資料1-3

サイバー対処能力強化法※1及び同整備法※2について

※１　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）

※２　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）

令和７年９月
内閣官房国家サイバー統括室

本説明の位置付け

- 国家安全保障戦略（令和４年12月16日閣議決定）や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における提言（令和６年11月29日とりまとめ）も踏まえた、**サイバー対処能力強化法及び同整備法**が、国会での審議・修正を経て、**本年５月16日に成立し、同月23日に公布された**。
- サイバー対処能力強化法においては、政府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したときには、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・周知を行うことができる旨など、**重要電子計算機に対するサイバー攻撃による被害の防止**の観点から、**政府の脆弱性に係る対応**が規定されている。
- このため、**サイバー対処能力強化法の施行**※に向けては、**今年度末までの告示改訂**を念頭に、今後、こうした同法の規定やその趣旨も踏まえ、**関係機関による脆弱性関連情報の取扱い及びこれに関する告示・ガイドラインのあり方**について、**本研究会で議論を行う**こととしたい。
- 本説明は、その**議論のキックオフ**として、**サイバー対処能力強化法の概要**を説明するもの。

※官民連携部分の施行は、法律の公布（令和７年５月23日）後１年６月を超えない範囲において政令で定める日

資料1-3

検討の背景

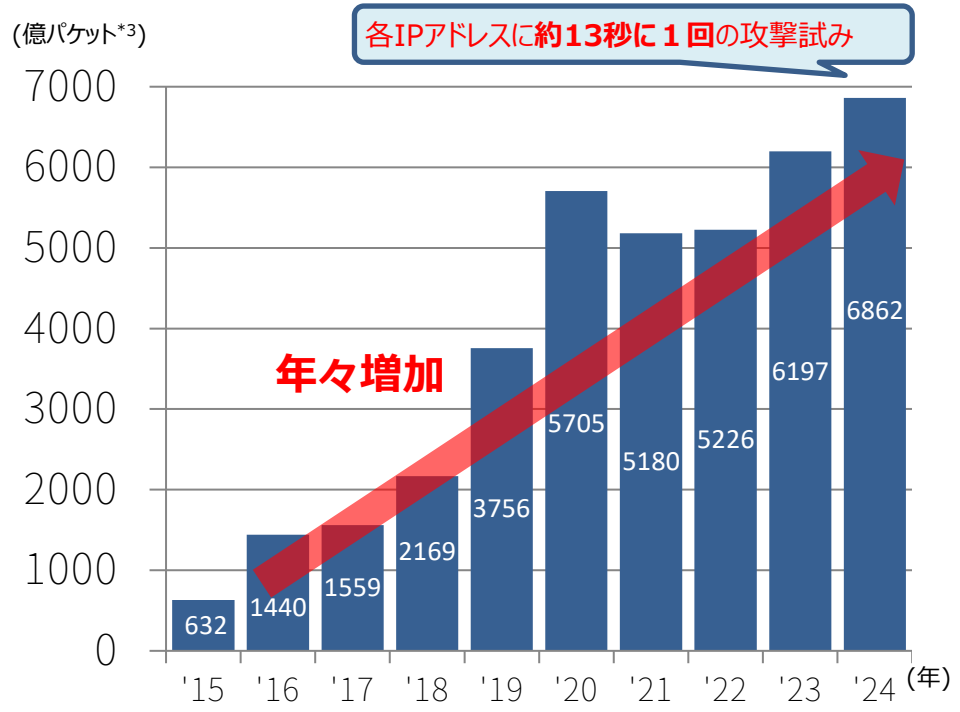
サイバー攻撃の変遷

- サイバー攻撃は巧妙化・深刻化するとともに、サイバー攻撃関連通信数や被害数は増加傾向にあり、**質・量両面でサイバー攻撃の脅威は増大**している。
- 令和６年中に観測された**サイバー攻撃関連の通信の99%以上が海外から発信**[*1]

*1出典：警察庁資料。令和６年中に警察庁が観測したサイバー攻撃関連の通信（ダークネット向けの攻撃通信を含むパケット）の99.4%が海外のIPアドレスを発信元とするもの。

サイバー攻撃関連通信や被害の量

NICT [*2]が観測したサイバー攻撃関連通信数の推移



*2 国立研究開発法人 情報通信研究機構
（National Institute of Information and Communications Technology）の略。
*3 １度に届くデータの塊のこと。センサーがデータを受信した回数と同義。

サイバー攻撃の巧妙化・深刻化

サイバー安全保障に関わる攻撃例

IT系システムの侵害

（暗号化・システム障害、身代金要求）

（例：2021年米コロニアルパイプライン業務停止、2022年大阪急性期・総合医療センターの業務停止、2023年名古屋港業務停止）

＋

有事に備えた重要インフラ等への侵入

（高度な侵入・潜伏能力）

（例：2014年クリミア併合、2022年ウクライナ侵略、2023年VoltTyphoonによるグアム等にある米軍施設や政府機関、重要インフラへの侵害）

＋

機微情報の窃取

（アクセス権限の獲得）

（例：2021~24年JAXAへの侵害、2023年NISCのメール窃取）

欧米主要国が先行する主な取組

官民連携関係

■ 主要国は、2010年代後半から最近にかけ、**政府からの情報提供、重要インフラ事業者による報告の義務化を制度化**

- 国家ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略(2023年)
  重要ｲﾝﾌﾗｻｲﾊﾞｰｲﾝｼﾃﾞﾝﾄ報告法(2022年)
- 国家ｻｲﾊﾞｰ戦略(2022年)
  ﾈｯﾄﾜｰｸ情報ｼｽﾃﾑ規則(2018年)
- 豪州ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略(2023年)
  重要ｲﾝﾌﾗ保安法(2018年)
- ｻｲﾊﾞｰﾚｼﾞﾘｴﾝｽ法(2024年)
  ﾈｯﾄﾜｰｸ情報ｼｽﾃﾑ指令(2016年)

通信情報の利用関係

■ 主要国は、**以前より、国家安全保障等の目的のために外国関係の通信情報を利用**

■ 政府における通信情報の利用について **専門の独立機関が監督**

- 英国：調査権限法
  (2016年制定)
- ドイツ：連邦情報局法
  (2016年改正)
- 米国：外国情報監視法
  (2008年改正)
- 豪州：通信情報傍受及び
  アクセス法(2021年改正)

アクセス・無害化関係

- 米国：Volt Typhoonによるボットネットワーク（感染ルータ群）に対する**無害化措置**（2024年）
- カナダ：政府ネットワークからの情報窃取防止目的で、攻撃者の海外サーバに対する**無害化措置**（2019年以降）
- 英国、豪州も同様の取組を推進。

