経済産業省

開会ごあいさつ

2026年2月10日

商務情報政策局 サイバーセキュリティ課

サイバー攻撃の現状

- **ランサム攻撃が引き続き大きな脅威**となっており、特に製造業における被害が目立つ。
- 委託先等を含めた**サプライチェーン全体でのセキュリティ対策の強化**が必要となっている。

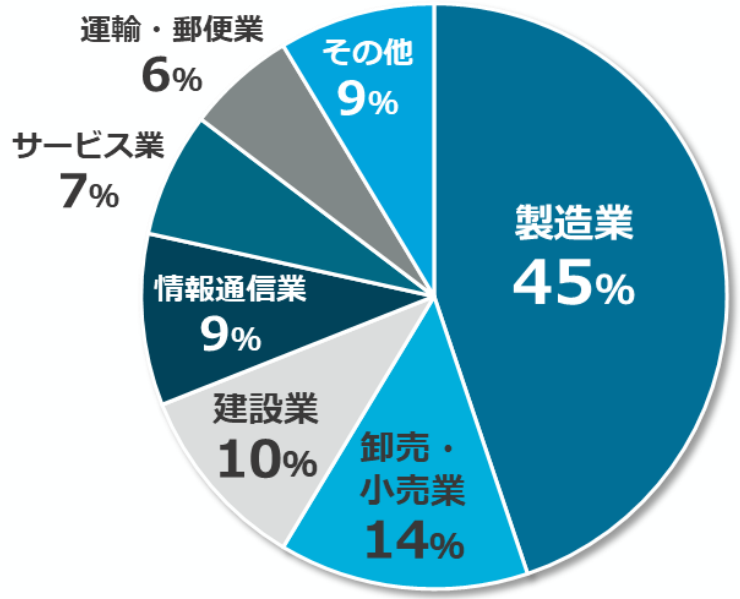
情報セキュリティ10大脅威 2026	
順　位	組織向け脅威
1位	ランサム攻撃による被害
2位	サプライチェーンや委託先を狙った攻撃
3位	AIの利用をめぐるサイバーリスク
4位	システムの脆弱性を悪用した攻撃
5位	機密情報を狙った標的型攻撃
6位	地政学的リスクに起因するサイバー攻撃
7位	内部不正による情報漏えい等
8位	リモートワーク等の環境や仕組みを狙った攻撃
9位	DDoS攻撃（分散型サービス妨害攻撃）
10位	ビジネスメール詐欺

中小企業の被害が全体の6割以上を占める

相対的にセキュリティ対策の弱い中小企業を起点に、大企業含むサプライチェーンを共有する企業を攻撃

初選出

ランサム攻撃の業種別被害割合



出典：独立行政法人情報処理推進機構（IPA）「情報セキュリティ10大脅威2026（令和８年１月）」、警察庁「令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について（令和７年９月）」を基に作成。

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
（SCS（Supply Chain Security）評価制度）

- 「対策状況は**外部から判断が難しい**」「**複数の取引先から様々な対策を要求**される」等の課題に対し、サプライチェーンにおける重要性を踏まえた上で満たすべき対策を提示しつつ、その状況を可視化する仕組みを構築。（本制度では、IT基盤が対象。）
- ２社間の取引契約等において、**発注企業が、受注側に適切な段階の”★”を提示**し、示された対策を促すとともに実施状況を確認することを想定。

構築する評価制度（案）

成熟度の定義	★ 3 [令和８年度末頃の制度開始を予定]	★ 4 [令和８年度末頃の制度開始を予定]	★ 5 [検討中]
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	全てのサプライチェーン企業が**最低限実装すべき**セキュリティ対策： • 基礎的な組織的対策とシステム防御策を中心に実施	サプライチェーン企業等が**標準的に目指すべき**セキュリティ対策： • 組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施	サプライチェーン企業等が到達点として目指すべき対策： • 国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善工程を整備、システムに対しては現時点でのベストプラクティスの対策を実施
評価スキーム	**専門家確認付き自己評価**	**第三者評価**	第三者評価

