強化法の具体的内容①　―届出・インシデント報告・罰則―



○国家サイバー統括室のイメージ：

- 「特定重要電子機器」として届出が必要なもののカテゴリーに関し、**現時点で内閣府の案**にとどまる。
- そのため、**右図A～Fはあくまでも政府が現時点で想定しているもの**である。
- **Eに関して**は「経済安全保障推進法」でいう「**特定重要設備**」である場合には別途届け出が必要。

※パブコメへの回答では**今後明確にするとのこと**

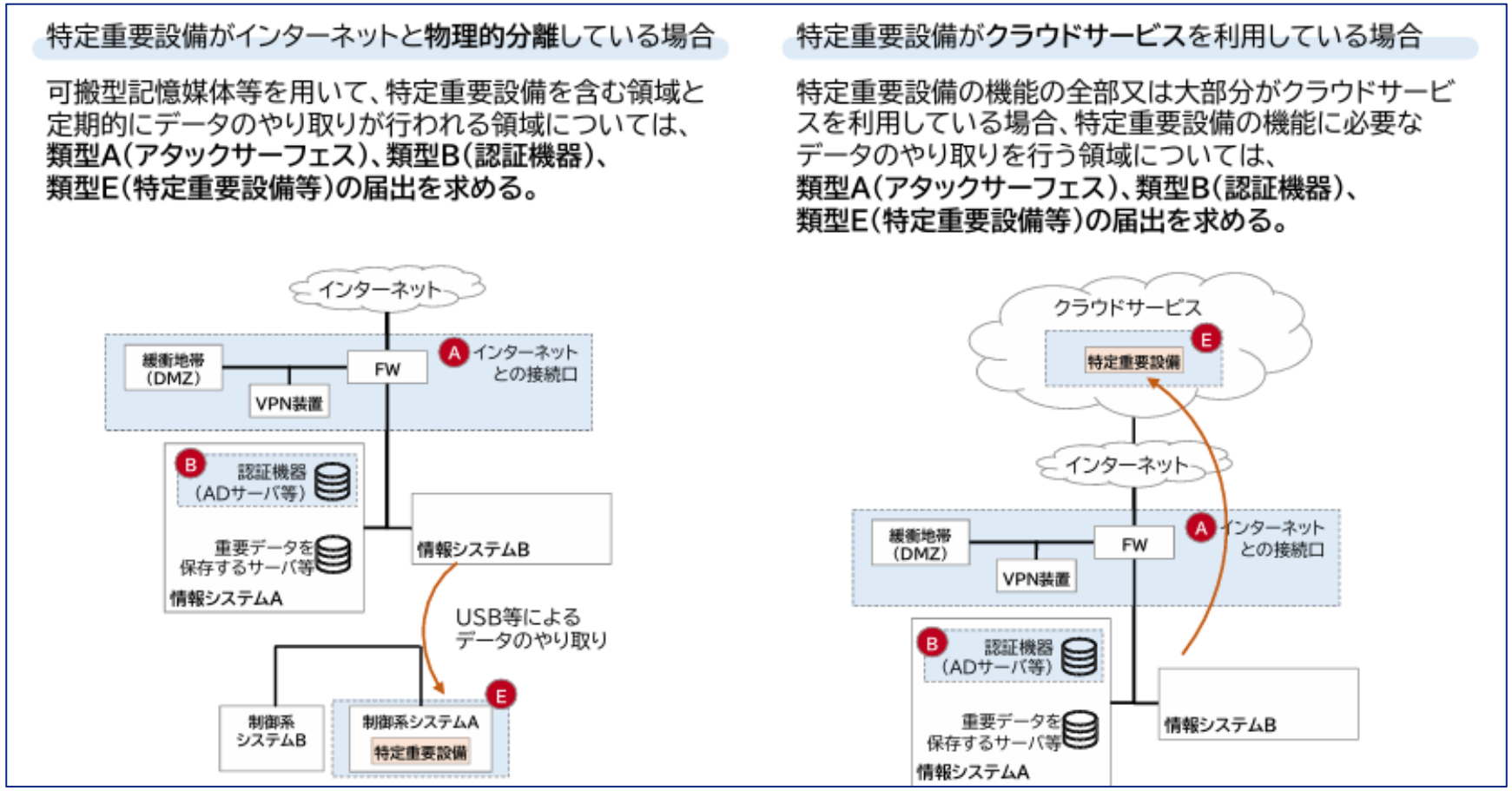



[出展]：国家サイバー統括室「サイバー対処能力強化法（官民連携の）施行に向けた考え方の案」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo05.pdf
[参考]：内閣府「サイバー対処能力強化法に基づく基本方針（案）に関するパブリックコメントの結果一覧」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo02.pdf

# 強化法の具体的内容①　―届出・インシデント報告・罰則―



- **特別社会基盤事業者が届出を所管省庁へ提出する具体例(案)**
  各事業者の持つシステム構成は千差万別であるため、政府としては事業者が届出を提出すべきポイントとして以下を提案している。




[出展]：国家サイバー統括室「サイバー対処能力強化法（官民連携の）施行に向けた考え方の案」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo05.pdf

# 強化法の具体的内容①　―届出・インシデント報告・罰則―



## ■ 業態ごとの重要システム例（当社の予想）

**別紙１　対象となる重要インフラ事業者等と重要システム例**

| 重要インフラ分野 | 対象となる重要インフラ事業者等[注1] | 対象となる重要システム例[注2] |
|---|---|---|
| 情報通信 | ・主要な電気通信事業者<br>・主要な地上基幹放送事業者<br>・主要なケーブルテレビ事業者 | ・ネットワークシステム<br>・オペレーションサポートシステム<br>・編成・運行システム |
| 金融　銀行等<br>生命保険<br>損害保険<br>証券<br>資金決済 | ・銀行、信用金庫、信用組合、労働金庫、農業協同組合等<br>・資金清算機関<br>・電子債権記録機関<br>・生命保険<br>・損害保険<br>・証券会社<br>・金融商品取引所<br>・振替機関<br>・金融商品取引清算機関<br>・主要な資金移動業者<br>・主要な前払式支払手段（第三者型）発行者　等 | ・勘定系システム<br>・資金証券系システム<br>・国際系システム<br>・対外接続系システム<br>・金融機関相互ネットワークシステム<br>・電子債権記録機関システム<br>・保険業務システム<br>・証券取引システム<br>・取引所システム<br>・振替システム<br>・清算システム |
| 航空 | ・主たる定期航空運送事業者 | ・運航システム<br>・予約・搭乗システム<br>・整備システム<br>・貨物システム |
| 空港 | ・主要な空港・空港ビル事業者 | ・警戒警備・監視システム<br>・フライトインフォメーションシステム<br>・バゲージハンドリングシステム |
| 鉄道 | ・ＪＲ各社及び大手民間鉄道事業者等の主要な鉄道事業者 | ・列車運行管理システム<br>・電力管理システム<br>・座席予約システム |
| 電力 | ・一般送配電事業者、主要な発電事業者　等 | ・電力制御システム<br>・スマートメーターシステム |
| ガス | ・主要なガス事業者 | ・プラント制御システム<br>・遠隔監視・制御システム |
| 政府・行政サービス | ・地方公共団体 | ・地方公共団体の情報システム |
| 医療 | ・医療機関<br>（ただし、小規模なものを除く。） | ・診療録等管理システム<br>・診療業務支援システム<br>・地域医療支援システム |
| 水道 | ・水道事業者及び水道用水供給事業者<br>（ただし、小規模なものを除く。） | ・水道施設や水道水の監視システム<br>・水道施設の制御システム |
| 物流 | ・大手物流事業者 | ・集配管理システム<br>・貨物追跡システム<br>・倉庫管理システム |
| 化学 | ・主要な石油化学事業者 | ・プラント制御システム |
| クレジット | ・主要なクレジットカード会社<br>・主要な決済代行業者<br>・指定信用情報機関　等 | ・クレジット（包括信用購入あっせん及び二月払購入あっせん）に係る決済システム<br>・信用情報提供・収集システム |
| 石油 | ・主要な石油精製・元売事業者 | ・受発注システム<br>・生産管理システム<br>・生産出荷システム |
| 港湾 | ・主要な港湾運送事業者・港湾管理者等 | ・ターミナルオペレーションシステム（TOS） |

注１　ここに掲げているものは、重点的に対策を実施すべき重要インフラ事業者等であり、行動計画の見直しの際に、事業環境の変化及びITへの依存度の進展等を踏まえ、対象とするものの見直しを行う。
注２　ここに掲げているものは、例であり全てではない。

重要インフラでも「**基幹インフラ**（p.6）」**に該当する事業者**に関し（例：通信、電力等）、**<u>これらシステムにおいて導入される電子計算機</u>**に留意する必要があると推測される。

[出展]：国家サイバー統括室「重要インフラのサイバーセキュリティに係る行動計画」（2025年　6月）https://www.cyber.go.jp/pdf/policy/infra/cip_policy_2025.pdf

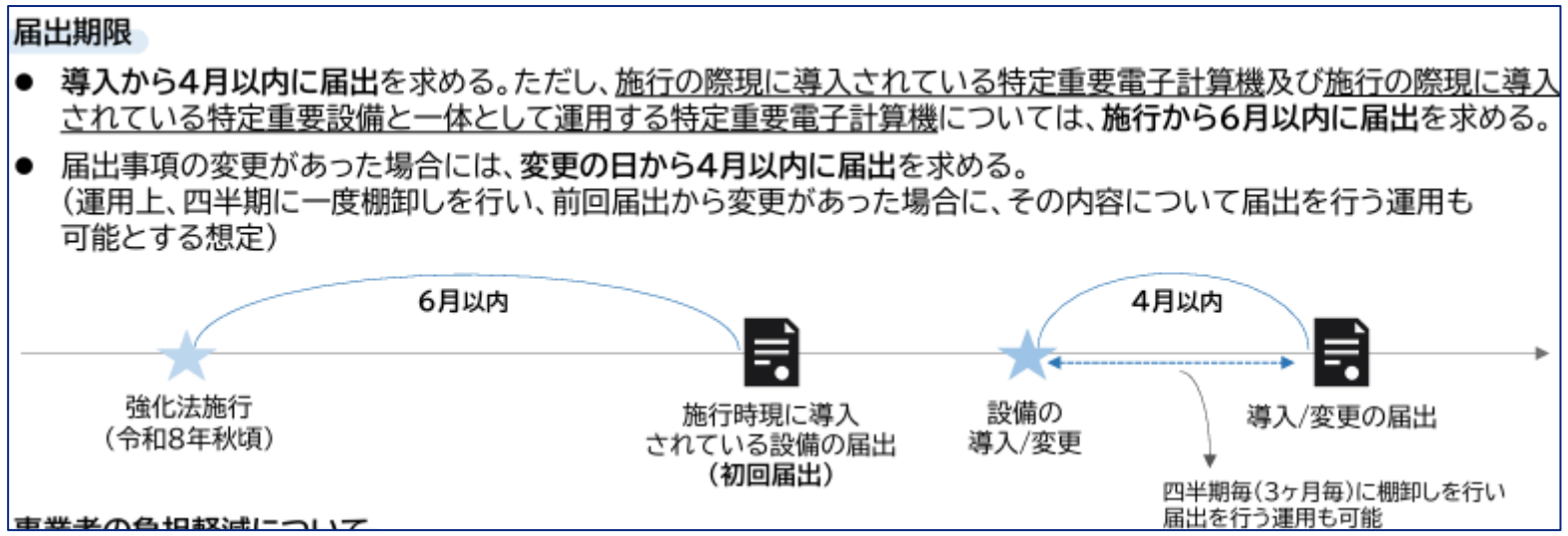
# 強化法の具体的内容①　―届出・インシデント報告・罰則―



- **届出提出の対象となる資産の範囲（案）**
  - アプライアンスの場合　　…ハードウェアの製品名、製造者名
  - アプライアンス以外の場合　…アプリケーション、ミドルウェア、OSといったソフトウェアの製品名、製造者名
  - クラウドサービスの場合　　…当該クラウドサービスのサービス名、サービス提供者名

  →基幹インフラ事業者の使用するシステムに沿った内容で届出を出すことを想定している。

- **届出の期間（予定）**




施行日（令和8年秋頃）時点で**既に**事業者で導入している場合：
→**6か月以内に設備の届出を出す**

施行日**以降に**新たに設備を導入・変更する場合：
→**導入・変更から4か月以内に行う**

[出展]：国家サイバー統括室「サイバー対処能力強化法（官民連携の）施行に向けた考え方の案」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo05.pdf

# 強化法の具体的内容①　―届出・インシデント報告・罰則―



## ■ 基幹インフラ事業者の資産届出に係るまとめ（想定）

### ● 現時点で政府が想定している届出対象の資産と手順

- 特定重要設備（「経済安全保障推進法」で届出を既に出しているものについては、強化法を基にした届出をスキップできる可能性を検討中）
- A～Fにあたる製品の**「製品名」「製造者名」**（アプライアンスの場合）
- A～Fにあたる製品の**OS、ミドルウェア、アプリケーション等の「製品名」「製造者名」**（非アプライアンスの場合）
- クラウドサービスに係る**「サービス名」「サービス提供者名」**
- **以上に該当する資産の導入から4か月以内**
- **施行時で既に導入されている資産は、施行日から6か月以内**
- **届出された資産の変更がある場合には変更の日から4か月以内**（運用上、四半期に（3か月毎）に棚卸しを行い届出を行う運用を検討中）
- 基幹インフラ事業者**以外の者が維持管理している**資産については、**当該維持管理を行うベンダー等から直接届出を行う**運用を検討中
- **類型A**（アタックサーフェス）については、**IPアドレスのレンジ等の届出**を検討中

### ● 現時点で政府が想定している届出対象外の資産

- **ハードウェア名等**についての報告（非アプライアンスの場合）
- 専ら一の基幹インフラ事業者の事業に供するもの（**専用設計品**）
- 基幹インフラ事業者の**大多数が使用していると考えられる汎用品**（届出義務の対象外とするよう扱いを検討中）

### ● 主務省令等で今後検討される可能性のある事項・未解決事項（2026年3月10日時点）

- 届出の粒度として、**製品のバージョン等**を含めるかの可否
- **台数・個体識別に係る届出**の必要性
- **構成図の提出**の可否
- **「変更」の定義**
- ベンダー等への責任の範囲



[出展]：国家サイバー統括室「サイバー対処能力強化法（官民連携の）施行に向けた考え方の案」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo05.pdf

# 強化法の具体的内容①　―届出・インシデント報告・罰則―



## ■　第5条（特定侵害事象等の報告）

特別社会基盤事業者は、特定重要電子計算機に係る特定侵害事象又は当該特定侵害事象の原因となり得る事象として主務省令で定めるものの発生を認知したときは、主務省令で定めるところにより、その旨及び主務省令で定める事項を特別社会基盤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。

➡ 第5条＝特別社会基盤事業者による**インシデント報告**

- 目的：「サイバーセキュリティの対策に必要となる報告等情報を取得する」「官民で有効な対処を行う」（＝官民連携の一つ）
  内閣府「重要電子計算機に対する特定不正行為による被害防止のための基本的な方針」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/kihonhoushin.pdf，p.5，22.