＊ 各国の法制及び実態の全てを網羅するものではない。

資料1-3

法律の内容について

- サイバー対処能力強化法（強化法）
- サイバー対処能力強化法整備法（整備法）

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。

全てのステイクホルダーがメリットを実感できる
サイバー攻撃対応のエコシステムを官民を横断して構築

守る対象（例）

政府・自治体等

基幹インフラ

機微情報保有事業者

機器・ベンダ

情報窃取

Internet

攻撃サーバ

通信事業者

機能停止

通信情報の利用
攻撃サーバ等を検知するため、明確な法的根拠を設けた上で、通信情報を利用【強化法】

アクセス・無害化措置
確認された攻撃サーバ等に対し、 必要に応じ無害化【整備法】

官民連携の強化
官民の情報共有により、事案の未然防止、対処支援強化を図る【強化法】

政　　府

体制整備【整備法】

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

P7 総　則
- 目的規定、基本方針等（第１章）

P8 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））

P11 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）

P16 → 分析情報・脆弱性情報の提供等（第８章）

P18 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）

P21 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

P24 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

強化法【法目的等】

目的規定（強化法第１条）

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不正な行為による被害の防止を図ることを目的として規定

通信の秘密の尊重（強化法第２条の２）

法の適用に当たっては、第１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旨を規定

※　衆議院での修正項目

基本方針の策定（強化法第３条）

法に定める事務を一体的かつ効果的に実施することを確保するため、以下の基本的事項を定める。

① 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こと
② 当事者協定の締結に関すること
③ 通信情報保有機関における通信情報の取扱いに関すること
④ 情報の整理及び分析に関すること
⑤ 総合整理分析情報の提供に関すること
⑥ 協議会の組織に関すること

等

強化法①【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

（詳細）官民連携の強化①

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）

○　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け出なければならないこととするとともに、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することとする（資産届出）。（第４条）

○　基幹インフラ事業者は、不正アクセス行為等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たこと又はその原因となり得る一定の事象を認知したときは、その旨及び一定の事項を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こととする。（第５条）

☆　そのサイバーセキュリティが害された場合に、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一定の電子計算機。

情報共有・対策のための協議会の設置（強化法第９章）

○　内閣総理大臣は、サイバー攻撃による被害の防止のため、重要電子計算機を使用する者等（あらかじめ同意を得た者に限る。）を構成員とする協議会を設置し、構成員に対し、守秘義務を伴う被害防止に資する情報を共有するとともに、必要な資料提出等を求めることができることとする（サイバーセキュリティ協議会を廃止し、強化・新設）。（第45条）

電子計算機の使用者に対する情報共有（強化法第８章第41条）

○　内閣総理大臣は、サイバー攻撃による被害の防止に必要な情報を公表・周知する。（第41条）

（詳細）官民連携の強化②

脆弱性対応の強化等（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）

○　内閣総理大臣及び電子計算機等供給事業所管大臣（☆１）は、重要電子計算機として用いられる電子計算機やプログラムにおける脆弱性を認知したときには、当該電子計算機等の供給者（☆２）に対し情報を提供することができることとする。（第42条第１項）

　電子計算機等供給事業所管大臣（☆１）は、脆弱性が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ものである場合には、当該電子計算機等の供給者（☆２）に対し、サイバー攻撃による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こととする。（第42条第２項）

☆１　ここでいう「電子計算機等供給事業所管大臣」とは、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を指す。

☆２　電子計算機等の「供給者」とは、電子計算機等の生産者、輸入者、販売者及び提供者を意味している。

○　電子計算機やプログラム等の供給者に対する責務規定（利用者のサイバーセキュリティ確保のための設計・開発、情報の継続的な提供等に努める旨）を設ける。（サイバーセキュリティ基本法 第７条第２項）

罰則の整備（強化法第12章）

・行政職員及び協議会構成員等による秘密の不正な利用・漏えいの行為
　⇨ ２年以下の拘禁刑又は100万円以下の罰金（第82条）

・基幹インフラ事業者がインシデント報告等を行わず、是正命令を受けてもなお対応しない場合
　⇨ 200万円以下の罰金（第83条）

・基幹インフラ事業者がインシデント報告等に関連し、資料提出等を求められても対応しない場合
　⇨ 30万円以下の罰金（第84条）

強化法②【通信情報の利用】

我が国に対する**サイバー攻撃の実態を把握するため、通信情報を利用し、分析**。これらについては、独立機関がチェック。制度設計に当たっては、**「通信の秘密」に十分配慮**

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

- 内閣総理大臣は、基幹インフラ事業者等との協定に基づき、通信情報を取得（このうち、外内通信に係る通信情報を用いて分析を実施、当該事業者に必要な分析結果を提供）（強化法第３章関係）

（同意によらない）通信情報の取得

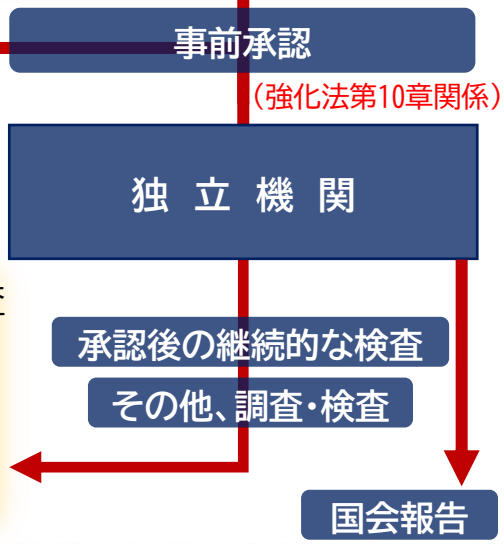
【外外通信の分析】

- 内閣総理大臣は、国外の攻撃インフラ等の実態把握のため必要があると認める場合には、独立機関の承認を受け、通信情報を取得（強化法第４章関係）

【外内通信又は内外通信の分析】

- 内閣総理大臣は、国内へのサイバー攻撃の実態把握のため、特定の外国設備との通信等を分析する必要があると認める場合には、独立機関の承認を受け、通信情報を取得（強化法第６章関係）

（※）外外通信：国内を経由し伝送される国外から国外への通信
外内通信：国外から国内への通信
内外通信：国内から国外への通信



自動的な方法による機械的情報の選別の実施（強化法第２条第８項、第22条、第35条関係）

- 内閣総理大臣は、取得した通信情報について、人による知得を伴わない自動的な方法により、調査すべきサイバー攻撃に関係があると認めるに足りる機械的情報を選別（それ以外のものを直ちに消去）

※ 機械的情報とは、アイ・ピー・アドレス、指令情報等の意思疎通の本質的な内容ではない情報

※ その他、「関係行政機関の分析への協力」（強化法第27条関係）、「取得した通信情報の取扱制限」（強化法第5章関係）等を規定

（詳細）通信情報の利用①

（同意によらない）通信情報の取得（強化法第４章、第６章）

（外外通信の分析のための取得）

内閣総理大臣は、外外通信であって、他の方法ではその実態の把握が著しく困難であるサイバー攻撃に関係するものが、特定の電気通信設備により伝送されていると疑うに足りる状況がある場合には、サイバー通信情報監理委員会の承認（☆１）を受けて、当該電気通信設備から通信情報が送信されるようにする措置（☆２）をとることができることとする。（第17条、第18条）