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

サプライチェーン間の結び付きが強固・複雑な主要製造業（自動車、半導体等）、流通、金融業等において、優先的に本制度の利用を促進。

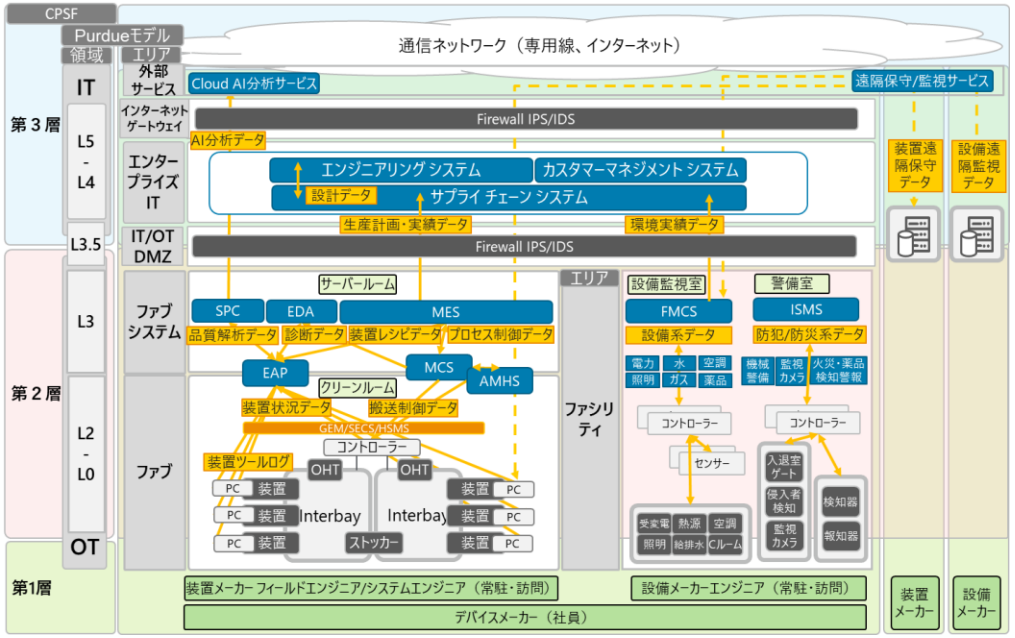
半導体関連産業のセキュリティ対策水準の強化

- 半導体関連産業の国内投資の促進が強力に進められているところ、国際的な枠組みとの整合も念頭に置きつつ、**半導体工場において求められるセキュリティ対策**に向けた検討を行い、2025年10月**「半導体デバイス工場におけるOTセキュリティガイドライン」を公表。**
- 本対策の内容を、経済産業省の**投資促進関係施策の要件等に紐付ける**こと等を検討。

ガイドラインの概要

- 海外では、半導体業界団体であるSEMIにより、半導体製造装置に係るE187/E188規格が策定され、米国立標準技術研究所（NIST）においてもCybersecurity Framework 2.0の半導体製造プロファイルの策定が進展。
- 本ガイドラインは、こうした国際的な規格とも整合しつつ、**生産目標の維持・機密情報保護・半導体品質の維持**のための工場セキュリティ対策の指針を示すもの。
- 半導体デバイス工場のリファレンスアーキテクチャに基づき、リスク対策フレームワーク（CPSF及びNIST CSF2.0）を活用し、**半導体デバイス工場の特徴を踏まえたリスク源（脅威、脆弱性）の洗い出し**を行うとともに、**対応するセキュリティ対策項目**について取りまとめ。

半導体デバイス工場のリファレンスアーキテクチャ

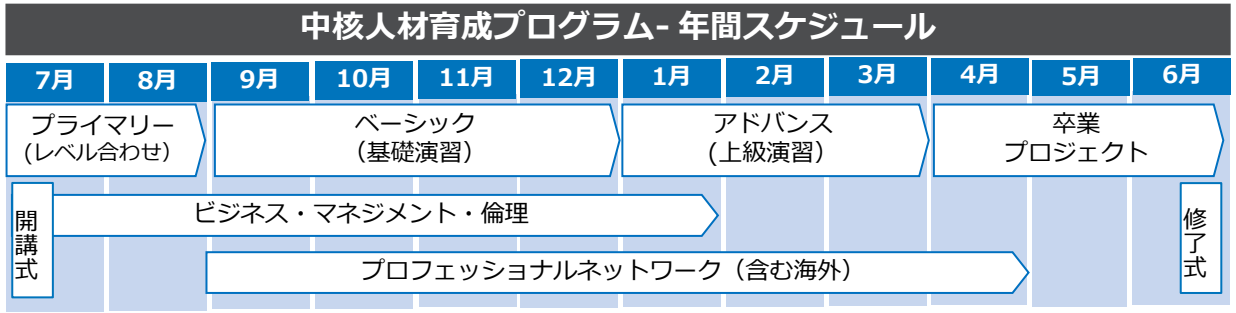


IPA産業サイバーセキュリティセンター（ICSCoE） ※2017年4月設置

- 社会インフラ・産業基盤における防護力の強化のため、OT(制御技術）とIT（情報技術）の知見を結集させた**世界レベルのサイバーセキュリティ対策の中核拠点**として、IPA内に発足。
- ICSCoEでは、世界的にも限られている、制御系セキュリティにも精通する講師を招き、テクノロジー、マネジメント、ビジネス分野を総合的に学ぶ１年の集中トレーニング等を実施。