- 特定侵害事象とは？
- 当該事象の対象となり得るものとして、「**特定不正行為（強化法第2条第4項）**」に該当する行為があげられる：
  ①　刑法（明治四十年法律第四十五号）第百六十八条の二第二項の罪に当たる行為
  （いわゆるコンピュータ・ウイルスに関する罪）
  ②　不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第四項に規定する不正アクセス行為をいう。第八十条第一項において同じ。）
  ③　電子計算機を用いて行われる業務に係る刑法第二編第三十五章の罪に当たる行為であって、当該電子計算機のサイバーセキュリティを害することによって行われるもの（当該電子計算機に接続された電気通信回線の機能に障害を与えることによって行われるものを含む。）
  （電子計算機損壊等業務妨害 など）
  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る事象

[参考]：国家サイバー統括室「サイバー対処能力強化法（官民連携の）施行に向けた考え方の案」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo05.pdf
[参考]：警視庁「不正指令電磁的記録に関する罪」（2025年　6月更新）https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/law/virus.html

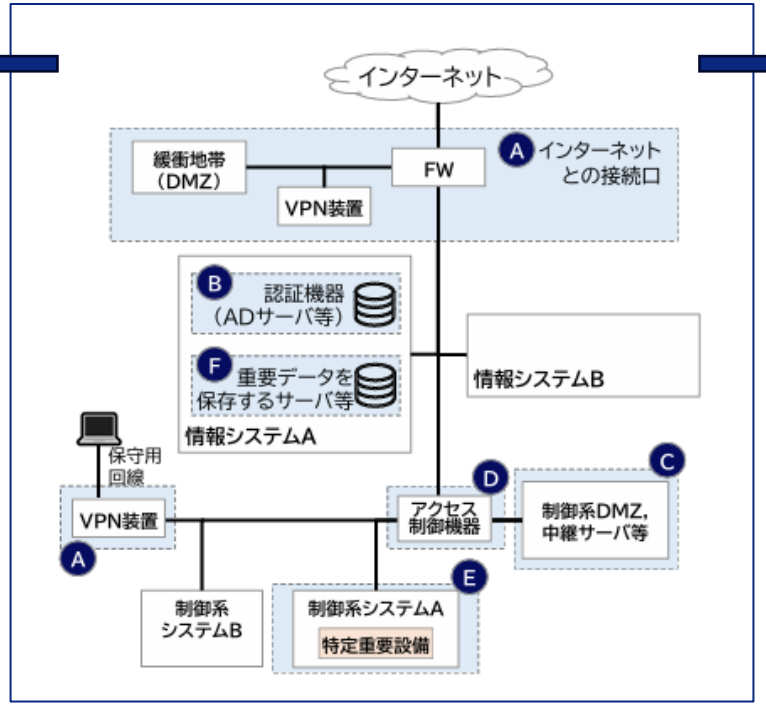
# 強化法の具体的内容①　―届出・インシデント報告・罰則―



● 事業者が行うべきインシデント報告の事案例

**A～D、Fのサイバーセキュリティが害される事象の場合**

・特定重要電子計算機において①～③に係る事象の**痕跡を認知した場合**
（マルウェアの実行やシステム内部に不正に侵入された痕跡を認知した場合等）




**E（特定重要設備）のサイバーセキュリティが害される事象の場合**

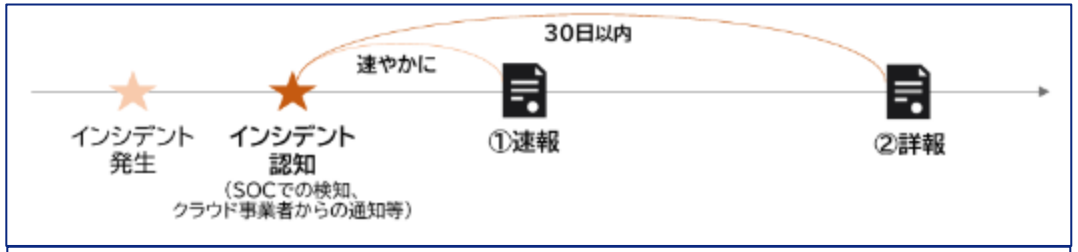
・当該特定重要設備の特定重要電子計算機において①～③に係る事象の**痕跡を認知した場合**
＋
・特定重要電子計算機において特定不正行為に**繋がる事象を認知をした場合**
例）マルウェアを受信した場合

[参考]：内閣府「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について」（2025年　8月）https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_gaiyou.pdf
[参考]：総務省「経済安全保障推進法」https://www.soumu.go.jp/menu_seisaku/kokumin/keizaianzenhosho/index_00001.html
[参考]：国家サイバー統括室「サイバー対処能力強化法（官民連携の）施行に向けた考え方の案」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo05.pdf

# 強化法の具体的内容①　―届出・インシデント報告・罰則―

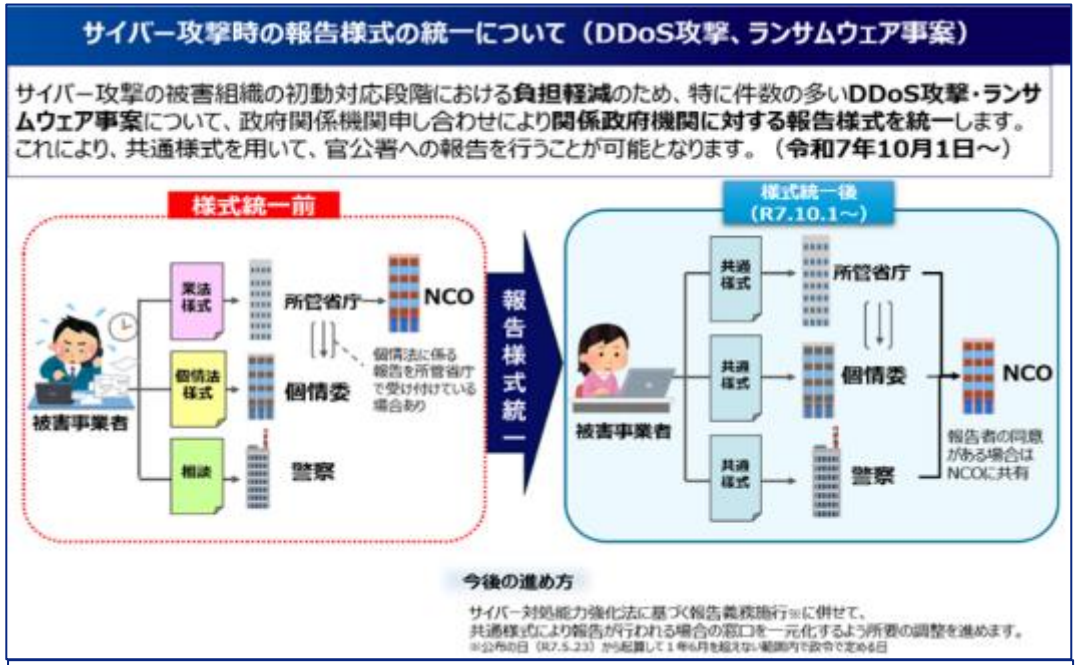


- **報告期限**




[出展]：国家サイバー統括室「サイバー対処能力強化法（官民連携の）施行に向けた考え方の案」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo05.pdf

- **報告事項**




[出展]：国家サイバー統括室「サイバー攻撃による被害発生時のインシデント報告様式の統一について」（2025年　10月）https://www.cyber.go.jp/policy/group/cyber/yoshikiichigenka.html

強化法第5条は「**報告しなければならない**」と定める所、罰則規定もあることから、今後検討すべき事項として以下が考えられる：

・①**速報**と②**詳報**のを合わせて強化法第5条の「報告」に値するのか？「報告」どの段階を指すのか？
・特に①速報の「速やかに」とは具体的にどの程度なのか？
➡政府としては**諸外国での例や、官民で有効な対処を行う観点を踏まえて期限を設定する**としている（2025年　12月時点）。

[参考]：内閣府「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 」（2025年　12月）
https://www.cao.go.jp/cybersecurity/pdf/kihonhoushin.pdf
[参考]：内閣府「重要電子計算機に対する特定不正行為による被害防止のための基本的な方針（案）に関するパブリックコメントの結果一覧」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo02.pdf

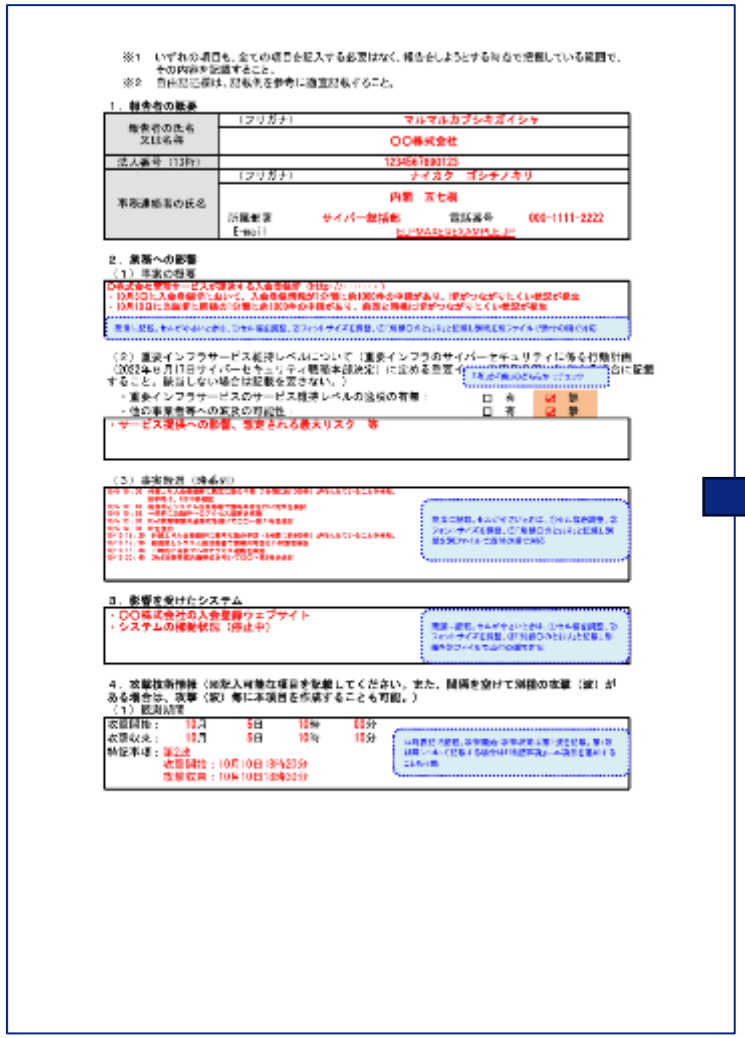
# 強化法の具体的内容①　―届出・インシデント報告・罰則―



- 攻撃技術情報に関する問い申合せの共通様式例（DDoS攻撃　ランサムウェアに関する申合せ）

ランサムウェア事案共通様式記載例（図1）

DDoS攻撃事案共通様式記載例（図2）



サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ方法

強化法第5条に基づき特別社会基盤事業者がインシデント報告を行うにあたり、国家サイバー統括室が提供する左図1.2の様式を活用して報告ができるよう、これら「共通様式を整備」し、また報告窓口に関しても「一元化するよう所要の調整を進める」としている。

[参考]：国家サイバー統括室「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」（2025年　9月）
ref_moushiawase0925.pdf



[出展]：国家サイバー統括室「サイバー攻撃による被害発生時のインシデント報告様式の統一について」（2025年　10月）https://www.cyber.go.jp/policy/group/cyber/yoshikiichigenka.html