（外内通信又は内外通信の分析のための取得）

内閣総理大臣は、外内通信又は内外通信であって、サイバー攻撃に用いられていると疑うに足りる状況のある特定の外国設備と送受信し、又は当該状況のある機械的情報が含まれているものの分析をしなければ被害防止が著しく困難であり、他の方法ではこれらの通信の分析が著しく困難である場合には、サイバー通信情報監理委員会の承認（☆１）を受けて、これらの通信が含まれると疑うに足りる外国関係通信を伝送する電気通信設備から通信情報が送信されるようにする措置（☆２）をとることができることとする。（第32条、第33条）

☆１　委員会は承認の求めがあった場合において、理由があると認めるときは、遅滞なく承認する。

☆２　ここで送信されるものは、国外関係通信、すなわち、外外通信、外内通信及び内外通信であるが、自動選別を行うことにより、それぞれ分析に必要なものが選別されることになる。

調査すべき情報の選別（強化法第１章第２条第８項、第５章第22条、第７章第35条）

内閣総理大臣は、取得した通信情報について、人による知得を伴わない自動的な方法により、対象とすべき通信のうち機械的情報（☆）であって調査すべきサイバー攻撃に関係があると認めるに足りる状況があるものを、承認を受ける際に定めた基準に基づき選別した後、それ以外のものを直ちに消去する措置を講ずることとする。（「自動選別」）（第22条、第35条）

☆　アイ・ピー・アドレス、指令情報等の意思疎通の本質的な内容ではない情報（第２条第８項）

（詳細）通信情報の利用②

当事者協定（同意）に基づく通信情報の取得（強化法第３章）

内閣総理大臣は、基幹インフラ事業者その他の電気通信役務の利用者との協定に基づき、当該利用者が送受信する通信情報の提供を受けることとする（この通信情報のうち、外内通信に係る通信情報を用いてサイバーセキュリティ確保のための分析を行うとともに、当該利用者のサイバーセキュリティの確保のため必要な分析結果を提供することとする）。（第11条～第13条）

☆　内閣総理大臣及び基幹インフラ事業者は、相互に、相手方に対し、協定締結のための協議の求めをすることができることとし、相手方は、正当な理由がない限り、協議に応じなければならないこととする（協定はあくまで任意）。

☆　前ページの「調査すべき情報の選別」（自動選別）は、協定に基づき取得した通信情報についても実施。

関係行政機関の分析への協力（強化法第５章第27条）

内閣総理大臣は、自動選別又は選別後の通信情報の分析をする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に対し、必要な協力を要請できることとし、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、協力を行うものとする。（第27条）

取得した通信情報の取扱制限（強化法第５章）

内閣総理大臣は、取得した通信情報について、自動選別を行う場合を除き、選別前の通信情報を自ら利用し、又は提供してはならないこととする。選別後の通信情報についても、関係行政機関に分析協力を要請する場合、アクセス・無害化を行う行政機関に提供する場合等を除き、提供してはならないこととする。　等（第５章）

（詳細）通信情報の利用③

独立機関の設置等（強化法第10章）

○　通信情報の利用の適正確保のため、サイバー通信情報監理委員会（いわゆる３条委員会）を置くこととする。（第46条）

○　委員会に、内閣総理大臣による（同意によらない）国外関係通信の取得に際しての遅滞のない審査・承認、通信情報の取扱いに対する継続的な検査、無害化措置に際しての審査・承認等の事務を行わせることとするほか、通信情報を保有する機関に対する勧告等の権限を付与する。（第63条～第68条）

○　委員会は、委員長及び委員４人をもって組織する。また、委員長及び委員は、専門的知見を有する者等から両議院の同意を得て、内閣総理大臣が任命する。（第50条）

○　また、同委員会は、その所掌事務の処理状況について、国会に報告するとともに、その概要を公表しなければならないこととする。この国会報告には以下の事項が含まれなければならない※。（第61条）

① 外外通信目的送信措置に係る承認の求め及び当該承認並びに措置期間の延長に係る承認の求め及び当該承認のそれぞれの件数
② 特定外内通信目的送信措置に係る承認の求め及び当該承認並びに措置期間の延長に係る承認の求め及び当該承認のそれぞれの件数
③ 特定内外通信目的送信措置に係る承認の求め及び当該承認並びに措置期間の延長に係る承認の求め及び当該承認のそれぞれの件数
④ 自動選別、取得通信情報の取扱い等に係る検査の結果の概要
⑤ 取得通信情報の取扱いが違反している旨の通知、懲戒処分の要求及び勧告のそれぞれの件数及び概要
⑥ サイバー危害防止措置執行官により行われた「アクセス・無害化措置」に係る承認の求め及び通知並びに当該承認のそれぞれの件数
⑦ ⑥の通知に係る勧告の件数及び概要
⑧ 自衛官により行われた「アクセス・無害化措置」に係る承認の求め及び通知並びに当該承認のそれぞれの件数
⑨ ⑧の通知に係る勧告の件数及び概要

※　衆議院での修正項目

（詳細）通信情報の利用④

罰則の整備（強化法第12章）

・通信情報を取り扱う行政職員による、通信情報の不正な利用・漏えいの行為
　⇨ データベース提供については、４年以下の拘禁刑又は200万円以下の罰金
　　その他は、３年以下の拘禁刑又は100万円以下の罰金　（第79条、第81条）

・通信情報を保有する行政機関の管理を侵害して通信情報を取得する行為
　⇨ ３年以下の拘禁刑又は150万円以下の罰金　（第80条）

強化法③【分析情報・脆弱性情報の提供等】（強化法第８章関係）

資料1-3

基幹インフラ事業者から
届出された**電子計算機の情報**
（第２章）

〃
報告された**インシデント情報**
（第２章）

選別した後の**通信情報**※
（第５章、第７章）

協議会を通じて得た情報
（第９章）

その他の情報
（外国政府から提供された情報等）

情報の整理・分析
（第37条）

通信情報や秘密を含み得る

総合整理分析情報
国の行政機関 等
（第38条）

通信情報は含まないが秘密は含み得る

提供用総合整理分析情報
協議会の構成員 等（※）
（第45条）

通信情報や秘密は含まず

周知等用総合整理分析情報
基幹インフラ事業者
電子計算機等の供給者
公表・周知 等
（第40条～第42条）

※　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）

（詳細）分析情報・脆弱性情報の提供等

分析情報の提供等（強化法第８章）

○　内閣総理大臣は、基幹インフラ事業者によるインシデント報告等に係る情報を含め、取得した情報を整理・分析し、その情報を、サイバーセキュリティ確保のため、アクセス・無害化を行う行政機関その他関係行政機関に提供するものとする。また、内閣総理大臣は、必要がある場合には、外国の政府等に対し、分析情報を提供することができることとするほか、事業所管大臣も、必要がある場合にはその情報を基幹インフラの事業者に提供することができることとする。（第37条～第40条）