□　１年を通じた集中トレーニング「中核人材育成プログラム」

□　電力、石油、ガス、化学、自動車、鉄道分野等の企業から1年間派遣
（第1期：76人、第2期：83人、第3期：69人、第4期：46人、第5期：48人、第6期：48人、第7期：65人、第８期：57人、第９期：55人）



- ○ IT系・制御系に精通した専門人材の育成
- ○ 模擬プラントを用いた対策立案
- ○ 実際の制御システムの安全性・信頼性検証等
- ○ 攻撃情報の調査・分析

現場を指揮・指導するリーダーを育成

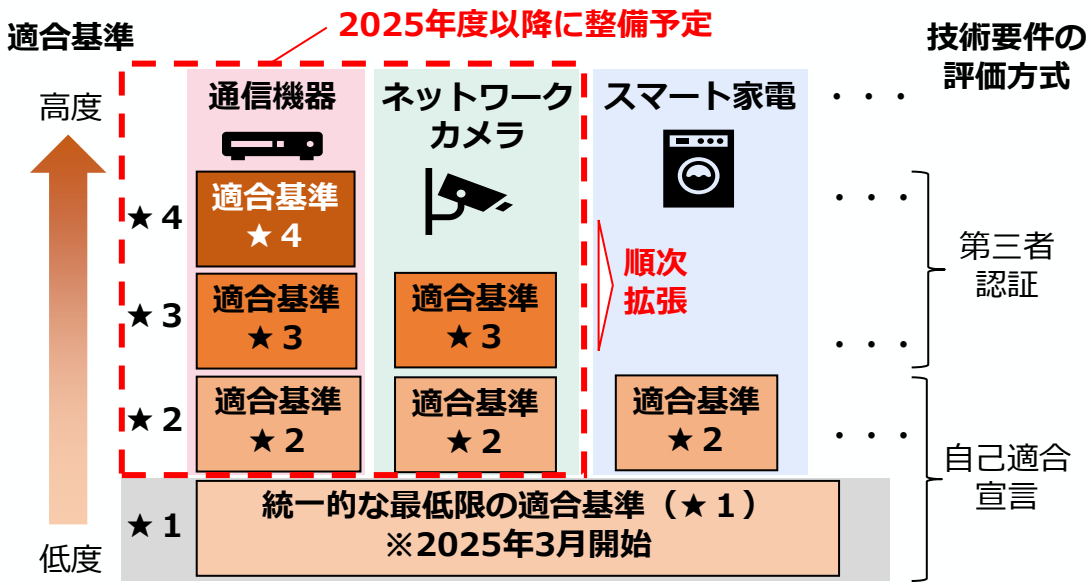
□　米・英・仏等の海外とも協調したトレーニングを実施

- ➢ DHSが開催する高度なサイバーセキュリティトレーニングである301演習への参加
- ➢ 政府機関、産業界等のセキュリティ専門家との意見交換や研究機関の施設見学等を実施

IoTセキュリティ適合性評価制度（JC-STAR）の開始

- 将来的に４段階での適合性評価を目指すこととしており、**１段階目（★１）**について、**2025年３月から申請受付**を開始し、**５月より「適合ラベル取得製品リスト」を公開。**
- **政府調達の要件化**に加え、地方公共団体、重要インフラ事業者等への**普及展開**を図るとともに**諸外国の関連制度との相互承認**を進めていく（2026年１月から英国との相互承認を開始）。

より高度な基準の策定（JC-STAR）



相互承認調整を進める外国制度の例

国・地域	シンガポール	英国	米国	EU
制度名	CLS	PSTI	U.S. Cyber Trust Mark	CRA
マーク	CYBERSECURITY LABEL CSA/IOTWABCD	–	U.S. CYBER TRUST MARK	CE
開始時期	2020年10月制度開始	2024年4月施行	2025年より基準策定開始（制度開始時期は調整中）	• 報告義務: 2026年9月 • その他: 2027年12月
任意/義務	任意	義務	任意	義務
対象	消費者向けIoT機器	消費者向けIoT機器	消費者用無線IoT製品	デジタル要素を含む製品