# 強化法の具体的内容①　―届出・インシデント報告・罰則―



## ■　第6条（命令）

特別社会基盤事業所管大臣は、特別社会基盤事業者が第四条第一項若しくは第三項又は前条の規定に違反していると認めるときは、**期限を定めて**、**当該特別社会基盤事業者に対し**、第四条第一項若しくは第三項の規定により**届け出るべきものとされている事項を届け出るべきこと又は前条の規定による報告を行い**、若しくは**その報告の内容を是正すべきことを命ずることができる**。

## ■　第7条（内閣総理大臣の意見の陳述）

内閣総理大臣は、特別社会基盤事業者が第四条第一項若しくは第三項又は第五条の規定に違反していると認めるときは、**特別社会基盤事業所管大臣**に対し、当該特別社会基盤事業者に対し前条の規定による命令を行うべき旨又は他の法令の規定により**当該違反を理由として命令その他の処分を行うことができる場合**にあっては、**当該特別社会基盤事業者に対し当該処分を行うべき旨の意見を述べることができる**。

第83条　第六条の規定による命令に違反したときは、当該違反行為をした者は、二百万円以下の罰金に処する。
第84条　第九条の規定による報告若しくは資料の提出をせず、又は虚偽の報告をし、若しくは虚偽の資料を提出したときは、当該違反行為をした者は、三十万円以下の罰金に処する。

# 強化法の具体的内容②
# ―通信情報の利用等―

KDDI Research

# 強化法の具体的内容② ―通信情報の利用等(1)―



- 協定に基づく通信情報の取得

■ 第11条（特別社会基盤事業者との協定の締結）

内閣総理大臣は、**特別社会基盤事業者との間**で、内閣総理大臣が、**当該特別社会基盤事業者を通信の当事者とする通信情報の提供を受けた上で、当該通信情報のうち外内通信情報**（外内通信（当該通信に係るアイ・ピー・アドレスその他の電気通信設備を識別する符号（第十七条第一項、第二十二条第二項第一号及び第三十三条第一項において「アイ・ピー・アドレス等」という。）から判断して、国外設備から国内設備（国外設備以外の電気通信設備をいう。第十七条第一項及び第三十三条第一項において同じ。）に送信される電気通信に該当すると認められる電気通信をいう。第二十二条第一項第一号、第三十二条第一項及び第三十五条第一項第一号において同じ。）により送受信が行われる情報に係る通信情報をいう。次条第一項において同じ。）**に該当するものを用いて、当該特別社会基盤事業者が使用する特定重要電子計算機その他の電子計算機のサイバーセキュリティの確保を図るために必要な分析を行い**、その**分析の結果及びこれに関連する情報**（第二号及び第十六条において「個別分析情報」という。）**を当該特別社会基盤事業者に提供することを内容とする協定であって、次に掲げる事項を含むものを締結することができる。**

一　内閣総理大臣が提供を受ける通信情報の範囲並びに提供の方法及び期間に関する事項

二　内閣総理大臣からの個別分析情報の提供の要領に関する事項

三　通信情報の提供のために施設又は設備の整備が必要な場合にあっては、当該施設又は設備の整備に関する事項

四　協定を変更し、又は廃止する場合の手続に関する事項

五　第三十八条第三項に規定する同意をする場合にあっては、その旨

六　その他内閣府令で定める事項

➡特別社会基盤事業者と「協定を結ぶ」ことで、特定社会基盤事業者の持つネットワークシステムにおけるサイバーセキュリティ対策を目的とした**外内通信情報**を当該事業者から提供してもらい、提供された情報を分析し、その分析結果及び関連情報（個別分析情報）を当該事業者に対し提供する協議をとることができる

# 強化法の具体的内容② ―通信情報の利用等(1)―



● 協定に基づく通信情報の取得

■ 第11条（特別社会基盤事業者との協定の締結）

2 内閣総理大臣及び特別社会基盤事業者は、**相互に、相手方に対し、前項の協定を締結することについて協議を求める**ことができる。この場合において、当該求めを受けた内閣総理大臣又は特別社会基盤事業者は、**正当な理由がない限り、当該求めに係る協議に応じなければならない**。

3 第一項の協定において、同項第一号に規定する**提供の方法**として、**当該協定を締結する特別社会基盤事業者に事業電気通信役務を提供する電気通信事業者が管理する当該特別社会基盤事業者を通信の当事者とする媒介中通信情報であって、当該特別社会基盤事業者が内閣総理大臣に提供することに同意した範囲のものが複製され、内閣総理大臣の設置する設備に送信されるようにする方法**（電気通信事業法第四条第一項に規定する通信の秘密の確保に支障がない方法に限る。）を定めようとする場合には、**当該協定は、内閣総理大臣、当該特別社会基盤事業者及び当該電気通信事業者により締結しなければならない**。

➡特別社会基盤事業者のもつネットワークシステムに使用している電気通信の提供者である電気通信事業者が持つ通信情報を国に提供する場合、この電気通信事業者も含めて協定を締結をしなければならない（三者協定が必要になる）。

＝第11条は、①特別社会基盤事業者もつ通信情報、②当該事業者のネットワークシステムに使用している電気通信事業者がもつ情報を国に提供して、その後分析等を行ってもらうための協定を国と企業で結ぶことが求められることとなる。（➡電気通信事業者は特に本強化法の内容に関わってくると想定される）



［参考］：榎本尚行（内閣委員会調査室）「能動的サイバー防御2法案の国会議論（２）－通信情報の利用と通信の秘密－」（参議院事務局企画調整室、2025年）立法と調査　477号　3-22頁。

# 強化法の具体的内容② ―通信情報の利用等(1)―



● 協定に基づく通信情報の取得

■ 第12条（特別社会基盤事業者以外の事業電気通信役務の利用者との協定の締結）

内閣総理大臣は、**事業電気通信役務の利用者**（事業電気通信役務を利用する者をいい、特別社会基盤事業者を除く。以下この項及び次条において「利用者」という。）との間で、**内閣総理大臣が、当該利用者を通信の当事者とする通信情報の提供を受けた上で、当該通信情報のうち外内通信情報に該当するものを用いて、当該利用者が使用する電子計算機のサイバーセキュリティの確保を図るために必要な分析を行い、その分析の結果及びこれに関連する情報**（第二号及び第十六条において「利用者個別分析情報」という。）**を当該利用者に提供する**ことを内容とする協定であって、次に掲げる事項を含むものを**締結することができる。**

一　内閣総理大臣が提供を受ける通信情報の範囲並びに提供の方法及び期間に関する事項

二　内閣総理大臣からの利用者個別分析情報の提供の要領に関する事項

三　通信情報の提供のために施設又は設備の整備が必要な場合にあっては、当該施設又は設備の整備に関する事項

四　協定を変更し、又は廃止する場合の手続に関する事項

五　第三十八条第三項に規定する同意をする場合にあっては、その旨

六　その他内閣府令で定める事項

2　前条第三項の規定は、前項の協定について準用する。

➡特別社会基盤事業者以外の事業者（事業電気通信役務を利用する者）においても、協定を国と結ぶことで外内通信に係る情報を提供し、当該情報を分析してもらい、当該利用者へその結果を提供してもらう協議をとることが可能になる。（通信事業者が持つ情報を提供する場合には、第11条第3項同様に三者協定を結ぶ必要が出てくる）。

※ただし、特別社会基盤事業者は「正当な理由がない場合は協定を結ぶ（第11条第2項）」のに対し、第12条の対象となる事業者にこうした規定は設けられていない。

# 強化法の具体的内容② ―通信情報の利用等(1)―



● 協定に基づく通信情報の取得(電気通信事業者の役割)

■ 第13条 (電気通信事業者に対する協議の求め)

内閣総理大臣は、**当事者協定**(第十一条第一項又は前条第一項の協定をいう。以下同じ。)**に基づき通信情報の提供を受ける方法として、協定当事者**(第十一条第一項の協定を締結する特別社会基盤事業者又は前条第一項の協定を締結する利用者をいう。以下同じ。)**に係る当事者管理通信情報を複製したものの提供を受ける方法をとることが困難な場合であって、当該協定当事者が**第十一条第三項(前条第二項において準用する場合を含む。)**に規定する方法をとることについて同意したとき**は、当該協定当事者に事業電気通信役務を提供する**電気通信事業者に対して、**当事者協定を締結することについて協議を求めることができる。この場合において、当該求めを受けた電気通信事業者は、正当な理由がない限り、当該求めに係る協議に応じなければならない。

➡第11条・第12条に該当する事業者で、当該事業者が通信情報を提供できない場合にあり、かつこれら事業者が同意した場合には、当該事業者に事業電気通信役務を提供する電気通信事業者へ協定を締結する協議を求めることができる。

■ 第15条 (通信情報の取得)

内閣総理大臣は、**その締結した当事者協定の定めるところに従い**、当該当事者協定の**協定当事者を通信の当事者とする通信情報の提供を受けることができる。**

➡第11条・第12条をもとに協定を結んだ当事者(特別社会基盤事業者、それ以外の事業者、電気通信事業者)から、内閣総理大臣は通信情報の提供を受けることができる。



KDDI Research

# 強化法の具体的内容②　―通信情報の利用等(1)―



- 協定に基づく通信情報の取得(電気通信事業者の役割)

強化法第13条における当事者協定及び同意とは？

・内閣府「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」(2025年　12月)

「法第13条に規定する**当事者協定**は、内閣府が、**特別社会基盤事業者その他の事業電気通信役務の利用者**(協定当事者)**との間で協定**(当事者協定)を締結し、**当事者協定による同意の下**で**協定当事者から取得した通信情報を利用するための制度**である。当該制度は、当事者協定により取得した通信情報を、①重要電子計算機に対する国外通信特定不正行為による被害を防止する目的、及び②協定当事者が使用する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目的で利用することで、①'重要電子計算機を使用する我が国の行政機関や特別社会基盤事業者等の全体、及び②'協定当事者の双方におけるサイバーセキュリティの確保に資するものである」

「また、本制度は、当事者協定の締結により**協定当事者から同意を得ていることを前提**として、その同意の範囲内で通信情報を利用するものであることから、有効な同意に基づかない当事者協定による通信情報の利用は、本制度の趣旨からしても、また、通信の秘密との関係においても許容されるものではない。このため、内閣府は、当事者協定の締結が事実上の強制とならないよう十分に配慮するとともに、間接的な強制を回避するためにも協議の結果として当事者協定を締結しなかった者に対して不当に不利益な取扱いをしないこととする。」

[参考]：内閣府「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 」（2025年　12月) https://www.cao.go.jp/cybersecurity/pdf/kihonhoushin.pdf

# 強化法の具体的内容②　―通信情報の利用等(1)―



- **電気通信事業者とは？**

・強化法第2条第6項第1号：
「事業電気通信役務(**電気通信事業者**(**電気通信事業法(昭和五十九年法律第八十六号)第二条第五号に規定する電気通信事業者をいう**。以下同じ。)が営む電気通信事業(同条第四号に規定する電気通信事業をいう。第十七条第一項において同じ。)により提供される同法第二条第三号に規定する電気通信役務をいう。以下同じ。)によって媒介される…」

・電気通信事業法第2条第5号：
「電気通信事業者　電気通信事業を営むことについて、**第九条の登録を受けた者**及び**第十六条第一項(同条第二項の規定により読み替えて適用する場合を含む。)の規定による届出をした者**をいう。」

**総務省「電気通信事業者数の推移」(2026年　1月更新)では、**
**27,041社が電気通信事業者として登録又は届出を出しているとされる。**

[参考]：総務省「電気通信事業者の推移」https://www.soumu.go.jp/johotsusintokei/field/tsuushin04.html

# 強化法の具体的内容② ―通信情報の利用等(2)―



## ● 協定に基づかない通信情報の取得(i)(電気通信事業者に対し)

■ 第17条 (外外通信目的送信措置)

内閣総理大臣は、**外外通信**(当該通信に係るアイ・ピー・アドレス等から判断して国外設備を送信元及び送信先とする電気通信に該当すると認められる電気通信であって、国内設備を用いて媒介されるものをいう。第二十二条第一項第二号において同じ。)であって、**重要電子計算機に対する国外通信特定不正行為のうちその実行のために用いられる電子計算機、当該電子計算機に動作をさせるために用いられる指令情報その他の当該国外通信特定不正行為に関する実態が明らかでないために当該国外通信特定不正行為による重要電子計算機の被害を防止することが著しく困難**であり、かつ、**この項の規定による措置以外の方法によっては当該実態の把握が著しく困難であるもの**に関係するものが、特定の国外関係電気通信設備(電気通信事業者の電気通信事業の用に供する電気通信設備であって、他の電気通信設備との接続の状況その他の事項により、当該電気通信設備を用いて提供される事業電気通信役務が国外関係通信(当該通信に係るアイ・ピー・アドレス等から判断して国外設備を送信元又は送信先とする電気通信に該当すると認められる電気通信をいう。以下この項、第三十二条第一項及び第三十三条第一項において同じ。)を媒介していると認められるものをいう。以下同じ。)を用いて提供される事業電気通信役務が媒介する国外関係通信に含まれると疑うに足りる場合において、**必要と認めるときは、当該国外通信特定不正行為に関する第二十二条第二項に規定する選別の条件を定めるための基準**(同項において「外外通信選別条件設定基準」という。)**を定め、サイバー通信情報監理委員会の承認を受けて、当該国外関係通信により送受信が行われる媒介中通信情報**(第三十二条第一項及び第三十三条第一項において「国外関係通信媒介中通信情報」という。)の一部(当該国外関係電気通信設備の伝送容量の百分の三十を上限とする。)が**複製され、内閣総理大臣の設置する設備**(第三十二条第一項及び第三十三条第一項において「受信用設備」という。)**に送信されるようにするための措置**(以下「外外通信目的送信措置」という。)**を講ずることができる**。

