

The background features a blue and white isometric illustration of a city skyline. Various buildings are depicted, some with shield icons containing checkmarks on their roofs, symbolizing security. A train is shown on tracks in the lower right, and a satellite dish is visible on the right side. The entire scene is framed by blue diagonal stripes at the top and bottom.

サイバー対処能力強化法等の施行について

2026年9月

内閣官房国家サイバー統括室

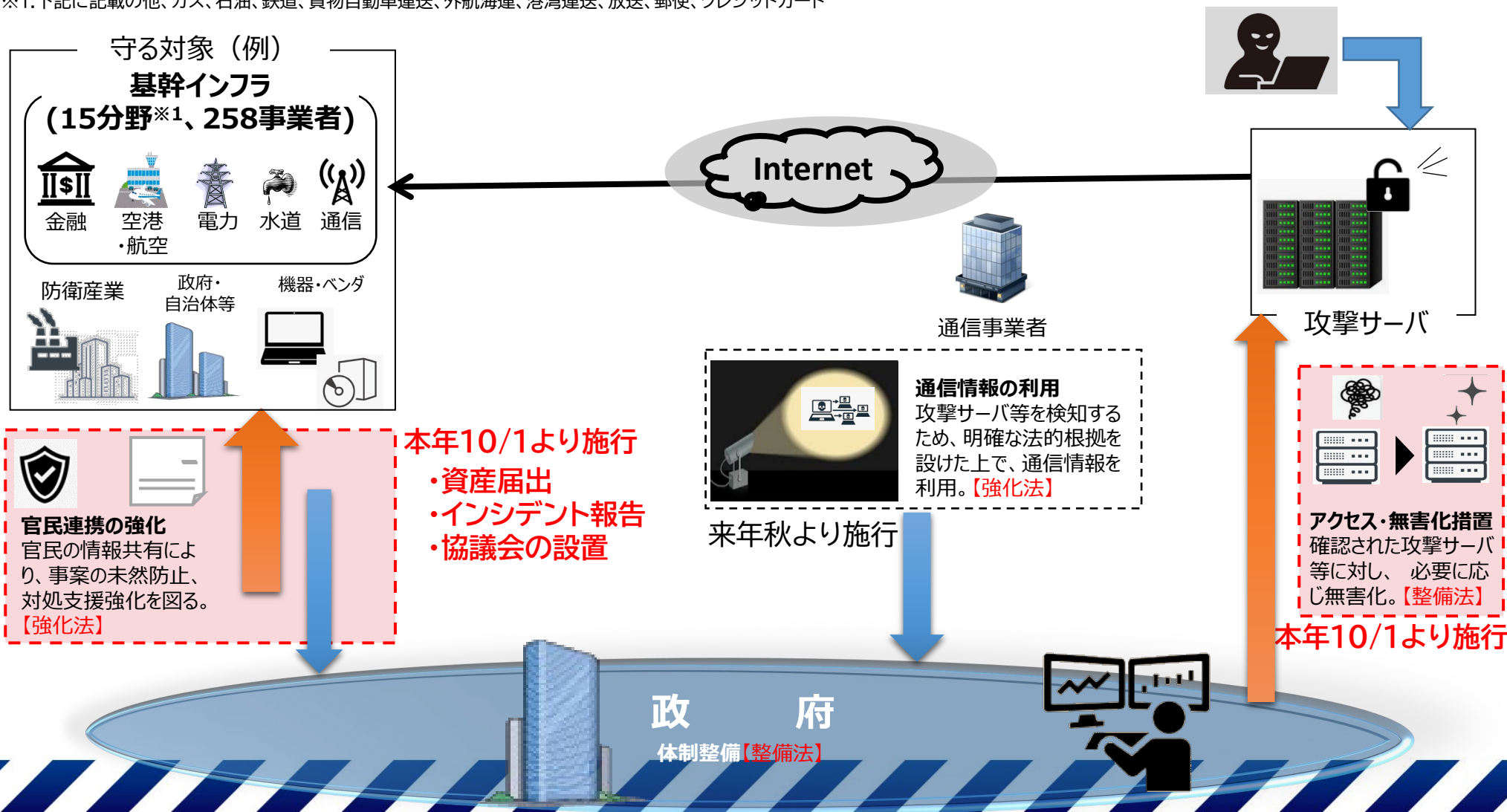
内閣府政策統括官（サイバー安全保障担当）

サイバー対処能力強化法・同整備法の全体イメージ

1

- 本年10/1以降、①基幹インフラ事業者等による対策に繋がる国独自の情報の積極的な提供（官民連携の強化）や、②攻撃サーバー等に対するアクセス・無害化措置を通じて、巧妙化するサイバー脅威から、国民生活や経済活動の基盤である基幹インフラ等を守る。