（再掲）　内閣総理大臣は、サイバー攻撃による被害の防止に必要な情報を公表・周知する。（第41条）

（再掲）　内閣総理大臣及び電子計算機等供給事業所管大臣（☆１）は、重要電子計算機として用いられる電子計算機やプログラムにおける脆弱性を認知したときには、当該電子計算機等の供給者（☆２）に対し情報を提供することができることとする。（第42条第１項）

（再掲）　内閣総理大臣は、サイバー攻撃による被害の防止のため、重要電子計算機を使用する者等（あらかじめ同意を得た者に限る。）を構成員とする協議会を設置し、構成員に対し、守秘義務を伴う被害防止に資する情報を共有するとともに、必要な資料提出等を求めることができることとする（サイバーセキュリティ協議会を廃止し、強化・新設）。（第45条）

罰則の整備（強化法第12章）

・行政職員及び協議会構成員等による秘密の不正な利用・漏えいの行為
　⇨　２年以下の拘禁刑又は100万円以下の罰金（第82条）

整備法①【アクセス・無害化】

サイバー攻撃による重大な危害を防止するための**警察・自衛隊による措置**等を可能とし、その際の**適正性を確保するための手続**を新設

警　　察

（警察官職務執行法第6条の2関係）

- 措置の主体は、警察庁長官が指名した警察官に限定
- 措置を実施する場面は、

① サイバー攻撃に用いられる電気通信等を認めた場合で

② そのまま放置すれば重大な危害が発生するおそれがあるため緊急の必要があるとき

- 措置の内容は、

① 攻撃関係サーバ等の管理者等への措置の命令

② 攻撃関係サーバ等への措置(※1)を自ら実施

(※1)インストールされている攻撃のためのプログラムの停止・削除など

- 国外の攻撃関係サーバ等への措置に際しての外務大臣との事前協議
- 措置に際しての手続は、独立機関の承認、警察庁長官等の指揮
  （承認を得るいとまがないと認める特段の事由がある場合：事後通知）

内閣官房(※3)の調整の下で緊密に連携

防 衛 省 ・ 自 衛 隊

（自衛隊法第81条の3・第91条の3・第95条の4関係）

- 内閣総理大臣が次の場合に通信防護措置を命じた上で、自衛隊の部隊等が措置を実施（新たな行動類型）（警察と共同対処）

① 一定の重要な電子計算機に対するサイバー攻撃であり

② 外国政府を背景とする主体による高度な攻撃と認められるものが行われ

③ 自衛隊が対処する特別の必要(※2)があるとき

(※2)自衛隊が有する特別な技術又は情報が必要不可欠であるなど

- 自衛隊及び日本に所在する米軍が使用する電子計算機をサイバー攻撃から職務上警護する自衛官が、緊急の必要があるときに無害化措置を実施
- 措置を実施する場面・措置の内容は、警察と同様
- 国外の攻撃関係サーバ等への措置に際しての外務大臣との事前協議
- 措置に際しての手続は、独立機関の承認、防衛大臣の指揮
  （承認を得るいとまがないと認める特段の事由がある場合：事後通知）

申請 ⇩ ⇧ 承認　　申請 ⇩ ⇧ 承認

独 立 機 関

（※３）アクセス・無害化については、その実施主体が警察及び自衛隊になるが、こうした措置は国家安全保障の観点から整合性のとれた形で行われる必要があり、内閣官房（新組織）が、国家安全保障局（NSS）とも連携しつつ、その司令塔機能を発揮。

（詳細）アクセス・無害化措置①

警察によるアクセス・無害化措置（警察官職務執行法（警職法）第６条の２）

○　警察庁長官が指名する警察官（サイバー危害防止措置執行官）は、サイバー攻撃又はその疑いがある通信等を認めた場合であって、そのまま放置すれば、人の生命、身体又は財産に対する重大な危害が発生するおそれがあるため緊急の必要があるときは、そのサイバー攻撃の送信元等である電子計算機の管理者その他関係者に対し、危害防止のため通常必要と認められる措置であって電気通信回線を介して行うものをとることを命じ、又は自らその措置をとることができることとする。

○　処置の対象たる電子計算機が国内に設置されていると認める相当な理由がない場合には、警察庁の警察官のみが処置をできることとし、あらかじめ、警察庁長官を通じて、外務大臣と協議しなければならないこととする。

○　サイバー危害防止措置執行官が、上記の処置をとる場合には、あらかじめ、サイバー通信情報監理委員会の承認を得なければならないこととする。
　ただし、サイバー通信情報監理委員会の承認を得るいとまがないと認める特段の事由がある場合にはこの限りでないこととし、当該処置後速やかに、当該処置について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こととする（同委員会は、必要に応じ勧告を実施）。

○　サイバー危害防止措置執行官は、措置の実施について、警察庁長官又は都道府県警察本部長の指揮を受けなければならないこととする。

（※）アクセス・無害化については、その実施主体が警察及び自衛隊になるが、こうした措置は国家安全保障の観点から整合性のとれた形で行われる必要があり、内閣官房（新組織）が、国家安全保障局（NSS）とも連携しつつ、その司令塔機能を発揮。

（詳細）アクセス・無害化措置②

防衛省・自衛隊によるアクセス・無害化措置（自衛隊法第81条の３、第91条の３及び第95条の４）

○　内閣総理大臣は、一定の重要電子計算機（☆１）に対する攻撃であって、本邦外にある者による特に高度に組織的かつ計画的な行為と認められるものが行われた場合において、自衛隊が対処を行う特別の必要がある（☆２）と認めるときは、当該重要電子計算機に対する通信防護措置をとるべき旨を命ずることができることとする（新たな行動類型の創設）。

☆１　国の行政機関等、地方公共団体、基幹インフラ、一定の防衛産業の重要な電子計算機。
☆２　☆１の電子計算機がサイバー攻撃を受け、国家及び国民の安全を著しく損なう事態が生じるおそれが大きく、自衛隊が有する特別の技術又は情報が必要不可欠であり、国家公安委員会から要請又はその同意がある場合。

○　通信防護措置をとるべき旨を命ぜられた部隊等は、警察と共同して当該通信防護措置を実施することとする。

その際、改正警職法を準用し、処置の対象たる電子計算機が国内に設置されていると認める相当な理由がない場合には、上記処置をとる当該部隊等の自衛官は、あらかじめ、防衛大臣を通じて、外務大臣と協議しなければならないこととする。

また、上記処置をとる当該部隊等の自衛官は、あらかじめ、防衛大臣を通じて、サイバー通信情報監理委員会の承認を得なければならないこととする。ただし、同委員会の承認を得るいとまがないと認める特段の事由がある場合にはこの限りでないこととし、当該処置後速やかに、当該処置について同委員会に通知しなければならないこととする（同委員会は、必要に応じ勧告を実施）。

さらに、当該部隊等の自衛官は、措置の実施について、防衛大臣の指揮を受けなければならないこととする。

○　自衛隊又は日本国にあるアメリカ合衆国の軍隊が使用する一定の電子計算機をサイバー攻撃から職務上警護する自衛官についても、同様に改正警職法の権限を準用することとする。