2 二以上の国外通信特定不正行為が次に掲げる場合に該当する場合における前項の規定の適用については、これらを一の国外通信特定不正行為とみなす。

一 その実行のために用いられる電子計算機(電気通信回線に接続されているものに限る。次号において同じ。)の全部又は一部が共通すると疑うに足りる状況がある場合

二 前号に掲げる場合のほか、電子計算機の動作をさせるために用いられる指令情報その他の国外通信特定不正行為の特徴が共通すると疑うに足りる状況がある場合

3 外外通信目的送信措置を講ずることができる期間(第十九条第一項において「措置期間」という。)は、六月とする。ただし、次条の規定による条件としてサイバー通信情報監理委員会が六月未満の期間を定めたときは、当該期間とする。

➡日本の基幹インフラ事業者等には行き届いていない、「海外」の国々における通信の情報に関し、その中継地点に日本の電気通信事業者が介在している場合に限り、その通信情報を国へ複製することが求められる場合がある。



KDDI Research

# 強化法の具体的内容② ―通信情報の利用等(1)―



- 協定に基づかない通信情報の取得(i)(電気通信事業者に対し)

■ 第20条 (電気通信事業者に対する協力の求め)

内閣総理大臣は、**外外通信目的送信措置の実施**に関し、国外関係電気通信設備を設置する**電気通信事業者**(以下この条、第三十二条第一項及び第三十三条第一項において「国外関係電気通信事業者」という。)に対し、**当該国外関係電気通信設備に関する情報の提供、当該実施のための機器の接続その他の必要な協力を求めることができる。この場合において、当該国外関係電気通信事業者は、正当な理由がない限り、これを拒んではならない。**

➡第17条の規定に該当し、かつ第20条において内閣総理大臣からの要請があった電気通信事業者から、内閣総理大臣は通信情報の提供を受けることができる。ここで、内閣総理大臣は当該国外関係電気通信事業者から情報の提供を要請するすることができ、正当な理由なく当該国外関係電気通信事業者は提供を拒否できない。

# 強化法の具体的内容② ―通信情報の利用等(2)―



- サイバー通信情報監理委員会の役割

## ■ 第14条（当事者協定を締結したときのサイバー通信情報監理委員会への通知）

内閣総理大臣は、**当事者協定を締結し、変更し、又は廃止したとき**は、遅滞なく、当該当事者協定又は変更の内容（当事者協定を廃止した場合にあっては、その旨）を**サイバー通信情報監理委員会**に通知しなければならない。

## ■ 第18条（サイバー通信情報監理委員会の承認）

サイバー通信情報監理委員会は、前条第一項の承認の求めがあった場合において、**当該求めに理由があると認めるときは、遅滞なく、当該承認をするものとする**。この場合において、サイバー通信情報監理委員会は、当該求めに係る外外通信目的送信措置の実施又は当該外外通信目的送信措置により内閣総理大臣が取得する取得通信情報の取扱いに関し、適当と認める条件を付することができる。

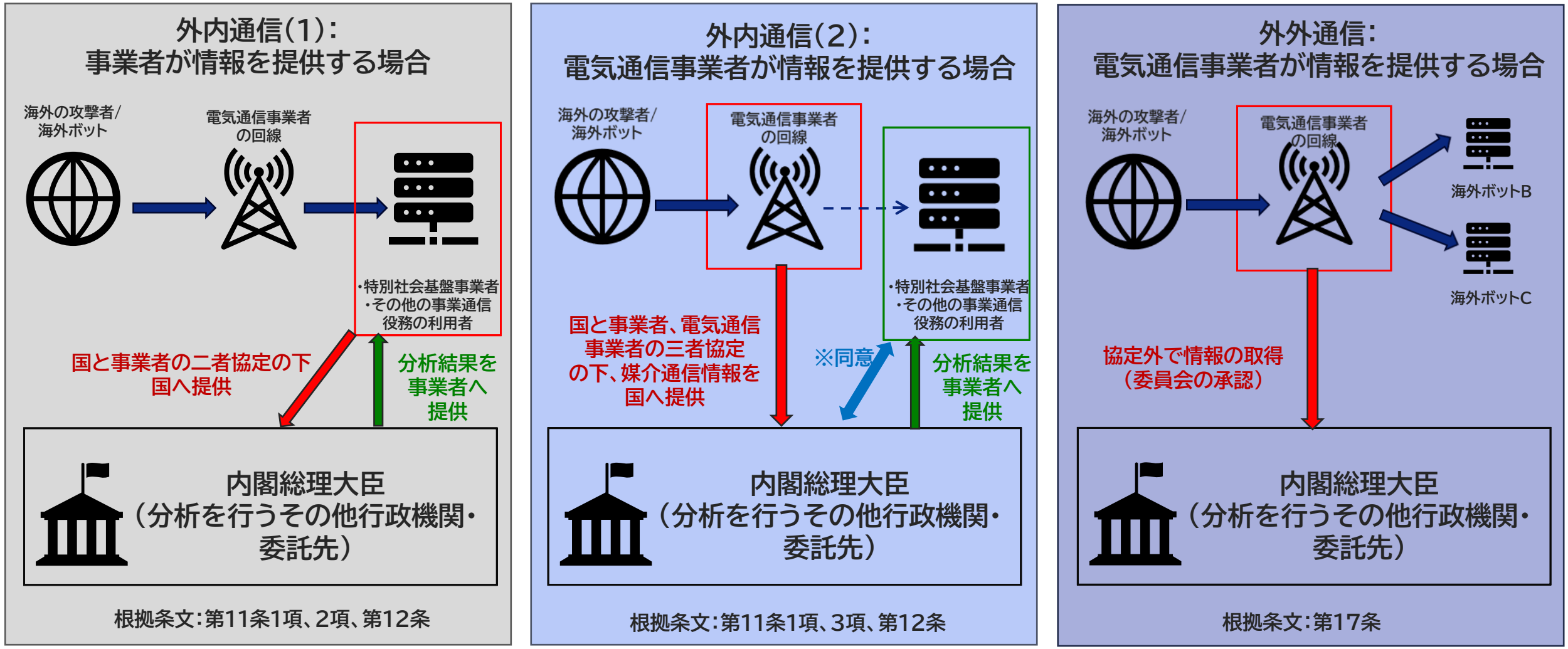
〇協定に基づいて内閣総理大臣が特別社会基盤事業者又はその他の利用者からの同意で情報を取得したい場合（第11条・第12条）：
➡協定の締結、協定の変更、協定の廃止があった場合にはサイバー通信情報監理委員会に遅滞なく通知が必要。

〇協定に基づかない場合で内閣総理大臣が電気通信事業者から情報を取得したい場合（第17条・第32条・第33条）：
➡サイバー通信情報監理委員会からの承認が必要。

# 強化法の具体的内容② ―通信情報の利用等(2)―



- 「どの通信が」、「誰から」、「どこへ」提供されるのか？(概念図)




※電気通信事業者から媒介通信情報を得る同意

政府資料を元にKDDI総合研究所が作成

# 強化法の具体的内容② ―通信情報の利用等(2)―



- 協定に基づかない通信情報の取得(ii)

■ 第32条 (特定外内通信目的送信措置)

内閣総理大臣は、**外内通信であって**、重要電子計算機に対する国外通信特定不正行為に用いられていると疑うに足りる状況のある特定の国外設備を送信元とし、又は**当該国外通信特定不正行為に用いられていると疑うに足りる状況のある特定の機械的情報**(外国の政府又は国際機関、関係行政機関その他の関係機関から自動選別以外の方法で取得した情報であって機械的情報に相当するものを含む。次条第一項及び第三十五条第二項第二号において同じ。)が含まれているもの(以下この項及び同条第二項において「特定外内通信」という。)の分析をしなければ**当該国外通信特定不正行為による重要電子計算機の被害を防止することが著しく困難であり、かつ、この項の規定による措置以外の方法(次条第一項に規定する特定内外通信目的送信措置を除く。)によっては当該特定外内通信の分析が著しく困難である場合**において、必要と認めるときは、この項の規定による措置により取得通信情報を取得した場合における第三十五条第二項に規定する選別の条件を定めるための基準(同項において「特定外内通信選別条件設定基準」という。)を定め、**サイバー通信情報監理委員会の承認を受けて、国外関係電気通信事業者の設置する特定の国外関係電気通信設備であって当該国外関係電気通信設備を用いて媒介される国外関係通信に当該特定外内通信が含まれると疑うに足りるものにより送受信が行われる国外関係通信媒介中通信情報が複製され、受信用設備に送信されるようにするための措置**(以下「特定外内通信目的送信措置」という。)**を講ずることができる**。

2 **第十七条第三項及び第十八条から第二十条までの規定**は、前項の規定により内閣総理大臣が特定外内通信目的送信措置を講ずる場合について**準用する**。この場合において、第十七条第三項及び第十九条第三項中「六月」とあるのは「三月」と、第十八条中「前条第一項」とあり、及び第十九条第一項中「第十七条第一項」とあるのは「第三十二条第一項」と読み替えるものとする。

➡国外から国内に向けてサイバー攻撃等が仕掛けられていると疑うに足りる状況において機械的情報が含まれているものを分析しないと重要電気計算機の被害を防止できなくなり、これ以外の方法がないとされ、必要である場合には、国外関係電気通信事業者のもつ通信情報が複製されたものを当該国外関係電気通信事業者から送信させる措置が、委員会の承認の下内閣総理大臣によって取られ得る。

# 強化法の具体的内容② ―通信情報の利用等(2)―



- 協定に基づかない通信情報の取得(ii)

■ 第33条 (特定内外通信目的送信措置)

内閣総理大臣は、**内外通信**(当該通信に係るアイ・ピー・アドレス等から判断して、国内設備から国外設備に送信される電気通信に該当すると認められる電気通信をいう。第三十五条第一項第二号において同じ。)**であって、重要電子計算機に対する国外通信特定不正行為に用いられていると疑うに足りる状況のある特定の国外設備を送信先とし、又は当該国外通信特定不正行為に用いられていると疑うに足りる状況のある特定の機械的情報が含まれているもの**(以下この項及び同条第二項において「特定内外通信」という。)の分析をしなければ当該国外通信特定不正行為による**重要電子計算機の被害を防止することが著しく困難であり、かつ、この項の規定による措置以外の方法によっては当該特定内外通信の分析が著しく困難である**場合において、必要と認めるときは、当該措置により取得通信情報を取得した場合における同条第二項に規定する選別の条件を定めるための基準(同項において「特定内外通信選別条件設定基準」という。)を定め、**サイバー通信情報監理委員会の承認を受けて、国外関係電気通信事業者の設置する特定の国外関係電気通信設備であって当該国外関係電気通信設備を用いて媒介される国外関係通信に当該特定内外通信が含まれると疑うに足りるものにより送受信が行われる国外関係通信媒介中通信情報が複製され、受信用設備に送信されるようにするための措置**(以下「特定内外通信目的送信措置」という。)**を講ずることができる。**

2 **第十七条第三項及び第十八条から第二十条までの規定**は、前項の規定により内閣総理大臣が特定内外通信目的送信措置を講ずる場合について**準用する。**この場合において、第十七条第三項及び第十九条第三項中「六月」とあるのは「三月」と、第十八条中「前条第一項」とあり、及び第十九条第一項中「第十七条第一項」とあるのは「第三十三条第一項」と読み替えるものとする。

➡国外からのサイバー攻撃等を違う国外へ行うために、例えば日本のサーバー等が踏み台として、見かけとしては日本から海外へ当該攻撃の通信が行われていると疑うに足りる状況において、機械的情報が含まれているものを分析しないと重要電気計算機の被害を防止できなくなり、これ以外の方法がないとされ、必要である場合には、国外関係電気通信事業者のもつ通信情報が複製されたものを、当該国外関係電気通信事業者から送信させる措置が、委員会の承認の下内閣総理大臣によって取られ得る。

