資料５

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

令和７年１２月
内閣府政策統括官（サイバー安全保障担当）

強化法の概要 【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）

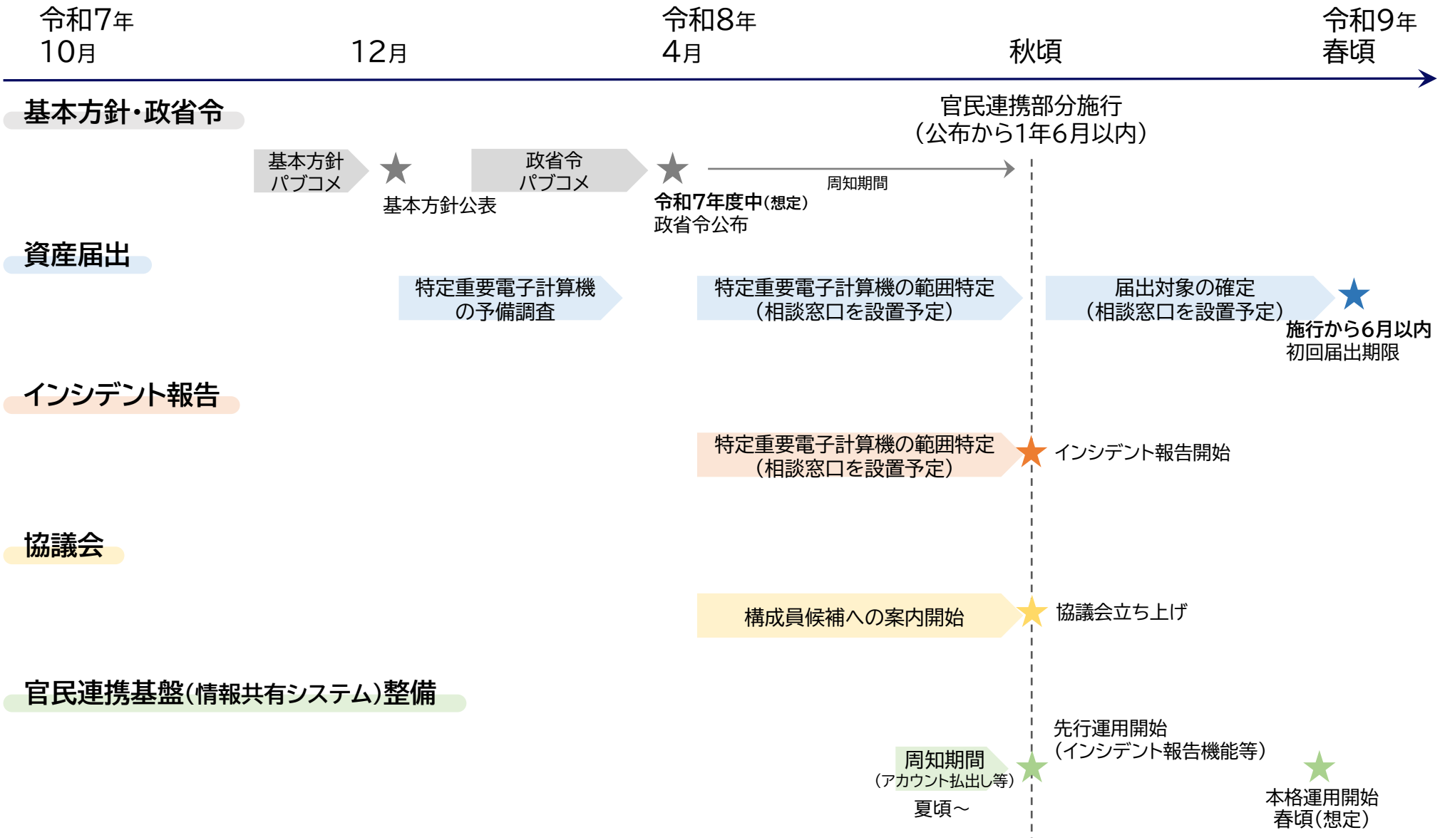
- 内閣総理大臣は、サイバー攻撃による被害の防止のため、関係行政機関の長により構成される「情報共有及び対策に関する協議会」を設置
- 協議会には、基幹インフラ事業者、電子計算機等のベンダー等をその同意を得て構成員として加える
- 構成員に対しては、守秘義務を伴う被害防止に関する情報を共有するとともに、必要な情報共有を求めることが可能