整備法②【組織・体制整備等】

能動的サイバー防御を含む各種取組を実現・促進するため、司令塔たる**内閣官房新組織の設置** 等、**政府を挙げた取組を推進するための体制を整備**（内閣官房（司令塔・総合調整）と内閣府（実施部門）が一体となって機能）

サイバーセキュリティ戦略本部の強化

（サイバーセキュリティ基本法第26条・第28条・第30条・第30条の2関係）

- サイバーセキュリティ戦略本部の改組

  サイバーセキュリティ戦略本部を

  ・本部長：内閣総理大臣

  ・本部員：全ての国務大臣

  とする組織に改組

  ※ 有識者から構成される「サイバーセキュリティ推進専門家会議」を設置

- サイバーセキュリティ戦略本部の機能強化

  サイバーセキュリティ戦略本部の所掌事務に

  ・ 重要インフラ事業者等のサイバーセキュリティの確保に関する国の施策の基準の作成

  ・ 国の行政機関等におけるサイバーセキュリティの確保の状況の評価

  を追加

内閣サイバー官の設置

（内閣法第19条の2及び第16条関係）

- サイバーセキュリティの確保に関する総合調整等の事務を掌理する内閣サイバー官を内閣官房に新設

※1 内閣サイバー官は、国家安全保障局次長を兼務

※2 内閣サイバーセキュリティセンター（NISC）の改組は政令で実施

内閣府特命担当大臣の設置等

（内閣府設置法第4条・第9条関係）

- 官民連携や通信情報の利用に関する事務を内閣府の所掌事務に追加
- これら事務を掌理する内閣府特命担当大臣の設置が可能

その他①（組織体制整備等）

サイバーセキュリティ戦略本部の改組（サイバーセキュリティ基本法第28条、第30条及び第30条の２）

サイバーセキュリティ戦略本部について、内閣総理大臣を本部長、全ての国務大臣を本部員とする組織に改組するとともに、有識者から構成されるサイバーセキュリティ推進専門家会議を設置する。

サイバーセキュリティ戦略本部の機能強化（サイバーセキュリティ基本法第26条）

サイバーセキュリティ戦略本部の所掌事務を見直し、

- 重要社会基盤事業者等のサイバーセキュリティ確保に関する国の基準の作成
- 国の行政機関等におけるサイバーセキュリティの確保の状況の評価　等

をその所掌事務に追加することとする。

（独）情報処理推進機構（ＩＰＡ）における事務の追加（情報処理の促進に関する法律第51条）

強化法の制定及び戦略本部の機能強化に伴い、（独）情報処理推進機構の事務に（強化法第11章）

- 情報の整理分析及び被害防止に必要な情報の周知等の事務（内閣総理大臣からの委託）
- 重要社会基盤事業者等のサイバーセキュリティの確保の状況の調査（戦略本部からの委託）

を追加することとする。（サイバーセキュリティ基本法第31条）

（国研）情報通信研究機構（ＮＩＣＴ）における事務の追加（ＮＩＣＴ法第14条）

戦略本部の機能強化に伴い、（国研）情報通信研究機構の業務に、国等の情報システムに対する不正な活動の監視及び分析に係る事務（戦略本部からの委託）を追加することとする。（サイバーセキュリティ基本法第31条）

その他②（組織体制整備等）

内閣府における所掌事務の追加等（内閣府設置法第４条、第64条）

強化法の制定に伴い、内閣府の所掌事務に強化法に関する事務（☆）を追加するとともに、同府に、サイバー通信情報監理委員会を置くこととする。

☆　強化法に基づく重要電子計算機に対するサイバー攻撃による被害の防止に関する事務（「官民連携の強化」及び「通信情報の利用」に関する部分）

内閣府特命担当大臣の設置（内閣府設置法第４条、第９条）

強化法の施行に伴い、内閣府設置法を改正することにより、強化法に関する事務を掌理する内閣府特命担当大臣を置くことができることとする。

内閣サイバー官の新設（内閣法第19条の２、第16条）

○　内閣官房に、サイバーセキュリティの確保に関する事務等を掌理する内閣サイバー官（次官級の特別職）一人を新たに置くこととする。

○　国家安全保障局次長を３人に増やすこととし、内閣サイバー官をもつて充てることとする。

☆　内閣サイバーセキュリティセンター（ＮＩＳＣ）の改組については、政令改正において措置。

その他③（その他関係法律の改正・施行日）

その他所要の改正（整備法第１条、第３条、第８条から第11条まで、第14条及び附則第５条）

強化法の施行に伴い、その他以下の法律を改正。

国家公務員法、特別職の職員の給与に関する法律、行政機関が行う政策の評価に関する法律 等（※）

（※）情報通信技術を活用した行政の推進等に関する法律、民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律、産業競争力強化法、情報通信技術を利用する方法による国の歳入等の納付に関する法律、デジタル庁設置法

検討規定（強化法附則第７条）

政府は、附則第１条第４号（注：通信情報の利用に係る規定）に掲げる規定の施行後３年を目途として、特別社会基盤事業者による特定侵害事象等の報告、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通信情報の取得、当該通信情報の取扱い等の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとする。

※　衆議院での修正項目

施行期日（強化法附則第１条、整備法附則第１条）

【強化法】一部を除き、公布の日から起算して１年６月を超えない範囲内において政令で定める日

☆　サイバー通信情報監理委員会の設置については１年を超えない範囲内において政令で定める日、通信情報の利用については一部を除き２年６月を超えない範囲内において政令で定める日。

【整備法】強化法の施行の日

☆　サイバーセキュリティ戦略本部の改組、内閣サイバー官の設置等については、６月を超えない範囲内において政令で定める日から施行。

国会における審議経過

令和7年2月7日（金）　サイバー対処能力強化法案及び同整備法案　閣議決定・国会提出

		審議時間（実績ベース）
衆議院		
3月18日（火）	本会議　趣旨説明質疑	
3月19日（水）	内閣委　提案理由説明、質疑①　2時間	
3月21日（金）	内閣委　質疑②　2時間45分	
3月26日（水）	内閣委　質疑③　3時間	
3月28日（金）	内閣委　参考人質疑	
4月2日（水）	内閣委　質疑④　7時間	計：21時間
4月3日（木）	内閣委、総務委、安全保障委　連合審査　3時間	
4月4日（金）	内閣委　質疑⑤　3時間	
	内閣委　質疑⑥　3時間15分（うち1時間15分　総理出席）	
	修正案説明、採決、附帯決議	
4月8日（火）	本会議　採決	
参議院		
4月18日（金）	本会議　趣旨説明質疑	
4月22日（火）	内閣委　提案理由説明、質疑①　1時間20分	
4月24日（木）	内閣委　質疑②　6時間	
5月8日（木）	内閣委　参考人質疑	
5月13日（火）	内閣委、総務委、外交防衛委　連合審査　2時間55分	計：18時間20分
	内閣委　質疑③　2時間50分	
5月15日（木）	内閣委　質疑④　5時間15分（うち1時間10分　総理出席）	
	採決、附帯決議	
5月16日（金）	本会議　可決・成立	
		総計：39時間20分