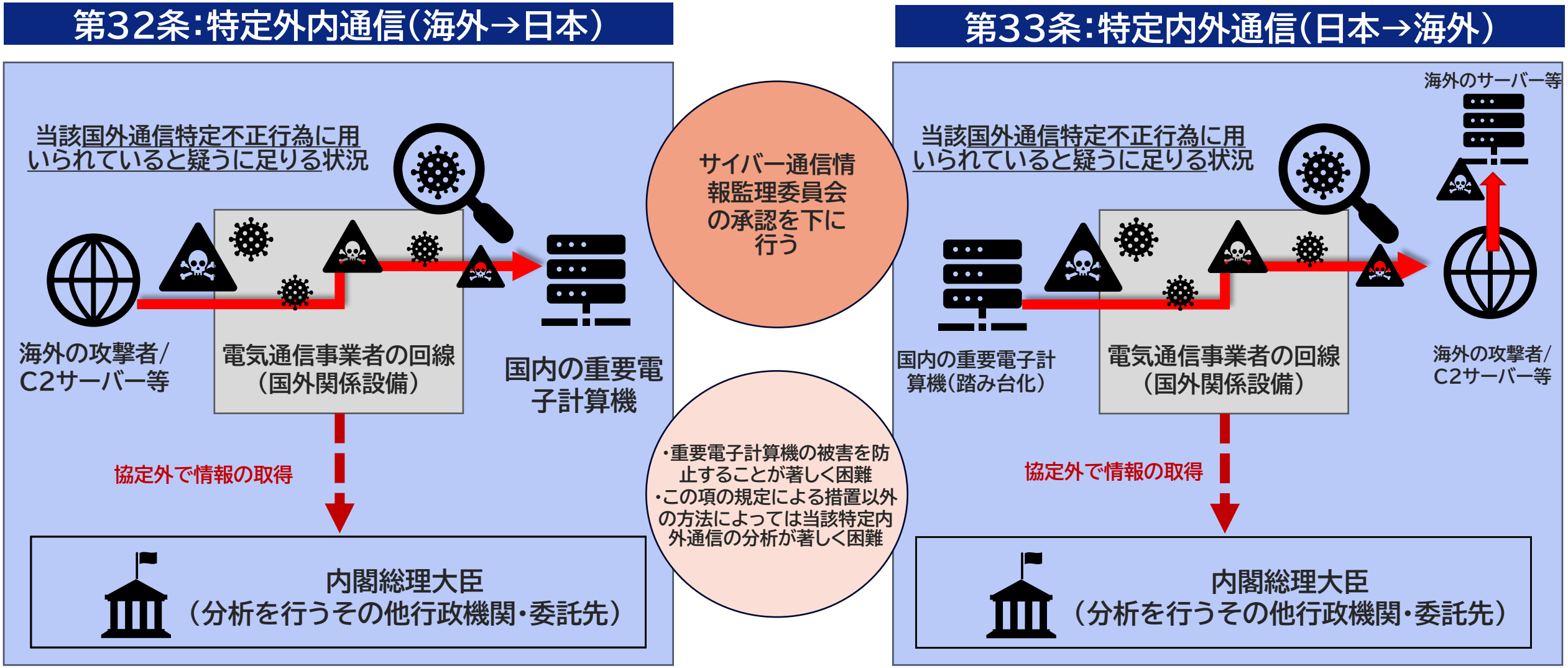


KDDI Research

# 強化法の具体的内容② ―通信情報の利用等(2)―



■ 協定に基づかない通信情報の取得(ii)(概念図)




政府資料を元にKDDI総合研究所が作成

# 強化法の具体的内容②　―通信情報の利用等（2）―



- **通信情報はどのように国へ渡すのか？**

「通信情報の利用に係る制度の運用に当たっては、内閣府及び法第27条第1項の関係行政機関は、情報保全にも配慮しつつ、通信情報の利用に係る分析能力の構築に努めることとする。具体的には、巧妙化・高度化するサイバー攻撃にも有効に対処できるよう、**関係行政機関は、通信情報の自動選別や整理・分析等を効果的に行うために必要な機能を具備したシステム・設備の的確な整備を進めることとする**。また、情報の整理・分析その他の本制度の運用に係る事務に従事する職員についても、サイバー安全保障、情報通信技術、法律などの専門的知識及び経験を有する多様な人材を確保するとともに、組織的かつ計画的にその育成を図ることとする。」

「通信の当事者の同意によらずに通信情報を取得し、利用する措置の実施に当たっては、**内閣府が設置する受信用設備に通信情報を送信する電気通信事業者の協力が必須である**。このため、法第20条では、内閣総理大臣は、法第17条第1項に規定する外外通信目的送信措置の実施に関し、国外関係電気通信設備を設置する電気通信事業者に対して、当該国外関係電気通信設備に関する情報の提供、当該実施のための機器の接続その他の必要な協力を求めることができると規定しており、また、当該協力の求めを受けた電気通信事業者は、正当な理由がない限り、これを拒んではならないと規定している。」

[参考]：内閣府「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 」（2025年　12月) https://www.cao.go.jp/cybersecurity/pdf/kihonhoushin.pdf

# 強化法の具体的内容② ―通信情報の利用等(3)―



- 国へ提供された通信情報のどの部分を分析し取扱うのか？

■ 第21条（定義）
この章において取得通信情報に係る「対象不正行為」とは、第十五条の規定により取得した取得通信情報である場合にあっては重要電子計算機に対する**国外通信特定不正行為又は協定当事者が使用する電子計算機に対する特定不正行為をいい、外外通信目的送信措置により取得した取得通信情報である場合にあっては当該外外通信目的送信措置に係る第十八条の規定による承認に係る国外通信特定不正行為**をいう。（自動選別の実施）

■ 第22条（自動選別の実施）
内閣総理大臣は、第十五条の規定又は外外通信目的送信措置により**取得通信情報を取得したときは**、当該取得通信情報の中から次に掲げる要件を満たす**機械的情報であるもののみを選別して記録する措置**であって、その選別が完了する前に当該取得通信情報が何人にも閲覧その他の知得をされない自動的な方法（第三十五条第一項において「自動的方法」という。）で行われるもの（以下「自動選別」という。）を講じなければならない。
一　第十五条の規定により取得した取得通信情報については、外内通信により送受信が行われたものであること。
二　外外通信目的送信措置により取得した取得通信情報については、外外通信により送受信が行われたものであること。
三　当該取得通信情報に係る対象不正行為に関係があると認めるに足りる状況のあるものであること。
2　前項第三号に掲げる要件を満たす取得通信情報を選別するための自動選別は、次の各号のいずれかに該当する情報のうち二以上のものを選別の条件に用いて行うものでなければならない。この場合において、外外通信目的送信措置により取得した取得通信情報についての選別の条件は、外外通信選別条件設定基準に従って定められたものでなければならない。
一　当該取得通信情報に係る対象不正行為に関係がある電気通信の送信元又は送信先であると認めるに足りる状況のある電気通信設備のアイ・ピー・アドレス等
二　当該取得通信情報に係る対象不正行為の実施に用いられるものと認めるに足りる状況のある指令情報
三　前二号に掲げる情報のほか、当該情報を選別の条件に用いて自動選別を行うことにより当該取得通信情報に係る対象不正行為に関係がある電気通信、電子計算機又は電磁的記録の探査が容易になると認めるに足りる状況のある情報
3　内閣総理大臣は、自動選別が終了したときは、直ちに、当該自動選別により得られた取得通信情報を除き、自動選別の対象となった取得通信情報の全てを消去しなければならない。

# 強化法の具体的内容②　―通信情報の利用等(3)―



■　第23条（利用及び提供の制限）

内閣総理大臣は、取得通信情報の自動選別を行う場合を除き、**自動選別を行う前の取得通信情報を自ら利用し、又は提供してはならない**。

2　内閣総理大臣は、第四項の規定による場合を除き、重要電子計算機に対する**国外通信特定不正行為**（対象不正行為であって当該国外通信特定不正行為に該当しないものを含む。）による被害を防止する目的（以下「特定被害防止目的」という。）以外の目的のために、自動選別により得られた取得通信情報（当該取得通信情報を複製し、又は加工して作成された情報（第二十九条に規定する提供用選別後情報となったものを除く。）を含む。以下「選別後通信情報」という。）を**自ら利用してはならない**。

3　内閣総理大臣は、次項の規定による場合を除き、**選別後通信情報を提供してはならない**。

4　内閣総理大臣は、次に掲げる場合には、選別後通信情報を、**特定被害防止目的以外の目的のために自ら利用**し、又は提供することができる。

一　第十五条の規定により取得した取得通信情報についての自動選別により得られた選別後通信情報（第三十八条第三項において「選別後当事者通信情報」という。）を、当該当事者協定の協定当事者の同意を得て、自ら利用し又は提供する場合

二　第二十七条第三項若しくは第二十八条（これらの規定を第三十六条の規定により適用する場合を含む。）の規定により選別後通信情報を提供し、又は第三十八条第一項若しくは第二項の規定により選別後通信情報を含む総合整理分析情報を提供する場合

三　第十七条第一項、第十九条第一項（第三十二条第二項及び第三十三条第二項において準用する場合を含む。）、第三十二条第一項又は第三十三条第一項の承認を求めるために、サイバー通信情報監理委員会に提供する場合

四　第六十三条第一項又は第二項の規定による検査に際し、サイバー通信情報監理委員会に提供する場合五　第六十四条第二項の規定により提供する場合

■　第24条（非識別化措置等）

内閣総理大臣は、特定記述等（電子メールアドレス（特定電子メールの送信の適正化等に関する法律（平成十四年法律第二十六号）第二条第三号に規定する電子メールアドレスをいい、ドメイン名（電気通信事業法第百六十四条第二項第二号に規定するドメイン名をいう。）以外の部分に限る。）その他の特定の個人を識別することができることとなるおそれが大きいと認められる情報（公開されていない他の情報との照合（容易に行うことができるものに限る。）により特定の個人を識別することができることとなるおそれが大きいと認められるものを含む。）をいう。以下この項及び次項において同じ。）が含まれている選別後通信情報を取り扱うときは、当該選別後通信情報について、当該特定記述等の全部又は一部を他の符号（特定記述等となるものを除く。）に変換することその他の方法によって他の情報と照合しない限り特定の個人を識別することができないようにするための措置（以下この条、第三十条第二号及び第六十三条第一項において「非識別化措置」という。）を講じなければならない。

2　内閣総理大臣は、選別後通信情報について前項の規定により非識別化措置を講じた場合において、当該選別後通信情報と選別後通信情報以外の情報であって特定記述等を含むものとの照合による分析を行うことが特定被害防止目的の達成のために特に必要があると認めるときは、当該選別後通信情報について、その必要な限度において、当該非識別化措置を講じた特定記述等の復元その他の当該特定記述等を利用することができるようにするための措置（以下この条、第三十条第二号及び第六十三条第一項において「再識別化措置」という。）を講ずることができる。

3　内閣総理大臣は、前項の規定による再識別化措置を講じた選別後通信情報について、再識別化措置の必要がなくなったときは、直ちに、再び非識別化措置を講じなければならない。

4　内閣総理大臣は、第二項の規定により再識別化措置を講ずる場合を除き、特定の個人を識別するために、第一項又は前項の規定により非識別化措置が講じられている選別後通信情報を他の情報と照合してはならない。



KDDI Research

# 強化法の具体的内容② ―通信情報の利用等(3)―



■　**第25条（選別後通信情報の保存期間等）**

内閣総理大臣は、選別後通信情報が記録された文書(図画及び電磁的記録(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。)を含む。以下この項において同じ。)を作成し、又は取得したときは、当該選別後通信情報を得るための**自動選別が終了した日の属する年度の翌年度の初日から起算して二年を超えない範囲内**(次項の規定により保存期間を延長した選別後通信情報が記録された文書を作成し、又は取得した場合においては、当該延長後の保存期間の満了の日までの期間を超えない範囲内)**で、当該選別後通信情報の保存期間を設定しなければならない。**

2　内閣総理大臣は、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又は第二十三条第四項各号(第三十六条の規定により適用する場合を含む。)に掲げる場合(これらの場合に該当することとなることが合理的に予測される状況にある場合を含む。)は、**二年を超えない**範囲内において保存期間(この項の規定により延長した保存期間を含む。以下この条において同じ。)を延長することができる。

3　内閣総理大臣は、**保存期間の満了の日前であっても、選別後通信情報を保存する必要がなくなったと認めるときは、速やかに、当該保存を終了することを決定する**ものとする。この場合において、保存期間は、その決定がされた日に満了したものとみなす。

4　内閣総理大臣は、選別後通信情報の保存期間が満了したときは、できる限り速やかに、当該選別後通信情報を消去しなければならない。

■　**第26条（安全管理措置等）**

内閣総理大臣は、選別後通信情報の取扱いの業務を行わせる職員の範囲を定めることその他の取得通信情報の安全管理のために必要かつ適切なものとして内閣府令で定める措置を講じなければならない。

2　取得通信情報の取扱いに関する事務に従事する内閣府の職員(サイバー通信情報監理委員会の委員長、委員、専門委員及び事務局の職員を除く。)又はその職にあった者は、正当な理由がなく、当該事務に関して知り得た取得通信情報に関する秘密を漏らし、又は盗用してはならない。

■　**第27条（関係行政機関の分析への協力）**

内閣総理大臣は、自動選別又は選別後通信情報の分析(以下この項において「自動選別等」という。)を行うために必要があると認めるときは、防衛大臣その他の関係行政機関の長(当該行政機関が合議制の機関である場合にあっては、当該行政機関。以下この条において同じ。)に対し、自動選別等に関する専門的知識を有する職員による技術的援助、自動選別等の実施に用いる電子計算機の貸与その他の必要な協力を要請することができる。

2　前項の規定による要請を受けた関係行政機関の長は、その所掌事務に支障を生じない限度において、同項の協力を行うものとする。

3　内閣総理大臣は、第一項の協力を行う関係行政機関の長が当該協力を行う場合において必要があると認めるときは、当該関係行政機関に対し、選別後通信情報を提供することができる。

■　**第28条（外国の政府等に対する選別後通信情報の提供）**

内閣総理大臣は、特定被害防止目的の達成のために必要があると認めるときは、外国の政府又は国際機関であって、この法律の規定により内閣総理大臣が選別後通信情報を保護するために講ずることとされる措置に相当する措置を講じているものに対し、選別後通信情報を提供することができる。

# 強化法の具体的内容② ―通信情報の利用等(3)―



■ **第29条（提供用選別後情報の作成）**
内閣総理大臣は、選別後通信情報を加工して、協議会の構成員その他の者にこれを提供したとしてもその通信の当事者の通信に係る権利利益の保護に支障を生ずるおそれがないものとして内閣府令で定める基準を満たすもの（第三十六条及び第三十七条において「提供用選別後情報」という。）を作成することができる。