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

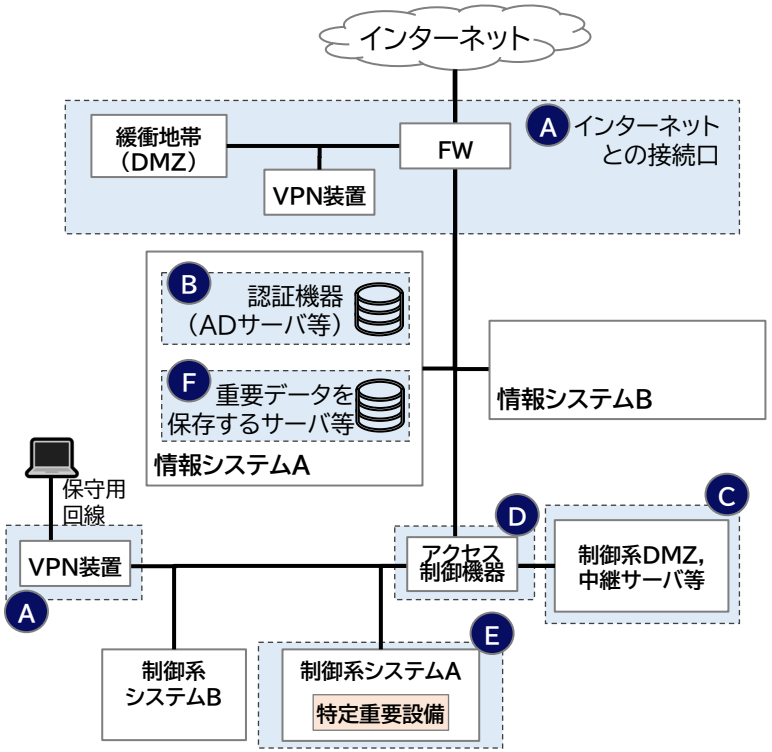
（※）電子計算機やそれに組み込まれるプログラムの供給を行う事業を所管する大臣

施行に向けたタイムライン



届出対象機器の考え方

- 特定重要電子計算機としては、特別社会基盤事業者の安定的な役務提供の確保や近年の脆弱性の悪用状況、多層防御の観点も踏まえ、アタックサーフェスの機器に加えて、以下のような類型の機器も対象とすべきではないか。
- 他方、業態毎にシステム構成は異なっており、具体的な届出対象は、業態別、個者別に今後具体的に検討する。



※1　ある類型に該当する機器が存在しない場合には、届出不要。
※2　一の機器が複数の類型に該当する場合は、
　　当該一の機器についてのみ届出を求める。

アタックサーフェス

A インターネットとの接続口（アタックサーフェス）の機器等

◆ **対象機器**
グローバルIPアドレスが割り当てられている機器

◆ **具体例**
✓ FW, VPN装置等

＋

多層防御の観点から重要と考えられる類型（考え方）

B 特定社会基盤役務の提供に係るシステムの認証を提供する機器等

C 「特定重要設備」を含むセグメントのDMZ等

D 「特定重要設備」を含むセグメントへのアクセスを制御する機器

E 特定重要設備又は当該特定重要設備と同一セグメントの機器

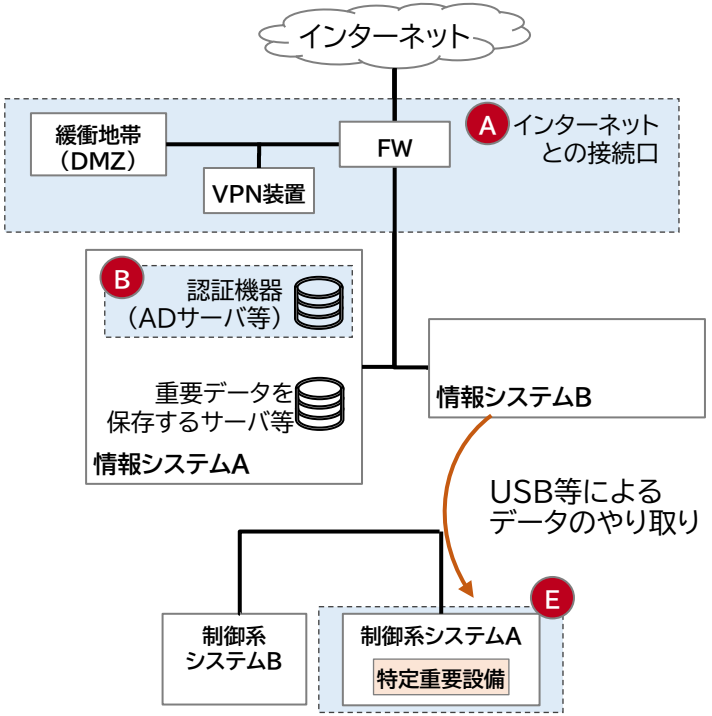
F A～Eの特定重要電子計算機に係る重要データ（認証情報等）を保存している機器

システム構成に応じた取扱い

- 特別社会基盤事業者のシステム構成は業態毎に大きく異なっており、例えばシステムが物理的分離している場合やクラウドサービスを利用している場合には、以下のような取扱いが考えられる。