※1. 下記に記載の他、ガス、石油、鉄道、貨物自動車運送、外航海運、港湾運送、放送、郵便、クレジットカード



① 官民連携の目指す姿

- 国民の生命・身体・財産の安全に直結する基幹インフラ等をサイバー攻撃から守る。
- 脅威に対処するために必要な情報について、強力な信頼・協力関係の下、政府と民間で積極的に提供しあい、行動につなげる。

② 取組方針

- 協議会について、構成員の能動的・積極的な参加を実現するため、以下に取り組む。
 - ① 適切な情報の取扱いルールの設定等により、秘匿性の高い情報を安心して共有できる枠組みを作る。また、構成員のニーズを丁寧に把握し、それを柔軟に盛り込んだ協議会運営を行う。
 - ② その上で、政府が率先して、インシデント報告や通信情報※、外国情報や政府への攻撃情報などの国独自の情報源をフル活用し、基幹インフラ事業者等を狙う脅威に関する分析も加えつつ、対策に繋がるアクションナブルな情報を、タイムリーかつピンポイントに提供していく。
 - ③ また、共有する情報を元に、被害を防止・軽減するための能動的な対処に官民協同で取り組む。
- 資産届出・インシデント報告について、「もらって終わり」ではなく、提供事業者の対策に繋がる有益な情報をフィードバックする。

※ 来年秋以降の活用

③ 10/1施行

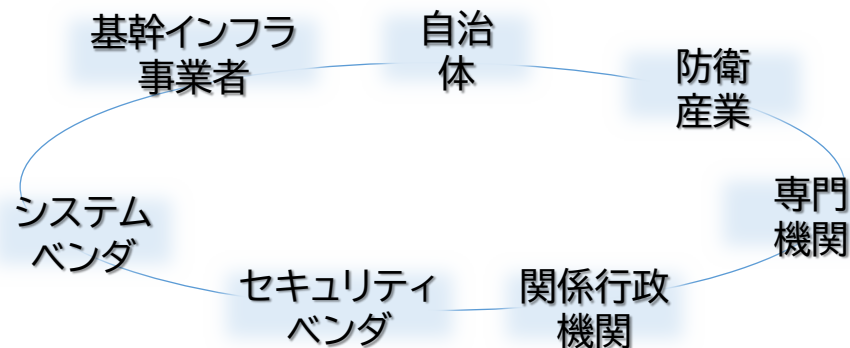
情報共有・対策のための協議会の設置

基幹インフラ事業者による
資産届出・インシデント報告

- 10/1より、協議会には基幹インフラ事業者を中心に約100組織が構成員として加入する予定。
- 国が入手した脅威情報は可能な限り迅速にサニタイズして提供しつつ、秘匿度の高い情報は秘密に指定し、情報保全を確保の上、1:1やTrusted Group(TG)などのより安全な環境で提供する。
- これらを柔軟に使い分け、基幹インフラ事業者等を狙う脅威に関する国独自の分析も加えつつ、構成員のCS対策に繋がるアクションブルな情報を、タイムリーかつピンポイントに提供していく。

対象者

協議会構成員※1



※1. 協議会には、幅広いサイバーセキュリティのため、協議会フレンズという情報共有の枠組を設け、サニタイズした情報を共有していく。

情報提供

サニタイズ情報(広く・早く共有)

(1)システムでの迅速な提供

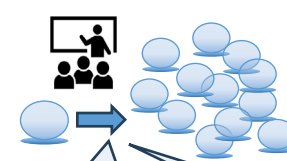


悪用された機器

脆弱性

レポート

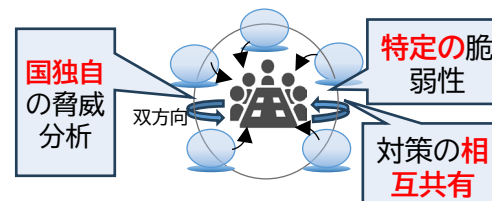
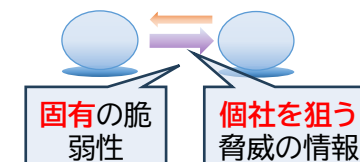
(2)対面での一斉共有