■ **第30条（サイバー通信情報監理委員会への通知）**
内閣総理大臣は、次に掲げる場合には、速やかに、その旨をサイバー通信情報監理委員会に通知しなければならない。
一　自動選別を行ったとき。
二　非識別化措置又は再識別化措置を講じたとき。
三　第二十五条第一項又は第二項（これらの規定を第三十六条の規定により適用する場合を含む。）の規定により保存期間を設定し、又は延長したとき。
四　第二十五条第四項（第三十六条の規定により適用する場合を含む。）の規定により選別後通信情報を消去したとき。
五　第二十七条第三項若しくは第二十八条（これらの規定を第三十六条の規定により適用する場合を含む。）の規定により選別後通信情報を提供し、又は第三十八条第一項若しくは第二項の規定により選別後通信情報を含む総合整理分析情報を提供したとき。

■ **第31条（通信情報保有機関における選別後通信情報の取扱い）**
内閣総理大臣は、次に掲げる場合には、速やかに、その旨をサイバー通信情報監理委員会に通知しなければならない。
一　自動選別を行ったとき。
二　非識別化措置又は再識別化措置を講じたとき。
三　第二十五条第一項又は第二項（これらの規定を第三十六条の規定により適用する場合を含む。）の規定により保存期間を設定し、又は延長したとき。
四　第二十五条第四項（第三十六条の規定により適用する場合を含む。）の規定により選別後通信情報を消去したとき。
五　第二十七条第三項若しくは第二十八条（これらの規定を第三十六条の規定により適用する場合を含む。）の規定により選別後通信情報を提供し、又は第三十八条第一項若しくは第二項の規定により選別後通信情報を含む総合整理分析情報を提供したとき。

# 強化法の具体的内容② ―通信情報の利用等(3)―



■ 第35条（自動的方法により取得通信情報を選別して記録する措置の実施）

内閣総理大臣は、**特定外内通信目的送信措置又は特定内外通信目的送信措置により取得通信情報を取得したとき**は、当該取得通信情報の中から次に掲げる要件を満たす**機械的情報であるもののみを選別して記録する措置**であって、**自動的方法で行われるものを講じなければならない**。

一 特定外内通信目的送信措置により取得した取得通信情報については、外内通信により送受信が行われたものであること。

二 特定内外通信目的送信措置により取得した取得通信情報については、内外通信により送受信が行われたものであること。

三 当該取得通信情報に係る対象不正行為に関係があると認めるに足りる状況のあるものであること。

2 前項第三号に掲げる要件を満たす取得通信情報を選別するための同項の措置は、次の各号のいずれかに該当する情報を選別の条件に用いて行うものでなければならない。この場合において、特定外内通信目的送信措置又は特定内外通信目的送信措置により取得した取得通信情報についての選別の条件は、それぞれ特定外内通信選別条件設定基準又は特定内外通信選別条件設定基準に従って定められたものでなければならない。

一 第三十二条第二項において準用する第十八条の規定による承認に係る特定外内通信の送信元となる特定の国外設備に係る情報又は第三十三条第二項において準用する第十八条の規定による承認に係る特定内外通信の送信先となる特定の国外設備に係る情報

二 第三十二条第二項において準用する第十八条の規定による承認に係る特定外内通信に含まれる特定の機械的情報又は第三十三条第二項において準用する第十八条の規定による承認に係る特定内外通信に含まれる特定の機械的情報

3 内閣総理大臣は、第一項の**措置が終了**したときは、直ちに、当該措置により得られた取得通信情報を除き、**当該措置の対象となった取得通信情報の全てを消去しなければならない**。

■ 第36条（取得通信情報の取扱いに関する規定の適用）

内閣総理大臣が特定外内通信目的送信措置又は特定内外通信目的送信措置により**取得通信情報を取得した場合**には、特定外内通信目的送信措置又は特定内外通信目的送信措置により取得した取得通信情報を外外通信目的送信措置により取得した取得通信情報と、前条第一項の措置を自動選別と、当該措置により得られた**取得通信情報**（当該取得通信情報を複製し、又は加工して作成された情報（提供用選別後情報となったものを除く。）を含む。）**を選別後通信情報とそれぞれみなして、第二十三条から第三十一条までの規定を適用**する。



KDDI Research

# 強化法の具体的内容②　―通信情報の利用等(3)―



■ **選別すべき情報に関する政府の見解**

● **日本国憲法第21条第2項：** 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

● **電気通信事業法第4条：** 電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。
※「取扱い中に係る通信」…発信者が通信を発した時点から受信者がその通信を受ける時点までの間をいう
→「例えば、企業内の情報通信システムのように発信者又は受信者の支配下にある電気通信設備の中での通信はこれになり得ない」
電気通信事業法における「通信の秘密の保護」の範囲
- 「『通信の秘密』には、**通信の内容のほか、通信当事者の住所・氏名・電話番号、発受信場所、通信の日時・時間・回数**なども含まれると解すべきである。」
（東京地方裁判所平成14年4月30日判決 等）
- 「**送信者情報**（個別の通信に結びつく送信者の氏名・住所等 ）は、**通信の内容そのものではないが、通信の秘密に含まれる**。」
（最高裁判所令和3年3月18日決定）

⇒「通信の秘密」の侵害にあたらない場合：
①当事者の有効な同意がある　②違法性阻却事由（法令行為に該当する、正当業務行為、正当防衛・緊急避難）に該当する

● **強化法第2条の2（通信の秘密の尊重）：**
この法律の適用に当たっては、第一条に規定する目的を達成するために**必要な最小限度において、この法律に定める規定に従って厳格にその権限を行使する**ものとし、**いやしくも通信の秘密その他日本国憲法の保障する国民の権利と自由を不当に制限するようなことがあってはならない**。

[引用]：内閣官房「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 通信情報の利用に関するテーマ別会合 第１回 事務局資料　資料5-2」(2024年　6月) file:///C:/Users/P448170/Downloads/siryou5-2.pdf
[参考]：内閣官房「『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』（第３回）議事要旨」（2024年　8月）https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai3/gijiyousi.pdf
[参考]：内閣官房「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 これまでの議論の整理」（2024年　8月）https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/giron_seiri/giron_seiri.pdf
[参考]：内閣府「重要電子計算機に対する特定不正行為による被害防止のための基本的な方針（案）に関するパブリックコメントの結果一覧」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo02.pdf

# 強化法の具体的内容② ―通信情報の利用等(3)―



## ■ 選別すべき情報に関する政府の見解

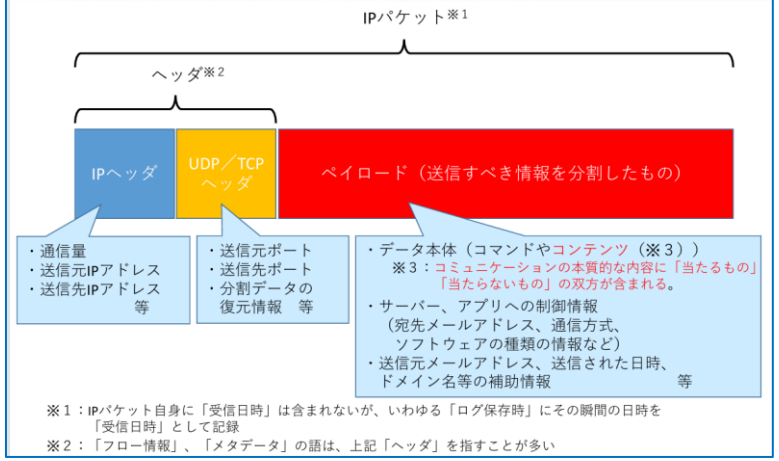
### 電子メールに係る通信情報内の「コミュニケーションの本質的内容」 35

黄色ハッチ部が「コミュニケーションの本質的内容」に相当。

| 番号 | 通信情報の内容 | 説明 | |
|---|---|---|---|
| 1 | From: hanako1@example.jp | 送信者メールアドレス | |
| 2 | To: taro2@cas.go.jp | 宛先メールアドレス | |
| 3 | Subject: 重要書類の送付について（至急） | 件名 | |
| 4 | Date: 2012/03/25 10:37 | 送信日時 | |
| 5 | Return-Path: <mail-system@example.jp> | 送信元メールアドレス（システムエラー時の返信先） | 受信側メールサーバーが追加する情報 等 |
| 6 | Received: from mail.cas.go.jp ([198.51.100.3]) by aa00bb01.cas.go.jp id <20120325103715817.****.****60@aa00bb01. cas.go.jp >; Sun, 25 Mar 2012 10:37:15 +0900 | 受信側組織内の伝送の記録 | |
| 7 | Authentication-Results: cas.go.jp; spf=pass reason=policy; sender-id=pass reason=policy | 受信側メールサーバでの迷惑メール判定結果 | |
| 8 | Received: from example.jp (mail. example.jp [203.0.113.1]) by cas.go.jp with ESMTP id D098B19 for <taro2@cas.go.jp>; Sun, 25 Mar 2012 10:37:15 +0900 (JST) | 送信側メールサーバから受信側メールサーバへの伝送の記録 | |
| 9 | Received: from hnkwinpc ([192.0.2.6]) by mail.example.jp with ESMTP id D098A05; Sun, 25 Mar 2012 10:37:03 +0900 (JST) | 送信側組織内の伝送の記録 | |
| 10 | Message-ID: <IMTw1fOIffff0KsJ@example.jp> | 送信側で付した番号 | |
| 11 | MIME-Version: 1.0<br>Content-Type: multipart/alternative ; boudary= "_Part_28873_0A61"<br>Content-Transfer-Encoding: 7bit | 本文の符号化の方式 | |
| 12 | 内閣官房サイバー準備室　御中<br><br>お世話になっております。<br>添付の至急ご確認をお願いします。<br><br>○○花子　拝 | 本文<br>（実際には符号化されて伝送。<br>左欄は復号化後の内容。以下同じ。） | |
| 13 | 重要書類.docx | 添付ファイル名<br>（技術的には本文の一部） | |
| 14 | これは重要書類です。直ちに保存して、なるべく多くの方に共有をお願いします。<br>よろしくお願いします。<br>84 a7 f3 9b 61 c1 08 99 27 1d 44 | 添付ファイルの内容<br>（技術的には本文の一部） | |

不正なコマンド（通常は表示されない）

### インターネットを流れるデータの構造 33




### コミュニケーションの本質的な内容ではない情報の例 34

| | | |
|---|---|---|
| コミュニケーションの本質的な内容に当たらない例 | ○ 送受信日時 | 2024.04.01 12:00:04 |
| | ○ ＩＰアドレス | 103.23.145.84 |
| | ○ 通信量 | 20kB |
| | ○ ポート番号 | 80 |
| | ○ コマンド | POST/ A3fe e3844A7D353007340284 HTTP/1.1 |
| | ○ プロトコル（通信方式） | HTTP / SSL / SMTP |
| | ○ ソフトウェアの種類 | Mozilla/4.0(…Trident/7.0;NET4.0c;…)… |
| | ○ ドメイン名 | cas.go.jp |
| | ○ メールアドレス | hogehoge@example.com（個人情報保護の観点から、個人を識別することができないように加工することが必要） |
| コミュニケーションの本質的な内容に当たる例 | × 電子メールの本文・件名 | |
| | × 添付ファイルの内容・名称 | |
| | × ＩＰ電話の通話内容 | |
| | × Ｗｅｂサイトに掲載されている文章、画像 | |



[出展]：内閣府「法律概要説明資料」https://www.cao.go.jp/cybersecurity/pdf/01sanko01.pdf

# 強化法の具体的内容② ―通信情報の利用等(3)―



- 誰が分析するのか？(i)

■ 第16条（通信情報の提供を受けた内閣総理大臣の措置）
前条の規定により**通信情報の提供を受けた内閣総理大臣**は、当該取得通信情報に係る第二十三条第四項第一号に規定する選別後当事者通信情報を用いて、当該当事者協定の協定当事者が使用する電子計算機の**サイバーセキュリティの確保に資する情報を得るための分析を行った上**で、当該協定当事者に係る個別分析情報又は利用者個別分析情報を当該協定当事者に**提供する**ものとする。
2 内閣総理大臣は、前項の分析においては、**当該個別分析情報又は利用者個別分析情報の提供に必要な範囲内**において、当該協定当事者が使用する電子計算機に対する**特定不正行為に関する分析を行うものとする**。

■ 第27条（関係行政機関の分析への協力）
**内閣総理大臣**は、**自動選別又は選別後通信情報の分析**(以下この項において「自動選別等」という。)**を行うために必要があると認める**ときは、**防衛大臣その他の関係行政機関の長**(当該行政機関が合議制の機関である場合にあっては、当該行政機関。以下この条において同じ。)**に対し、自動選別等に関する専門的知識を有する職員による技術的援助、自動選別等の実施に用いる電子計算機の貸与その他の必要な協力を要請することができる**。
2 前項の規定による要請を受けた関係行政機関の長は、その所掌事務に支障を生じない限度において、同項の協力を行うものとする。
3 内閣総理大臣は、第一項の協力を行う関係行政機関の長が当該協力を行う場合において必要があると認めるときは、当該関係行政機関に対し、選別後通信情報を提供することができる。

■ 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。

➡ここから、基本的には「内閣総理大臣」が分析を行うという名目になっている。

# 強化法の具体的内容② ―通信情報の利用等(3)―



- 誰が分析するのか？(ii)