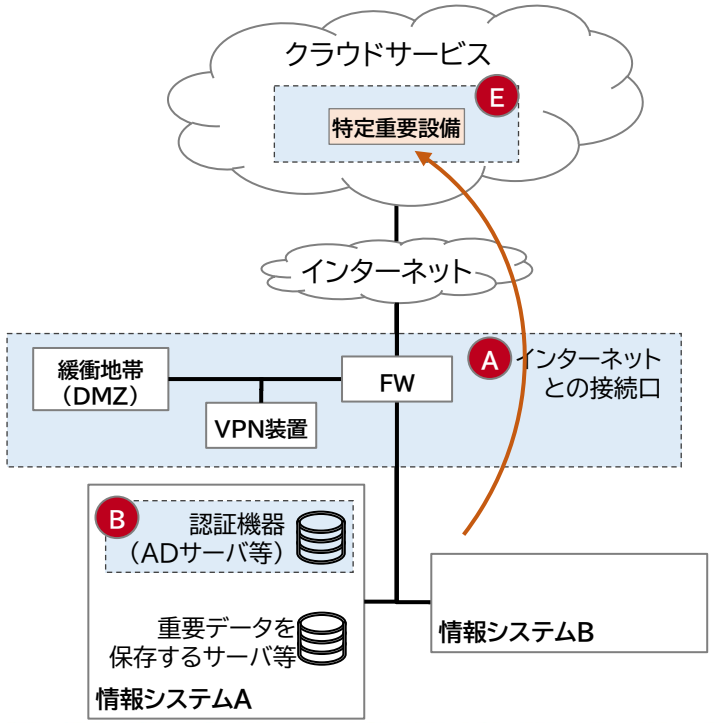
特定重要設備がインターネットと**物理的分離**している場合

可搬型記憶媒体等を用いて、特定重要設備を含む領域と定期的にデータのやり取りが行われる領域については、**類型A（アタックサーフェス）、類型B（認証機器）、類型E（特定重要設備等）の届出を求める。**



特定重要設備が**クラウドサービス**を利用している場合

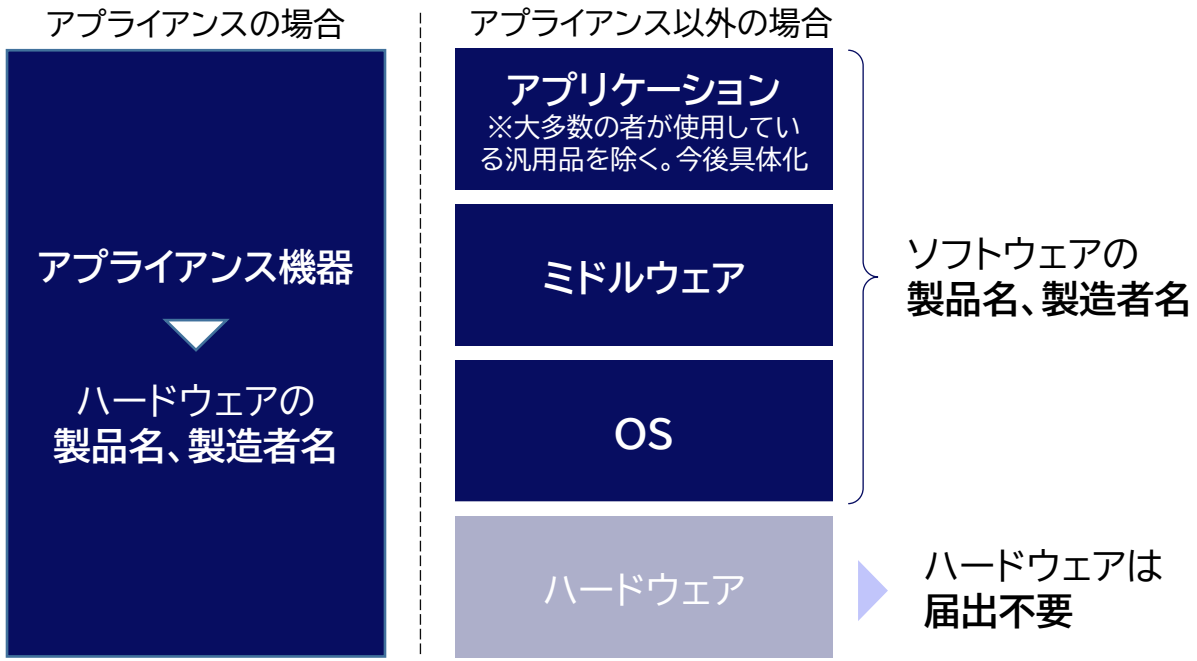
特定重要設備の機能の全部又は大部分がクラウドサービスを利用している場合、特定重要設備の機能に必要なデータのやり取りを行う領域については、**類型A（アタックサーフェス）、類型B（認証機器）、類型E（特定重要設備等）の届出を求める。**