（参考）調達者への制度展開戦略と初期ターゲット

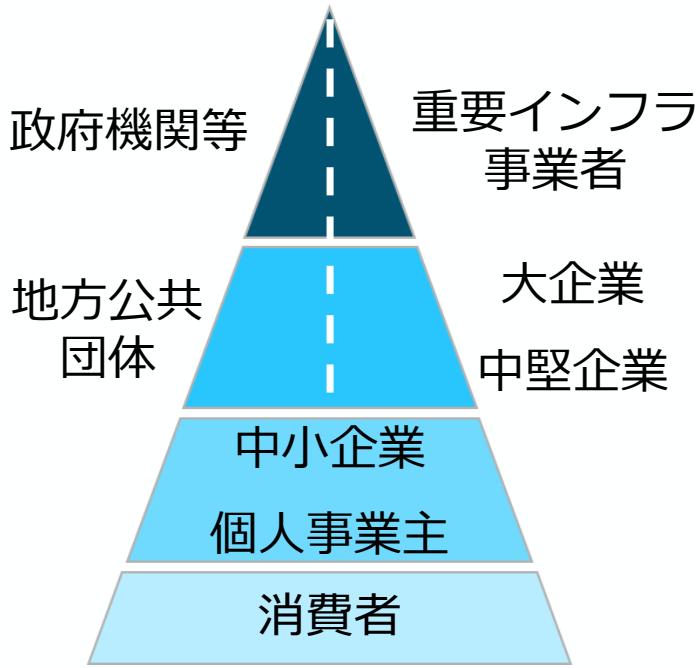
- **政府機関等、重要インフラ事業者、地方公共団体等**に関連するガイドラインや補助金等にJC-STARを位置づけ、調達や補助金等の要件として位置づけを図っていく。
- 併せて、IoT製品ベンダー・団体等へのラベル取得の働きかけ、及び民間企業・消費者への本制度の目的やラベルの意義等の周知を行い、ラベル取得製品の調達・購入を浸透させていく。

「政府機関等の対策基準策定のためのガイドライン」等

✓ 2025年度の改定で、**JC-STARを選定基準に含めることを追記**済み(※1)

「地方公共団体セキュリティポリシーガイドライン」等

✓ 2025年3月の改定にて反映済み(※2)



✓ 令和7年度の「再生可能エネルギー導入拡大・系統用蓄電池等電力貯蔵システム導入支援事業費補助金」や「長期脱炭素電源オークション」においてラベルの取得が要件化

※1：NCO「政府機関等の対策基準策定のためのガイドライン（令和7年度版）の一部改定（令和７年９月）」 https://www.nisc.go.jp/pdf/policy/general/rev_pointr7_9.pdf
※2：総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」等の意見募集の結果及び改定版の公表（令和７年３月）」 https://www.soumu.go.jp/menu_news/s-news/01gyosei02_02000355.html

SBOM国際共同ガイダンスの策定・共同署名について

- 2025年９月、経済産業省は内閣官房国家サイバー統括室と共に、サイバーセキュリティのためのSBOMの共有ビジョンに関する国際ガイダンスへの共同署名を発表。
- 同文書は、経済産業省及び米CISAの主導により、**SBOMの活用の重要性を広く国際的に発信**するとともに、**SBOM運用上の国際共同ガイダンスを整備**することを目的として作成したもの。

共同署名の参加国（計15か国）

日本、アメリカ、ドイツ、フランス、イタリア、オランダ、カナダ、オーストラリア、ニュージーランド、インド、シンガポール、韓国、ポーランド、チェコ及びスロバキア

同文書の内容

（1）SBOMとは何か、（2）SBOM導入のメリット、（3）SBOMにおけるステークホルダーとその影響、（4）セキュア・バイ・デザインにおけるSBOMの重要性

今後の予定

より技術的な内容を具体化したガイダンスの策定に向けて引き続き国際議論を進める予定。


TLP:CLEAR

A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity

Publication: September 3, 2025

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security
Czech National Cyber and Information Security Agency
French Cybersecurity Agency
Germany's Federal Office for Information Security
Indian Computer Emergency Response Team
Italy's National Cybersecurity Agency
Japan's Ministry of Economy, Trade and Industry
Japan's National Cybersecurity Office
Netherland's National Cyber Security Centre
New Zealand's National Cyber Security Centre
Poland's Research and Academic Computer Network
Cyber Security Agency of Singapore
Slovakia's National Security Authority
Republic of Korea's National Intelligence Service/National Cyber Security Center
Korea Internet and Security Agency