■ 第72条（事務の委託）
**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。

➡以上条文から「内閣総理大臣」は**「その他行政機関」や「関係行政機関」へ分析に係る協力の要請**ができるとされている。

➡本条文に係る政令は成立していないものの、内閣府としては関係機関を次のように想定している：

「例えば、関係行政機関に対してそれぞれの所管業種に関する情報を求めることや、**独立行政法人情報処理推進機構(IPA)、国立研究開発法人情報通信研究機構（NICT)、一般社団法人 JPCERT コーディネーションセンター等のサイバーセキュリテ ィに関する高い専門性と情報収集能力を有する関係機関**に対して、当該関係機関が 検知･分析した脆弱性情報やネットワークの観測状況、その他当該機関の高い専門性 に基づく情報等の情報提供を求めることが想定される。」

[参考]：内閣府「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 」（2025年　12月) https://www.cao.go.jp/cybersecurity/pdf/kihonhoushin.pdf
[参考]：内閣府「重要電子計算機に対する特定不正行為による被害防止のための基本的な方針（案）に関するパブリックコメントの結果一覧」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo02.pdf

# 強化法の具体的内容②　―通信情報の利用等(3)―



➡政令案(2026年　1月)
・第2条:
法第72条第1項で定める法人は、**次の各号に掲げる委託を行う事務の区分**に応じ、当該豪に定める法人とする。
- 第1号:
**法第37条に規定する事務**　国立研究開発法人通信研究機構
＝**報告等情報、選別後通信情報、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の整理及び分析**を行う。

- 第2号:
**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
＝**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。

➡しかし、パブリックコメントの意見及び政府の回答からの懸念点として以下があげられている:

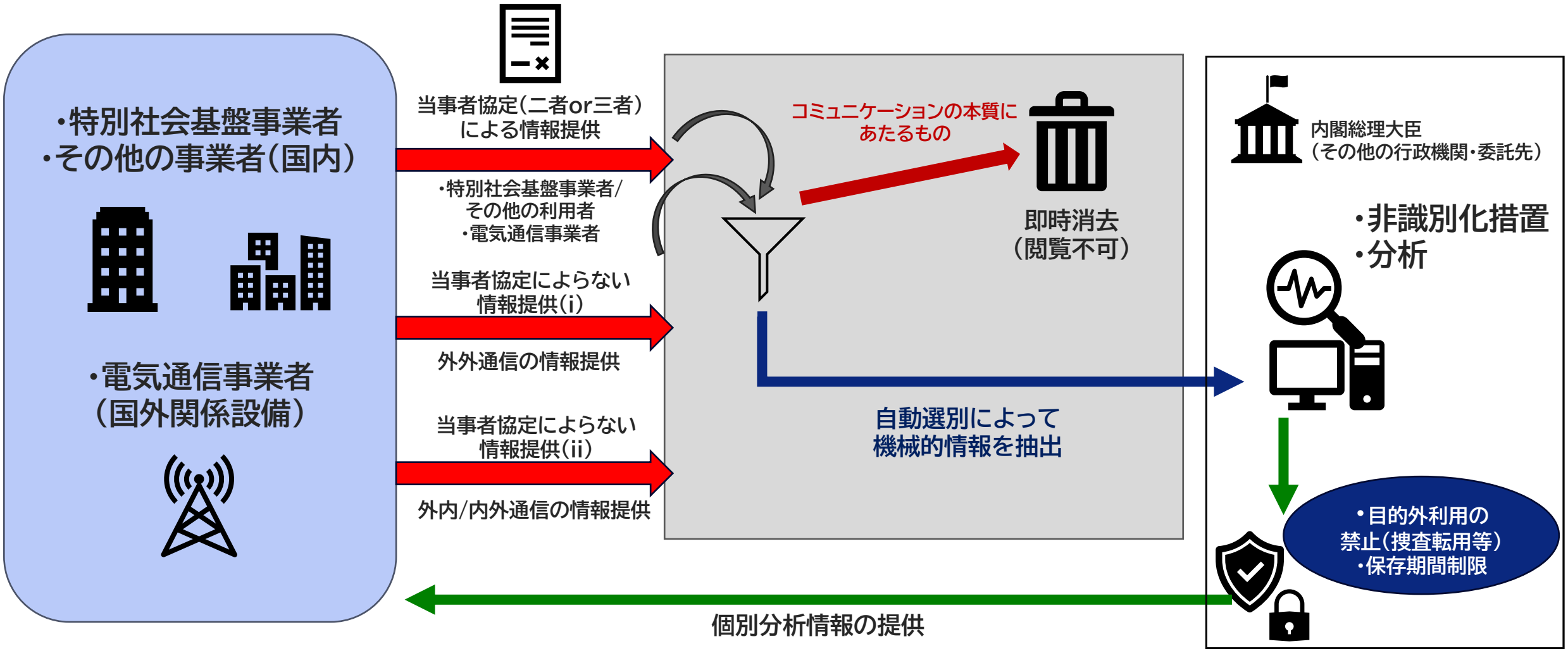
「**委託する相手**は「重要経済安保情報保護活用法」で規定する**適正評価(セキュリティクリアランス)を実施すべき**と考えます。」という意見に対し「**今後の制度運用の参考**にする」と回答。

[参考]:内閣府「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 」(2025年　12月) https://www.cao.go.jp/cybersecurity/pdf/kihonhoushin.pdf
[参考]:内閣府「重要電子計算機に対する特定不正行為による被害防止のための基本的な方針(案)に関するパブリックコメントの結果一覧」(2025年　12月) https://www.cao.go.jp/cybersecurity/pdf/04shiryo02.pdf
[参考] 内閣府政策統括官「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施行令案」(2026年　1月) https://public-comment.e-gov.go.jp/contents/about-public-comment/

# 強化法の具体的内容② ―通信情報の利用等（まとめ）―



- 国へ提供された通信情報のどの部分を分析するのか？



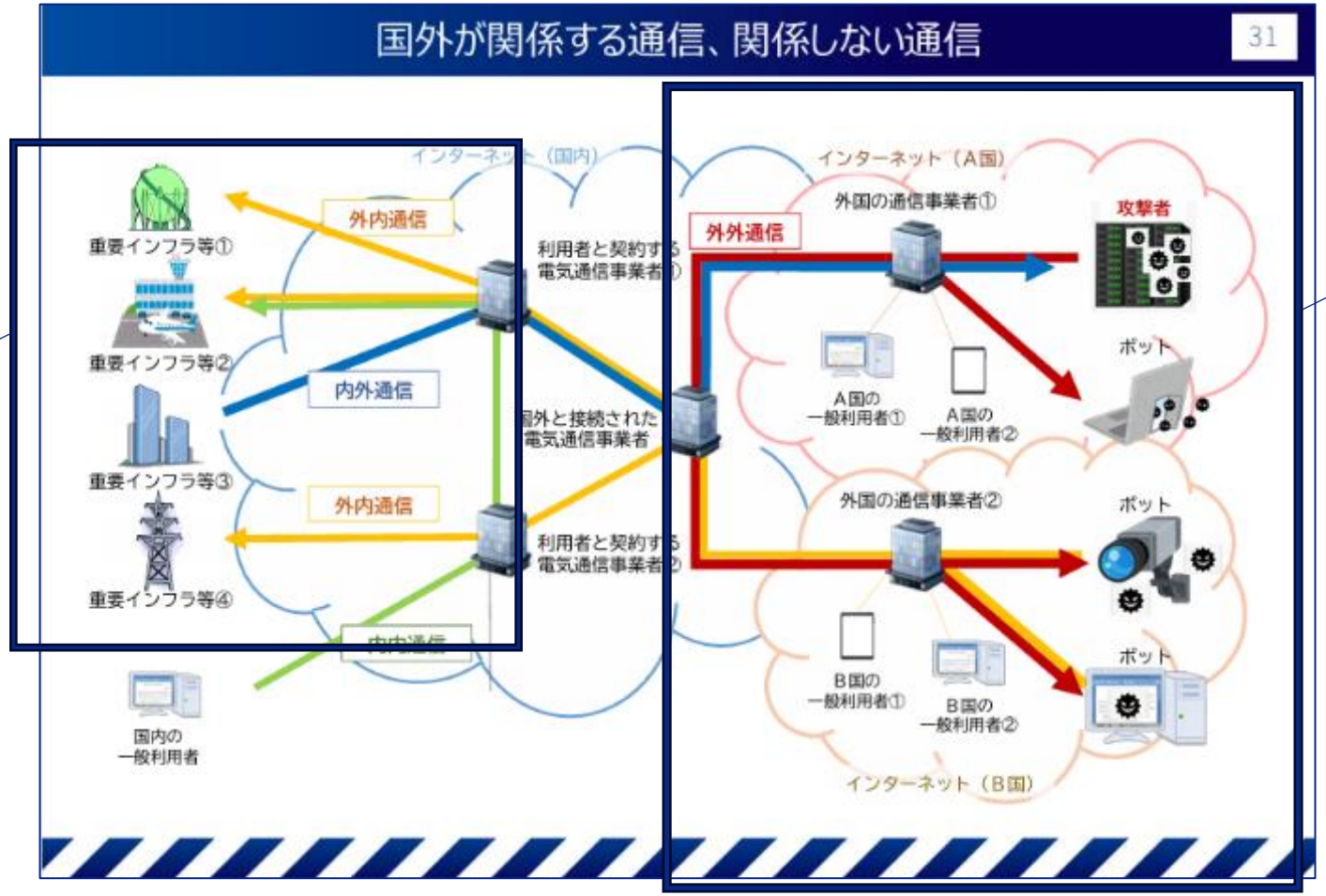

政府資料を元にKDDI総合研究所が作成

# 強化法の具体的内容② ―通信情報の利用等（参考）―



- 国へ提供する通信情報の内容解説

**特別社会基盤事業者を通信の当事者とする通信情報**
（第11条第1項）




この枠内黄色線：
電気通信を提供者である**電気通信事業者が持つ通信情報**（第11条第3項、第12条第2項）

この枠内赤線：
第17条

[出展]：国家サイバー統括室「サイバー対処能力強化法及び同整備法について」（2025年　9月）https://www.cao.go.jp/cybersecurity/pdf/setsumei.pdf

# 強化法の具体的内容③
## ―情報共有―

# 強化法の具体的内容③ ―情報共有(1)―



## ● 国へ提供された通信情報の分析後はどうなるのか？(行政機関等への提供)

■ **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**第三十一条第二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　第一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(電気通信事業法第二条第七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。

## ● 国へ提供された通信情報の分析後はどうなるのか？(外国への提供)

■ **第39条（外国の政府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に関する事務を遂行するために必要があると認めるときは、外国の政府又は国際機関であって、この法律の規定により国の行政機関が提供用総合整理分析情報(総合整理分析情報であって選別後通信情報を含まないものをいう。以下同じ。)を保護するために講ずることとされる措置に相当する措置を講じているものに対し、当該提供用総合整理分析情報を提供することができる。



KDDI Research

# 強化法の具体的内容③ ―情報共有(2)―



● 国へ提供された通信情報の分析後はどうなるのか？(基幹インフラ事業者に対する情報提供)

■ 第40条 (特別社会基盤事業者に対する情報提供)
第三十八条第一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**。

● 国へ提供された通信情報の分析後はどうなるのか？(電子計算機を使用する者に対する情報提供)

■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。

# 強化法の具体的内容③ ―情報共有(3)―



## ● 国へ提供された通信情報の分析後はどうなるのか？(供給者に対する情報提供)

■ 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ぜい弱性(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。以下この条及び第四十五条第二項において同じ。)**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。

➡**電子計算機等の生産者、輸入者、販売者及び提供者**の意味をしている「供給者」に関係する条文においては、内閣総理大臣又は供給者を所管する大臣からの**情報提供のみならず、被害を防止するために必要な措置を講ずるよう要請がなされ得る。**

➡しかし、「どの省庁」が「どういった供給者」を所管・想定しているのかという明確な基準等の具体的な指定は現時点で明らかではない。

[参考]：国家サイバー統括室「サイバー対処能力強化法及び同整備法について」（2025年　9月）https://www.cao.go.jp/cybersecurity/pdf/setsumei.pdf

# 強化法の具体的内容③ ―情報共有(3)―



- **想定:国家サイバー統括室「サイバーインフラ事業者に求められる役割等の検討会」(令和6年(2024年) 9月~)**

➡この検討会において、サイバーインフラ事業者[1]と顧客に求められる責務と、責務を果たすための要求事項(役割別の具体的な取組の在り方)を含む**ガイドライン案の策定**が議論されていた。

[1]サイバーセキュリティ基本法第7条において、サイバー関連事業者(インターネットその他の高度情報通信ネットワ ークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者)等の責務が規定されている事業者のうち、政府機 関等及び重要インフラ事業者を始め広く社会で活用される情報・通信システム、ソフトウェア製品及びICTサービスを開発し提供する事業者並びに当該情報・通信システム等のソフトウェアのライフサイクルとサプライチェーンに関わる事業者をいう。