届出粒度

届出の粒度

- 脆弱性情報の提供の観点から、ソフトウェア（アプリケーション、ミドルウェア及びOS）の製品名、製造者名の報告を求め、ハードウェア名等については報告を求めないこととする。
- 他方、アプライアンス※については、そのハードウェアの製品名、製造者名の届出を求める。
  ※特定用途のプログラムが組み込まれた機器であって、通常当該プログラム以外のプログラムを組み込むことができないもの。



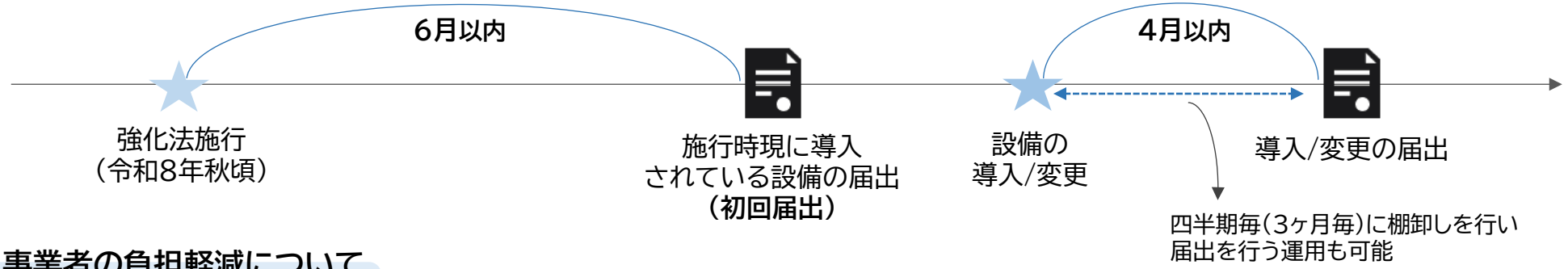
クラウドサービスを利用している場合

- クラウドサービスを利用している場合、当該クラウドサービスの**サービス名、サービス提供者名**を届出。
  （特定重要設備又は構成設備に該当する場合は、**製品名、製造者名**を届出）
- 特定重要設備がクラウドサービスを利用して実装されている場合の考え方は前ページ参照。

届出に係る事項

届出期限

- **導入から4月以内に届出**を求める。ただし、施行の際現に導入されている特定重要電子計算機及び施行の際現に導入されている特定重要設備と一体として運用する特定重要電子計算機については、**施行から6月以内に届出**を求める。
- 届出事項の変更があった場合には、**変更の日から4月以内に届出**を求める。
  （運用上、四半期に一度棚卸しを行い、前回届出から変更があった場合に、その内容について届出を行う運用も可能とする想定）



事業者の負担軽減について

- 基幹インフラ事業者以外の者が維持管理している特定重要電子計算機については、当該維持管理を行っている者（ベンダー等）から直接届出を行うことを可能とできないか検討中。
- 特定重要電子計算機の類型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を届け出て、政府による外部スキャンを行う方法も可能とするよう、詳細な運用を検討中。
- 特定重要設備又は構成設備について、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。

届出の例外

- 専ら一の基幹インフラ事業者の事業の用に供するもの（**専用設計品**）については、届出義務の対象外とする。
- **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**についても、届出義務の対象外とするよう扱いを検討。

報告対象の事案

- 報告対象の事案(「おそれ」部分)については、以下のような事案を対象とし、さらに具体的な事象については MITRE ATT&CK等のフレームワークも参考に今後整備予定のガイドラインに記載。
- 特定重要設備以外の機器については、**特定不正行為の痕跡を認知した場合**にも報告を求める。
- 類型Eの機器(特定重要設備等)については、機能停止・低下に至る可能性が特に大きいことから、**特定不正行為の痕跡に加え、特定不正行為に繋がる事象**についても報告を求める。