5月23日（金）　サイバー対処能力強化法及び同整備法　公布

資料1-3

参　考

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**。

【略】

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する。そのために、**サイバー安全保障分野における情報収集・分析能力を強化**するとともに、**能動的サイバー防御の実施のための体制を整備**することとし、以下の(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。

能動的サイバー防御を含むこれらの取組を実現・促進するために、**内閣サイバーセキュリティセンター（ＮＩＳＣ）を発展的に改組**し、**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**する。そして、**これらのサイバー安全保障分野における新たな取組の実現のために法制度の整備**、運用の強化**を図る**。

「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」について

「国家安全保障戦略」（令和４年12月16日閣議決定）に基づき、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べく、当該分野における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、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（令和６年６月６日内閣官房長官決裁）

有識者

（肩書きは令和６年11月29日時点）

上沼　紫野	LM虎ノ門南法律事務所弁護士
遠藤　信博	日本電気株式会社特別顧問
落合　陽一	筑波大学デジタルネイチャー開発研究センター長/准教授
川口　貴久	東京海上ディーアール株式会社主席研究員
川添　雄彦	日本電信電話株式会社代表取締役副社長 副社長執行役員 一般社団法人 電気通信事業者協会参与 一般社団法人 ICT-ISAC理事
酒井　啓亘	早稲田大学法学学術院教授
佐々江　賢一郎	公益財団法人 日本国際問題研究所理事長　【座長】
宍戸　常寿	東京大学大学院法学政治学研究科教授
篠田　佳奈	株式会社BLUE代表取締役
辻　伸弘	SBテクノロジー株式会社プリンシパルセキュリティリサーチャー
土屋　大洋	慶應義塾大学大学院政策・メディア研究科教授
野口　貴公美	一橋大学副学長、法学研究科教授
丸谷　浩史	株式会社日本経済新聞社常務執行役員 大阪本社代表 兼 名古屋支社代表
村井　純	慶應義塾大学教授
山岡　裕明	八雲法律事務所弁護士
山口　寿一	株式会社読売新聞グループ本社代表取締役社長
吉岡　克成	横浜国立大学大学院環境情報研究院/先端科学高等研究院教授

開催実績

6月7日　全体会合①：開催趣旨、現状説明
テーマ別会合①
6月19、20日 【イ：通信情報の利用】
7月1日 【ウ：アクセス・無害化】
7月3日 【ア：官民連携の強化】

7月8日　全体会合②：ヒアリング等（経済３団体）
テーマ別会合②
7月23日 【ア：官民連携の強化】
7月24日 【ウ：アクセス・無害化】
7月26日 【イ：通信情報の利用】

8月6日　全体会合③：これまでの議論の整理
テーマ別会合③
8月26日 【イ：通信情報の利用】
8月27日 【ウ：アクセス・無害化】
9月 2日 【ア：官民連携の強化】

11月29日　全体会合④：提言取りまとめ

※ テーマ別会合：国家安全保障戦略（ア）～（ウ）それぞれのテーマについて、関心の高い有識者を中心に集中的な議論を行う会合

基幹インフラ事業者とは

経済安全保障推進法

国民生活及び経済活動の基盤となる「特定社会基盤役務」の安定的な提供を確保するため、国が規制対象となる「特定社会基盤事業」「特定社会基盤事業者」「特定重要設備」を指定。

- ✓ **「特定社会基盤役務」**：国民生活及び経済活動の基盤となる役務であって、その安定的な提供に支障が生じた場合に国家及び国民の安全を損なう事態を生ずるおそれがあるもの
- ✓ **「特定社会基盤事業」**：対象１５事業（下表参照）のうち、特定社会基盤役務の提供を行うものとして政令で定めるもの
- ✓ **「特定社会基盤事業者」**：特定社会基盤事業を行う者のうち、その使用する特定重要設備の機能が停止し、又は低下した場合に、その提供する特定社会基盤役務の安定的な提供に支障が生じ、これによって国家及び国民の安全を損なう事態を生ずるおそれが大きいものとして主務省令で定める基準に該当する者
- ✓ **「特定重要設備」**：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