緊急度高の横断的脆弱性

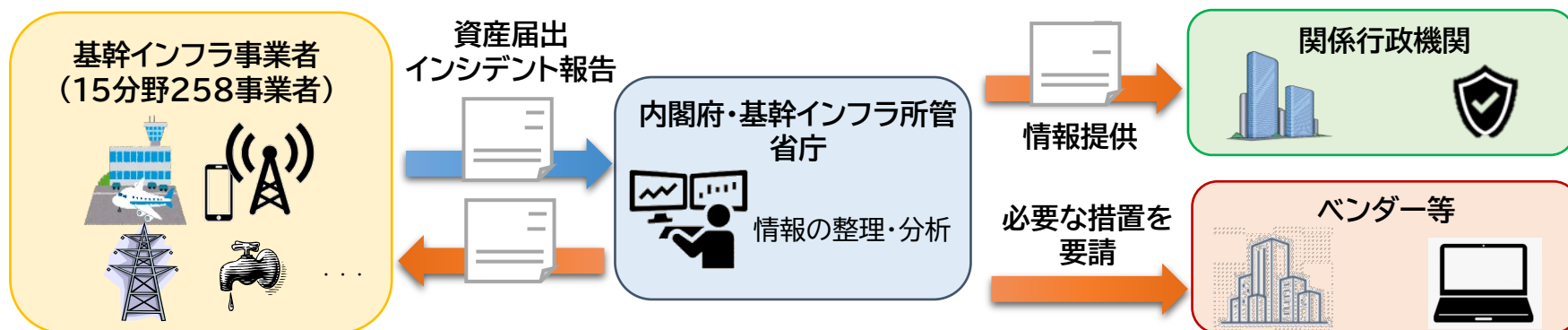
他社インシデントの速報

秘匿度の高い情報(深く・密に共有)

(3)Trusted Group
特定メンバーで双方向の共有(4)1:1での共有
タイムリー・ピンポイントな注意喚起

- 基幹インフラ事業者から来年3月までに届出される資産情報と、国が入手する未公表のものも含む脆弱性情報を突合。当該脆弱性に関する資産を特定し、ピンポイントで該当する基幹インフラ事業者に速やかに注意喚起する。これにより、AIで加速する脆弱性悪用にも対抗する。
- 10月1日より義務付けが始まる国へのインシデント報告は、技術情報等を可能な限りタイムリーに横展開※1し、他事業者への被害拡大を抑える。また、脅威分析にも活用し、基幹インフラ事業者等を狙う脅威の未然の把握に繋げる。

※1.事案発生のためインシデント対処中の被害組織への配慮が前提



資産届出

情報提供

- 基幹インフラ事業者は、導入済の特定重要電子計算機の製品名等を来年3月までに事業所管大臣に届出※2。
- 新規導入の特定重要電子計算機については導入から4か月以内の届出を求める。

※2. 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

インシデント報告

- 本年10月1日より、基幹インフラ事業者は、特定重要電子計算機のサイバーインシデント(マルウェアの実行、不正アクセス等)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

対処のあり方を戦略的に検討する体制の立上げ

※一定期間内において特定の主体が国・重要インフラ等の特定の組織・分野に対して特定の攻撃手法・攻撃インフラを用いて繰り返し行うサイバー攻撃活動

- 我が国を標的とするサイバー攻撃キャンペーン(※)等について、NCO、警察庁、防衛省・自衛隊等関係省庁が常に情報収集・分析・評価。
- 当該結果に基づき、対処のあり方を戦略的に検討・調整する局長級の検討体制を立上げ。

【対処のあり方の例】注意喚起、テイクダウン、パブリック・アトリビューション、アクセス・無害化措置等



パブリック・アトリビューション

サイバー攻撃情勢に関する情報収集・分析等の強化

- 国内関係機関と連携して情報の収集・分析・共有を強化することに加え、海外関係機関とも、有益な情報交換を継続・推進。
- 新協議会等を通じ、民間部門との連携を更に強化。



NCO、警察、防衛省・自衛隊の連携強化

- 共同対処に際しては、NCO、警察、防衛省・自衛隊から派遣されたりエゾンが、対処状況の情報共有、実施主体の役割分担を調整。
- 対処状況については、踏み台サーバ等が容易に利用可能なサイバー空間における特性を踏まえて、視覚的に理解しやすい形で情報共有。



実践的な訓練の実施

- NCO主催で、関係省庁との共同訓練をこれまでに複数回実施。
 - ・ サイバー通信情報監理委員会への承認申請などの行政プロセスを仮想実施。
 - ・ 攻撃元サーバや、攻撃痕跡(IoC^(※))等をサイバー空間上で仮想設定した実践的な訓練を実施。

(※)IoC: Indicator of Compromise(IPアドレス等)



訓練の様様

より高度な能力の確保に向けた取組の推進

- AIを活用したサイバー対処能力の強化等に関する事業を令和9年度予算で実施に向け要求中。
- NCO、警察庁及び自衛隊のサイバー関連部署が同一の場所で勤務して、相互の連携・運用を更に強化するための新庁舎を整備予定。



新庁舎
(イメージ)