特定侵害事象

特定不正行為

① 不正指令電磁的記録(マルウェア)が実行可能な状態に置かれた場合

② 不正アクセス行為(不正アクセス禁止法第2条第4項に定める不正アクセス行為をいう。)が行われた場合

③ 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業務妨害が行われた場合

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

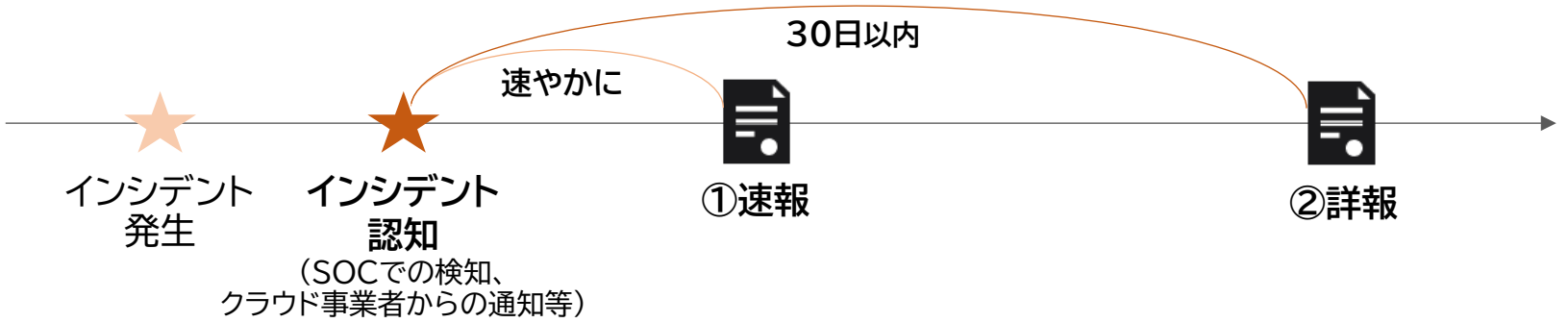
特定侵害事象の原因となり得る事象

類型E以外の機器	類型E(特定重要設備等)の機器
✓ **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)	✓ **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した場合** ①’マルウェアを受信した場合 ②’不正アクセス行為を行う通信を発見した場合(アクセス制御機能の制限を免れるような情報等が入力された場合、認証情報が窃取された場合等) ③’虚偽の情報、不正な指令を受信した場合

報告期限・報告事項

報告期限

- インシデントの認知後① **速やかに速報**、② **30日以内に詳報**の提出を求める。
  いずれも、**報告時点で把握している事項についてのみ届出**を求める。
- SaaSを利用している場合、PaaSを利用している場合(ミドルウェア、OSに係るものに限る。)については、
  クラウドサービス事業者から通知があった時点で「認知」とみなす。
  (PaaS(アプリケーションに係るもの), IaaSの場合には、オンプレ設備と同様に扱う。)