- **経済産業省「サイバーインフラ事業者に求められる役割等に関するガイドライン(案)」(令和7年 10月)**

**➡本ガイドライン案において経済産業省は右図のような事業に携わる供給者を想定していることから、例えば顧客(=重要インフラ事業者や政府機関)にソフトウェア製品供給しているとされる事業者が強化法第42条に関係すると想定される。**

表 3 サイバーインフラ事業者及びステークホルダーの分類

| 分類 | 名称 | 説明 |
|---|---|---|
| サイバーインフラ事業者 | 開発者 | ソフトウェア製品、ソフトウェアサービス、組み込みソフトウェア、あるいはこれらのソフトウェアで構成されるシステム・サービスの設計を含めた開発又はインテグレーションに従事する事業者・人員<br>ソフトウェア開発ベンダー、ソフトウェアサービスプロバイダ、機器開発ベンダー、ソフトウェアやシステムの開発請負事業者、ソフトウェアコンポーネント開発事業者、インフラ事業者、自社開発ソフトウェアの開発部門などにおいて、ソフトウェアの開発又はインテグレーションを行う事業者等が対象となる。 |
| | 供給者 | 顧客にソフトウェア製品、ソフトウェアサービス、組み込みソフトウェア(ハードウェア製品を含む)、あるいはこれらのソフトウェアで構成されるシステム・サービスを提供する事業者・人員[9]<br>ソフトウェア製品やソフトウェアを含む機器の販売会社、ソフトウェアサービスプロバイダ、システムの開発運用請負事業者、インフラ事業者、ソフトウェア開発ベンダーなどにおいて、ソフトウェアやシステム・サービスを提供する事業者等が対象となる。 |
| | 運用者 | 顧客に対して主にシステム・サービスの運用を支援する役務を提供する事業者・人員[10] |
| ステークホルダー | 顧客 | 政府機関等及び重要インフラ事業者を始め、ソフトウェアの利用主体となる事業者等 |
| | その他関係機関 | サイバーレジリエンス向上の支援を担う組織 |

(3) システムを対象とした一般的な役割分担の想定

本ガイドライン(案)が対象とするサイバーインフラ事業者が扱うソフトウェアの資産について、ソフトウェアで構成するシステムの開発・契約形態・利用形態を踏まえた関係を図 1 に示す。ここでは、サイバーインフラ事業者を、システムの開発・契約・利用の観点から、以下の 2 つの役割を想定している。

[9] 供給者内に、開発者・運用者が含まれるケースもある。また、サイバーインフラ事業者に販売会社が含まれるケースでは、供給者に準じた責務が求められる。
[10] ソフトウェアの利用主体である顧客がソフトウェアを運用することが一般的であるが、システム・サービス又はこれらを構成するソフトウェアの運用には専門的な知識や技能が必要な場合も多い。ここでは、顧客との契約により、サイバーインフラ事業者がソフトウェアの運用(又はその一部)を支援する場合を想定する。

6

[参考]:経済産業省「サイバーインフラ事業者に求められる役割等に関する ガイドライン(案)」(2025年 10月)https://www.meti.go.jp/press/2025/10/20251030002/20251030002-1.pdf
[参考]:経済産業省・NISC「サイバーインフラ事業者に求められる役割等の検討の方向性」(2024年 9月)https://www.cyber.go.jp/pdf/council/cs/ciip/yakuwari/kaigi01/01shiryou04.pdf



KDDI Research

# 強化法の具体的内容③ ―情報共有（4）―



## ● 協議会の設置

■　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、第一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。第二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。

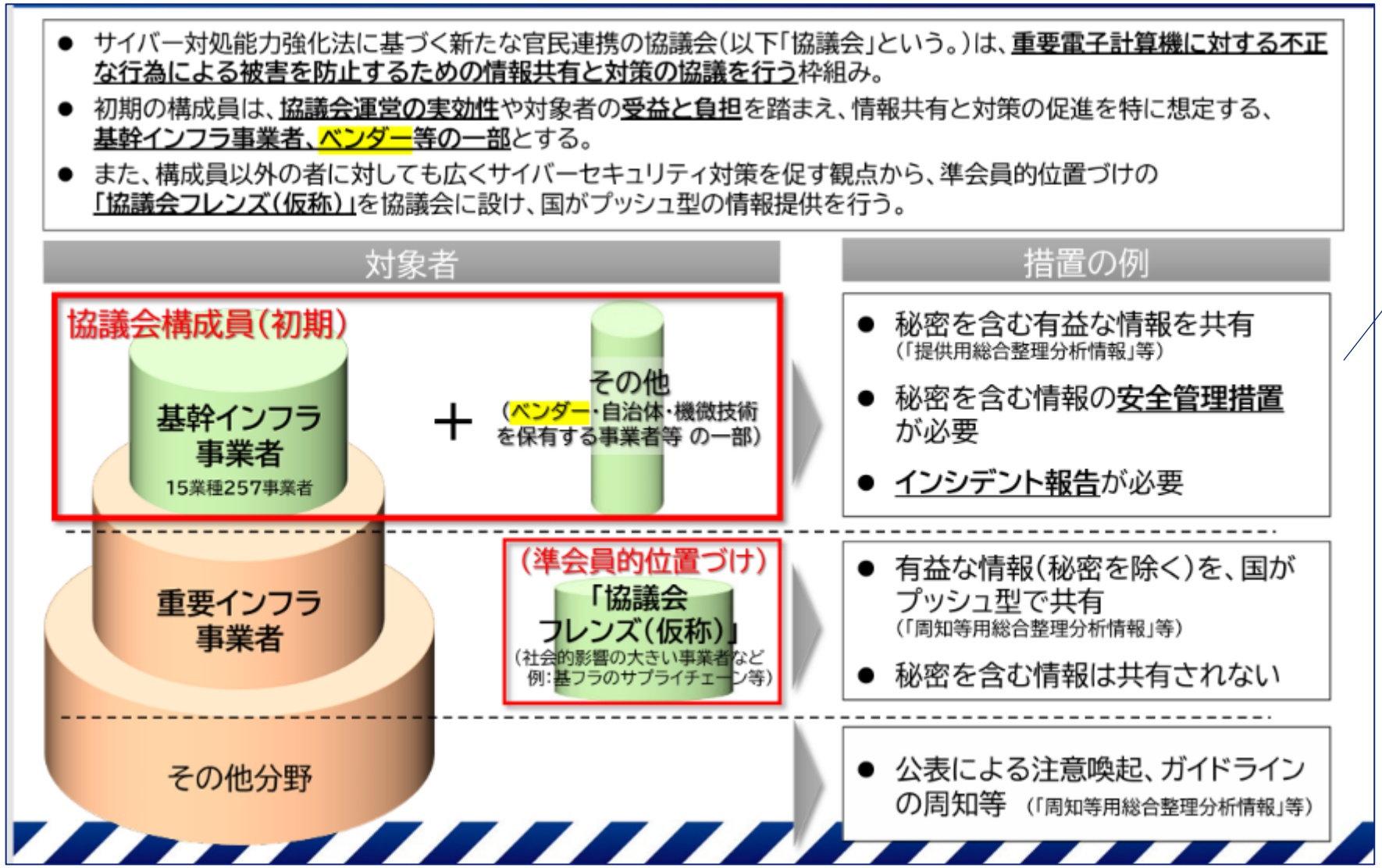
6　構成員は、前項前段の規定による協議会の求めに応じて資料を提出するときは、当該資料の取扱いに関し意見を付すことができるものとし、意見を付した構成員以外の構成員は、その意見に配慮しなければならない。ただし、重要電子計算機に対する特定不正行為による被害を防止するため特に必要があると認めるときは、この限りでない。

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。

# 強化法の具体的内容③ ―情報共有(4)―






[出展]：国家サイバー統括室「サイバー対処能力強化法（官民連携の）施行に向けた考え方の案」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo05.pdf

協議会で共有される情報の中には、例えば重要経済安保情報についても構成員が取り扱えるようにする可能性を示唆する政府の意見もあった。

そのため、2025年12月におけるパブコメでの意見では、協議会に参加する者も含めたクリアランス制度の実施が必要になるのではないかという意見も散見された。

[参考]：内閣府「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 」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/kihonhoushin.pdf
[参考]：内閣府「重要電子計算機に対する特定不正行為による被害防止のための基本的な方針（案）に関するパブリックコメントの結果一覧」（2025年　12月）https://www.cao.go.jp/cybersecurity/pdf/04shiryo02.pdf

# 参考資料

# 特定重要設備に関する主務省令一覧(1)



■ **内閣府政策統括官「経済安全保障推進法の安定社会基盤役務の安定的な提供の確保に関する制度の解説 」**(2024年 10月)

「主務省令」次の11の省令を指す。

- 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 律に基づく特定社会基盤事業者の指定等に関する内閣府令(令和5年内閣 府令第61号)
- 内閣府・法務省関係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に基づく特定社会基盤事業者の指定等に関する命令 (令和5年内閣府・法務省令第2号)
- 内閣府・法務省・財務省関係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に基づく特定社会基盤事業者の指定等に関 する命令(令和5年内閣府・法務省・財務省令第1号)
- 内閣府・財務省関係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に基づく特定社会基盤事業者の指定等に関する命令 (令和5年内閣府・財務省令第6号)
- 内閣府・財務省・農林水産省関係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に基づく特定社会基盤事業者の指定等 に関する命令(令和5年内閣府・財務省・農林水産省令第2号)

[参考] 内閣府政策統括官「経済安全保障推進法の安定社会基盤役務の安定的な提供の確保に関する制度の解説」(2024年 10月)https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_kaisetsu.pdf

# 特定重要設備に関する主務省令一覧(2)



- 内閣府・厚生労働省関係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に基づく特定社会基盤事業者の指定等に関する命令(令和5年内閣府・厚生労働省令第6号)
- 内閣府・農林水産省関係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に基づく特定社会基盤事業者の指定等に関する命令(令和5年内閣府・農林水産省令第4号)
- 総務省関係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に基づく特定社会基盤事業者等に関する省令(令和5年総務省令第64号)
- 厚生労働省関係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に基づく特定社会基盤事業者等に関する省令(令和5年厚生労働省令第103号)
- 経済産業省関係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に基づく特定社会基盤事業者等に関する省令(令和5年経済産業省令第41号)
- 国土交通省関係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に基づく特定社会基盤事業者等に関する省令(令和5年国土交通省令第62号)

[参考] 内閣府政策統括官「経済安全保障推進法の安定社会基盤役務の安定的な提供の確保に関する制度の解説」(2024年 10月)https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/doc/infra_kaisetsu.pdf



KDDI Research

# 特定重要設備に関する届出先の一覧



## 各事業所管省庁の各種届出・報告等の受付先及び相談窓口

| 事業 | 省庁名 | 担当課室名 |
|---|---|---|
| 電気 | 経済産業省（各種届出等の受付先及び相談窓口） | 資源エネルギー庁 電力・ガス事業部 電力基盤整備課<br>資源エネルギー庁 電力・ガス事業部 電力産業・市場室 |
| ガス | | 資源エネルギー庁 電力・ガス事業部 ガス市場整備室 |
| 石油 | | 資源エネルギー庁 資源・燃料部 燃料供給基盤整備課<br>資源エネルギー庁 資源・燃料部 燃料流通政策室 |
| 水道 | 国土交通省（各種届出等の受付先及び相談窓口） | 水管理・国土保全局水道事業課水道計画指導室 |
| 鉄道 | | 鉄道局総務課企画室 |
| 貨物自動車運送 | | 物流・自動車局貨物流通事業課 |
| 外航貨物 | | 海事局外航課 |
| 航空 | | 航空局航空ネットワーク部航空事業課 |
| 空港 | | 航空局航空ネットワーク部航空ネットワーク企画課<br>航空局航空ネットワーク部首都圏航空課<br>航空局航空ネットワーク部近畿圏・中部圏空港課 |
| 港湾運送<br>※相談窓口のみ | 国土交通省（相談窓口） | 港湾局港湾経済課 |
| 電気通信<br>放送<br>郵便 | 総務省（各種届出等の受付先）<br>総務省（相談窓口） | サイバーセキュリティ統括官室 |
| 金融 | 金融庁（各種届出等の受付先）<br>金融庁（相談窓口）<br>農林水産省（各種届出等の受付先）<br>農林水産省（相談窓口） | 金融庁総合政策局リスク分析総括課経済安全保障室<br>農林水産省経営局金融調整課 |
| クレジットカード | 経済産業省（各種届出等の受付先及び相談窓口） | 商務・サービスグループ商取引・消費経済政策課 |

■ 経済安全保障推進法の下、基幹インフラ事業者が届出を提出する特定重要設備の届出先一覧及び現時点での届出報告件数

### 2024年度 事前届出件数及び事後報告件数

- ✓ 2024年度※1の事前届出（導入等計画書及び緊急導入等届出書。重要な変更含む。）件数は972件、事後報告件数は195件。
- ✓ 各省庁における事前届出件数、事後報告件数は以下のとおり。

| 届出対象 | 2024年度 | | | |
|---|---|---|---|---|
| | 事前届出件数※2 | | | 事後報告件数 |
| | 導入 | 重要維持管理等 | 合計 | |
| 経済産業省（資源エネルギー庁含む） | 45 | 120 | 165 | 90 |
| 国土交通省 | 11 | 82 | 93 | 3 |
| 総務省 | 103 | 225 | 328 | 40 |
| 金融庁・農林水産省※3 | 33 | 353 | 386 | 62 |
| 合計 | 192 | 780 | 972 | 195 |

※1 2024年度は、制度開始日である2024年5月17日から2025年3月31日までの期間を集計している。
※2 事前届出件数は、導入等計画書等の届出件数の他、導入等計画書の変更の案の届出件数（重要な変更の届出件数）も含まれる。
※3 農林水産省所管の金融分野を合算して計上。

［引用］内閣府「基幹インフラ役務の安定的な提供の確保に関する制度」https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/infra.html

KDDI Research

# 夢中を、みんなの感動に。


KDDI Research