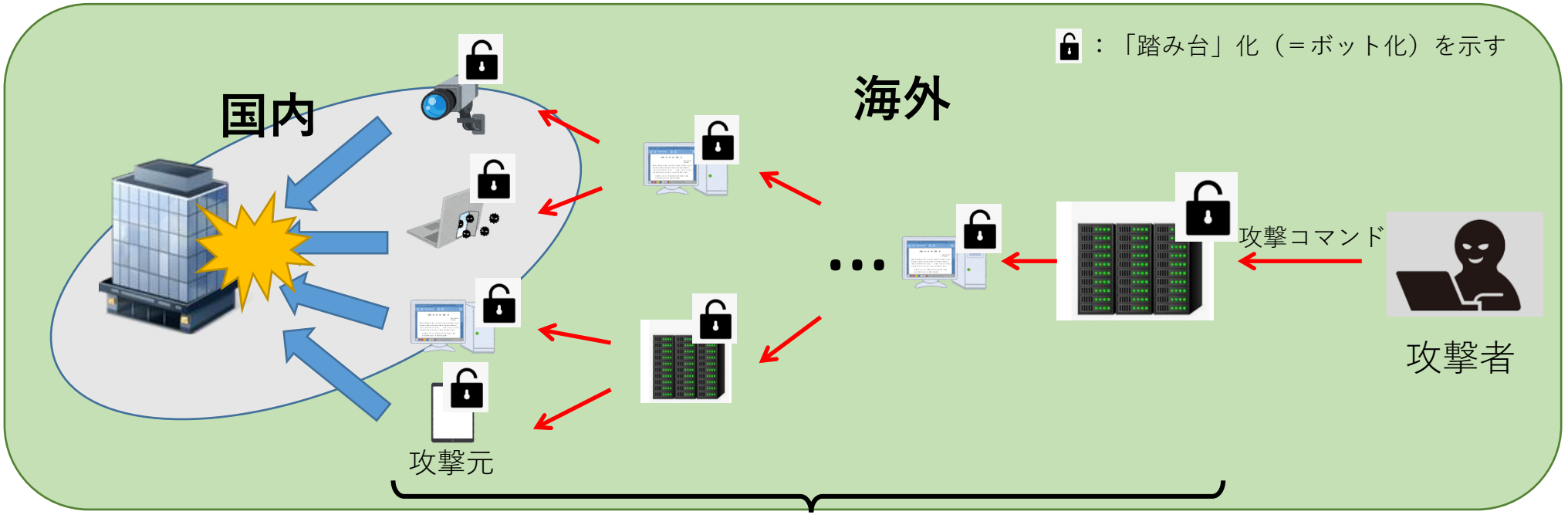
基幹インフラ制度の対象事業（特定社会基盤事業）　（計２５７者）

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）

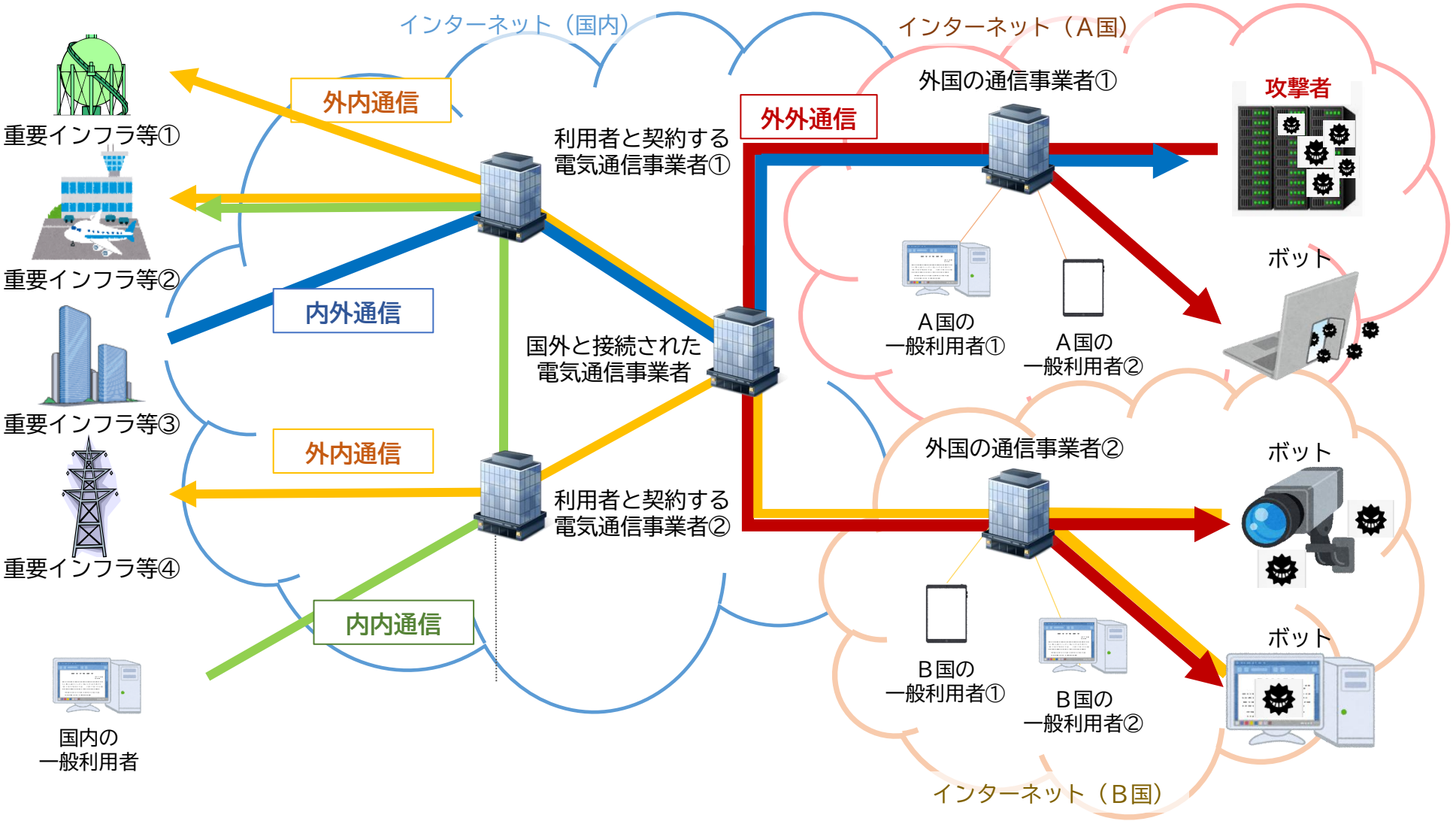
※ 経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第43号）
※ 内閣府「特定社会基盤事業者として指定した者（令和７年７月31日時点）」から作成
※ サイバーセキュリティ基本法の「重要社会基盤事業者（重要インフラ）」とは別概念

サイバー攻撃の手法

- サイバー攻撃は、「攻撃者が保有する機器」から直接行われるのではなく、「乗っ取られた機器」（いわゆる「踏み台」）を通じて行われる。
- 攻撃者は、身を隠すため、「踏み台」は一段ではなく何段も重ねて使う。
- 結果、被害者から見える攻撃元が「国内」であったとしても、「攻撃者」を追跡するうちに「海外にある踏み台」に辿り着くことが大宗。加えて、殆どの攻撃元が海外であることが実情。
- 「踏み台」を多数組み合わせ、攻撃コマンド一つで多様な攻撃ができるように準備された「攻撃インフラ」を「ボットネット」と、個々の踏み台を「ボット」と呼ぶ。