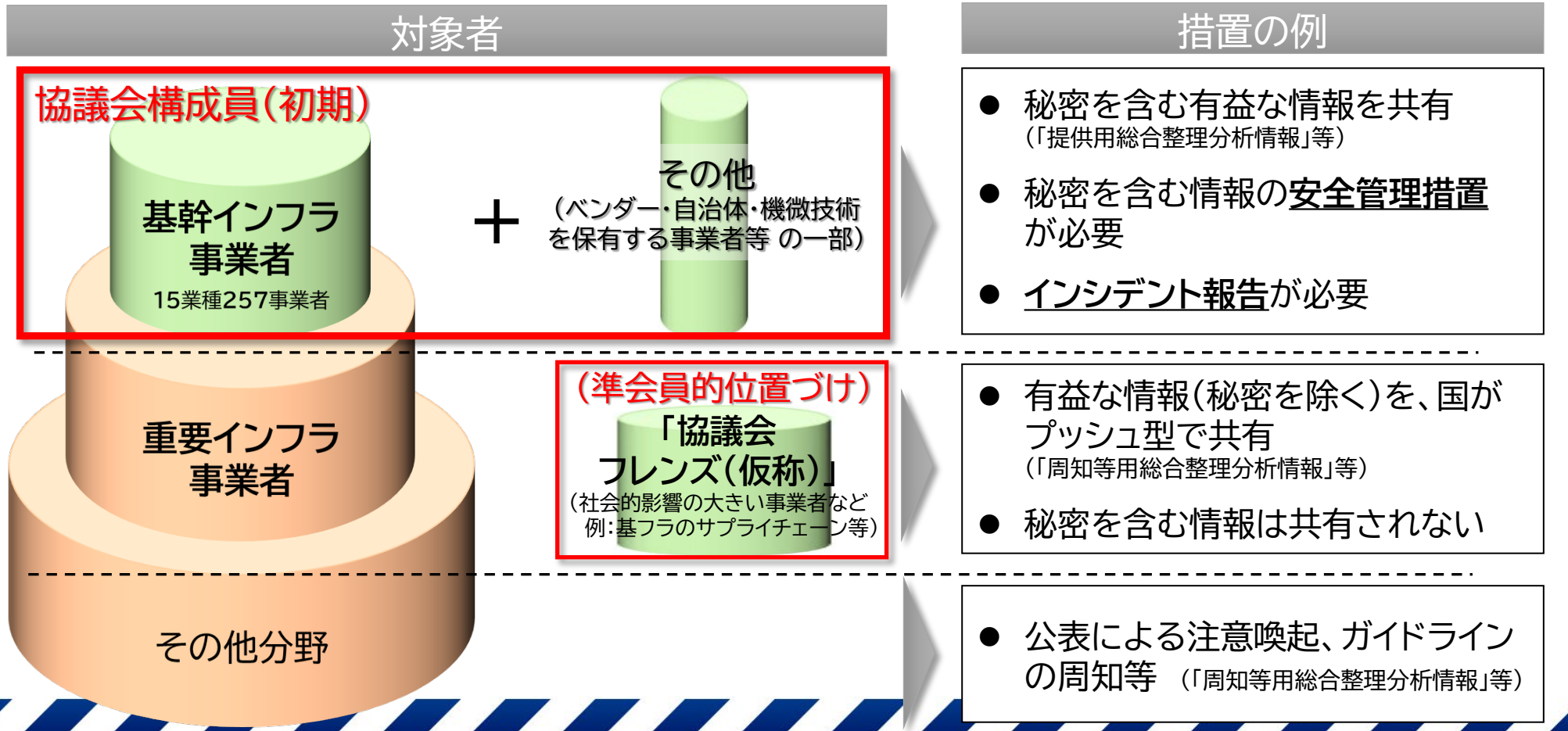


報告事項

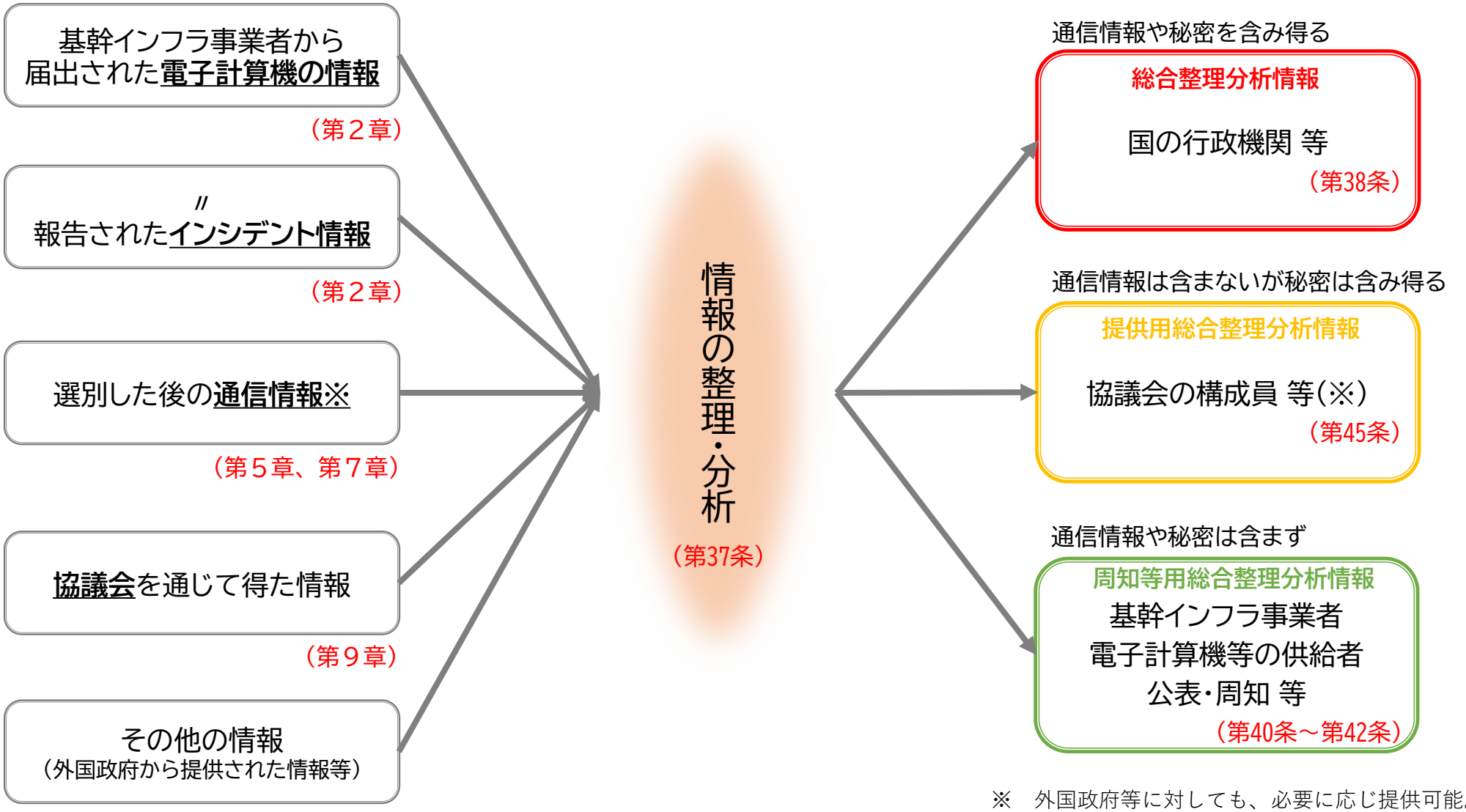
- 発生した事象の概要(業務、システムへの影響等)、攻撃技術情報等について報告を求める。
- このうち、攻撃技術情報については、サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ
  (令和7年5月28日関係省庁申合せ)で定める**DDoS攻撃事案共通様式**及び**ランサムウェア事案共通様式**における
  攻撃技術情報欄記載の事項について報告を求めることとする。
  (DDoS攻撃事案及びランサムウェア事案以外の事案については、今後詳細を検討。)