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

TLP:CLEAR

サイバー対処能力強化法及び同整備法の全体像

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

概　要

総　則　□ 目的規定、基本方針等（第１章）

官 民 連 携（強化法）

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

（第２章）

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

（その他、雑則（第11章）、罰則（第12章））

通信情報の利用（強化法）

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

→ □ 分析情報・脆弱性情報の提供等 ←（第８章）

アクセス・無害化措置（整備法）

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

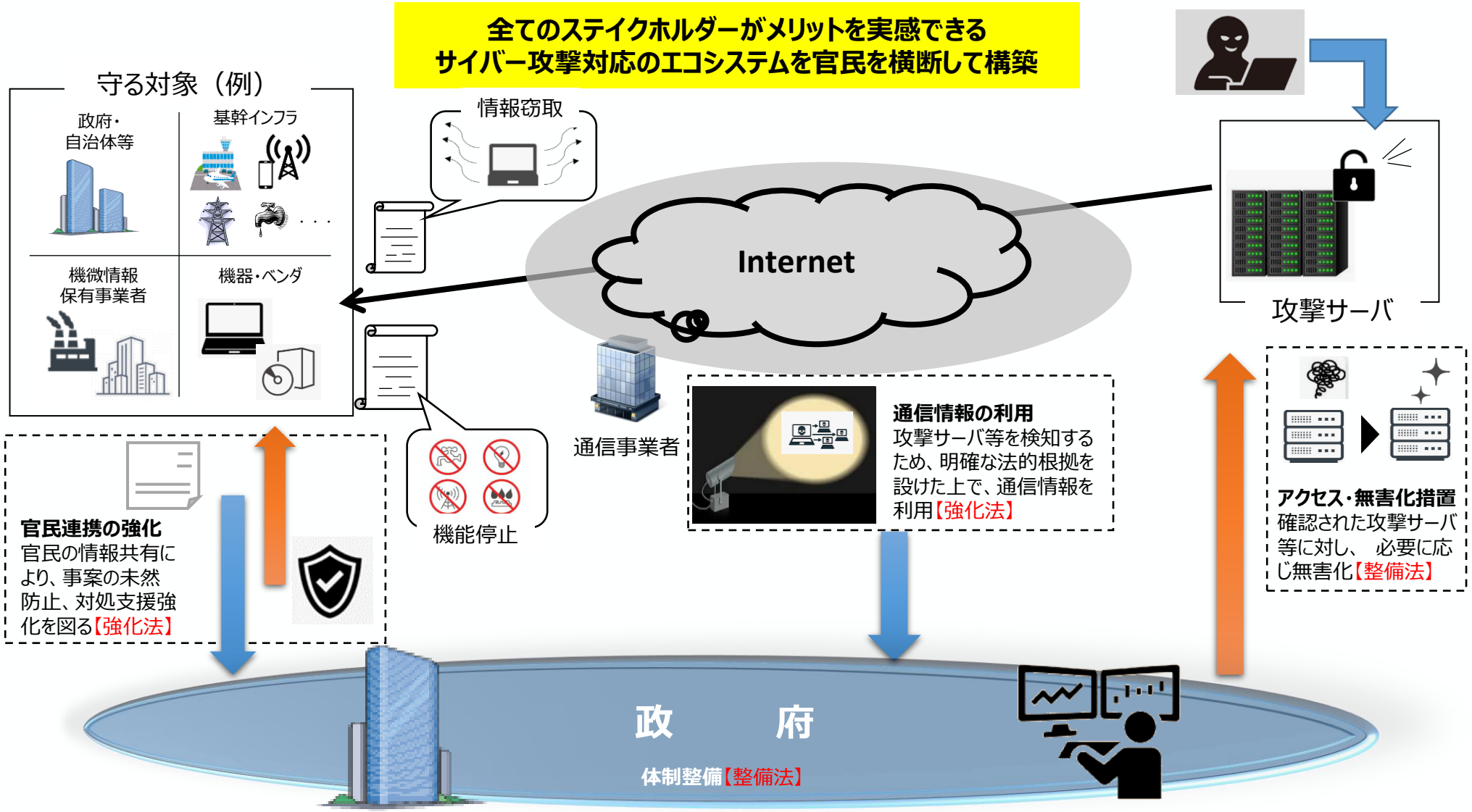
組織・体制整備等（整備法）

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

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

全体イメージ

「国民生活や経済活動の基盤」と「国家及び国民の安全」をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備する。



経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html

経済産業省　サイバーセキュリティ　検索