想定される協議会構成員のイメージ（初期）

- サイバー対処能力強化法に基づく新たな官民連携の協議会（以下「協議会」という。）は、**重要電子計算機に対する不正な行為による被害を防止するための情報共有と対策の協議を行う**枠組み。
- 初期の構成員は、**協議会運営の実効性**や対象者の**受益と負担**を踏まえ、情報共有と対策の促進を特に想定する、**基幹インフラ事業者、ベンダー等の一部**とする。
- また、構成員以外の者に対しても広くサイバーセキュリティ対策を促す観点から、準会員的位置づけの**「協議会フレンズ（仮称）」**を協議会に設け、国がプッシュ型の情報提供を行う。



強化法に基づく情報の整理・分析と情報提供の全体像

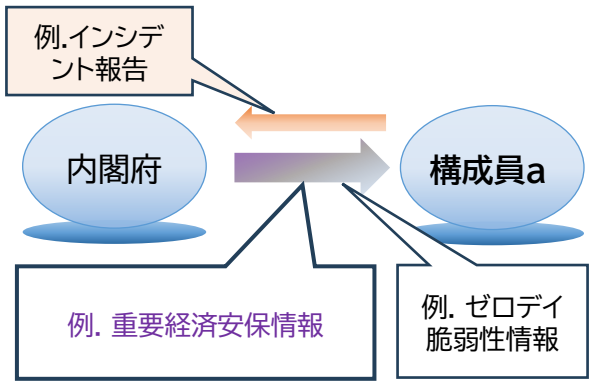


※　外国政府等に対しても、必要に応じ提供可能。
（第28条、第39条）

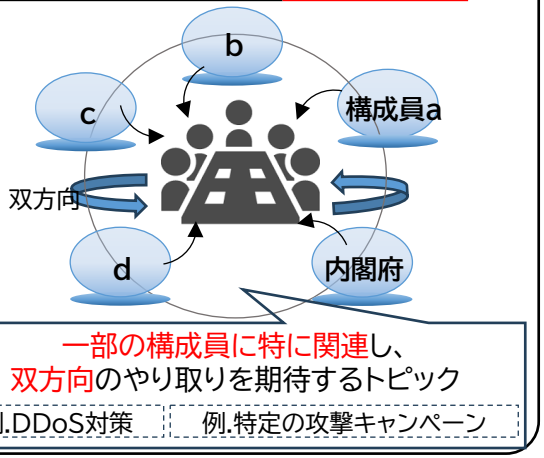
運営形態のイメージ

- 構成員への情報共有は、機微度や内容、対象者等に応じて、主に下記の5つの枠組みを活用する。

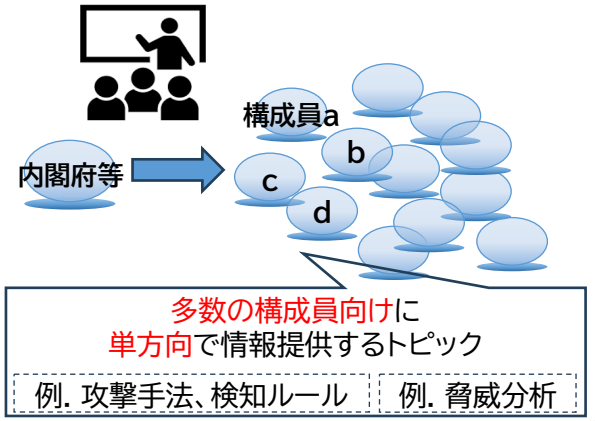
⑴1対1での共有



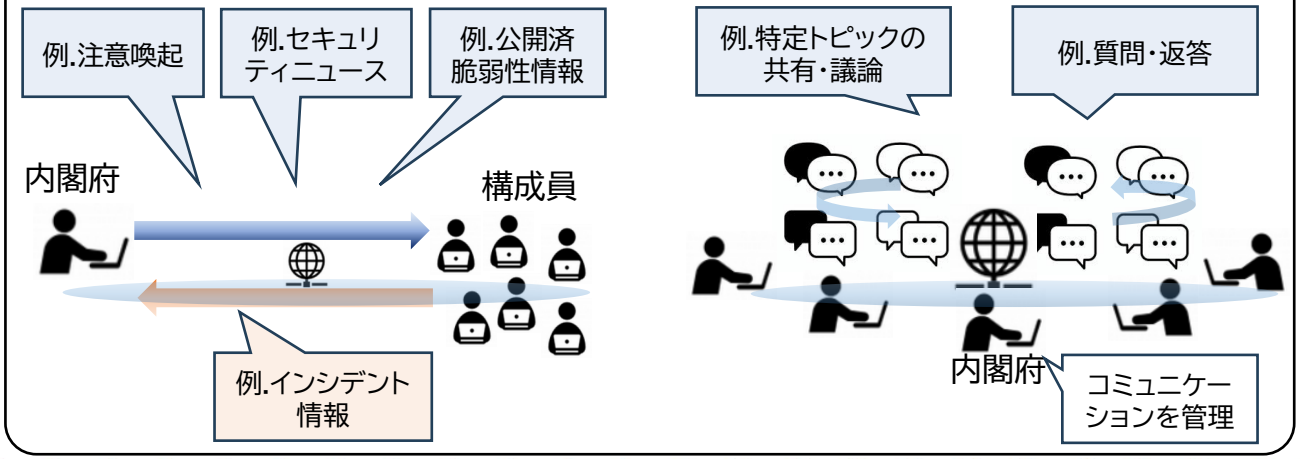
⑵ワーキンググループ形式で限定メンバーとの共有と議論



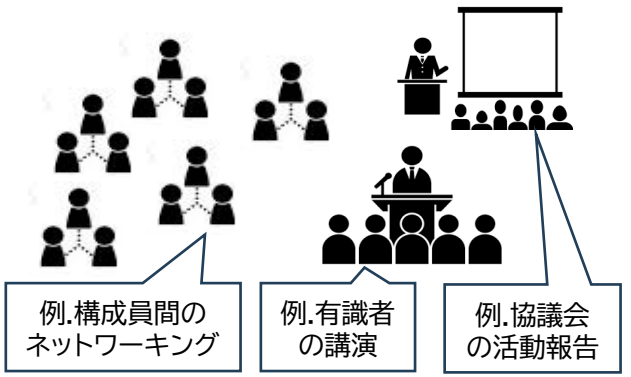
⑶セミナー形式で構成員横断的に共有



⑷新システム上での共有・コミュニケーション



⑸活動報告・交流・講演



今後のスケジュール

- 今後、具体的な運営手続等を検討し、**令和7年度内に協議会の規約、規程等の案**を作成する。
- **令和8年秋頃 協議会の発足**に向けて、関係省庁とも協議の上、年明け以降、構成員の候補となる事業者等との調整を進め、**来春以降、参加の案内**を進める。

令和7年12月	「サイバー対処能力強化法の施行等に関する有識者会議」及び「サイバーセキュリティ推進専門家会議」 開催
	「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」及び「サイバーセキュリティ戦略」 閣議決定（予定）
令和8年春	協議会規約案・規程案等の策定
	協議会構成員候補への案内開始
令和8年秋頃	新協議会の発足

官民連携基盤整備に係る考え方

- 新法の施行に係る事務（インシデント報告、特定重要電子計算機の届出、官民双方向の情報共有）を行うシステムを整備。
  さらに、報告、届出に関連する各省の手続き等についても、官民連携基盤を活用して行えるよう所要の調整を進める。
- **インシデント報告等の機能**については**施行（公布から1年6月以内）に合わせて先行運用開始。**
  その他機能も含め**令和9年春頃までに本格運用開始。**

今後の進め方・リリースタイミング等

検討・構築（～令和8年7月頃）	先行運用開始（令和8年夏頃～）	本格運用開始（令和9年春頃～）

◆今後調整が必要な事項
- ✓ 概念検証の実施
- ✓ アカウントの払出し・管理方法 等

インシデント報告機能

コミュニケーション機能（リリース時期調整中）

特定重要電子計算機の届出機能

経済安保推進法に係る届出機能
（リリース時期等調整中）

情報発信機能

報告窓口の一元化に向けて

- 関係省庁申合せ※を踏まえ、本システムを活用した報告窓口の一元化に向け、今後関係法令、手続きとの整合等について関係省庁と調整を進める。
  ※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（令和7年5月28日関係省庁申合せ）