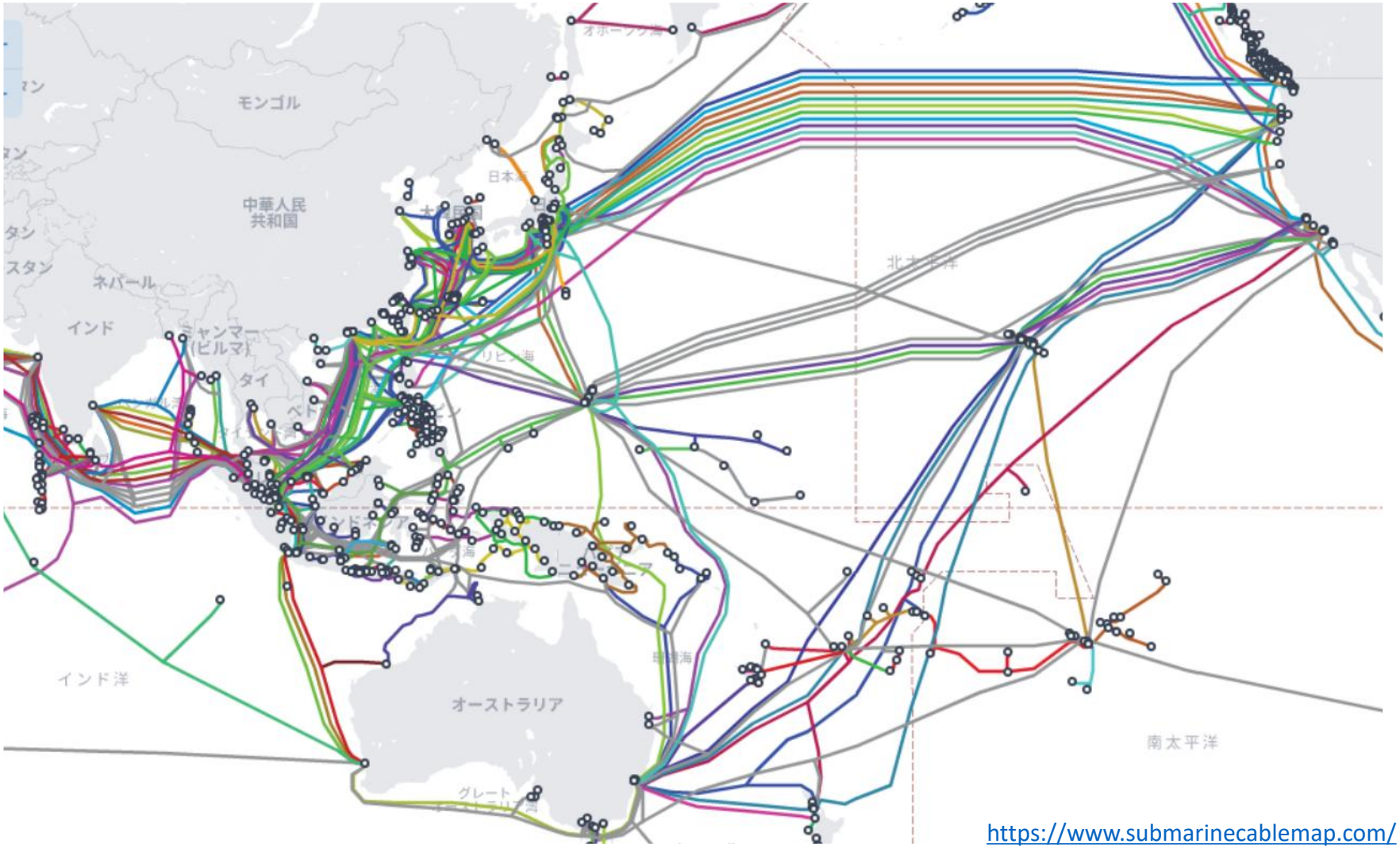


国外が関係する通信、関係しない通信



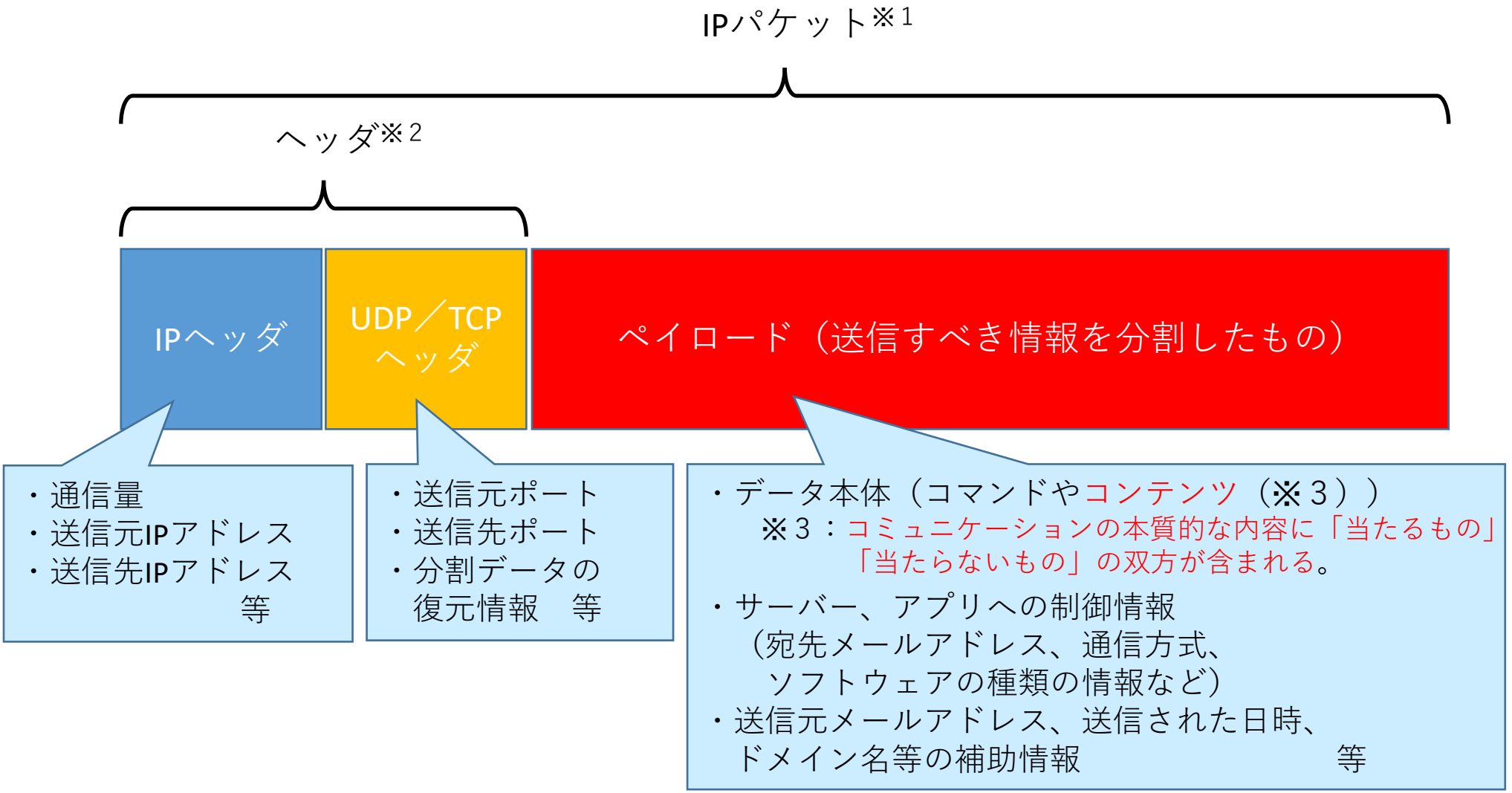
物理的な「インターネットのインフラ」

- 米国＝アジア間の通信は「太平洋を横断する海底ケーブル」を経由
- また日本が太平洋横断ケーブルの「ハブ」になっている ≒ 太平洋を横断する殆どの通信が「日本乗換」



https://www.submarinecablemap.com/より

インターネットを流れるデータの構造



※１：IPパケット自身に「受信日時」は含まれないが、いわゆる「ログ保存時」にその瞬間の日時を「受信日時」として記録

※２：「フロー情報」、「メタデータ」の語は、上記「ヘッダ」を指すことが多い

コミュニケーションの本質的な内容ではない情報の例

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 e3844A7D35300734D2BA 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

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」

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）
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 Content-Type: multipart/alternative ; boudary= "_Part_28873_0A61" 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 お世話になっております。 添付の至急ご確認をお願いします。 ○○花子　拝	本文 （実際には符号化されて伝送。 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 （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。 よろしくお願いします。 84 a7 f3 9b 61 c1 08 99 27 1d 44	添付ファイルの内容 （技術的には本文の一部）

受信側メールサーバ等が追加する情報

不正なコマンド
（通常は表示されない）

アクセス・無害化措置の実施の流れ

サイバー攻撃の実態を踏まえ、アクセス・無害化についての総論的な意思決定

国家安全保障会議（NSC）
※サイバー安全保障担当大臣・外務大臣・防衛大臣・国家公安委員長も参加

対処方針

個別のアクセス・無害化措置について、警察・自衛隊の役割分担等を検討・決定

内閣官房

サイバー安全保障担当大臣

指導

連携

新組織

内閣サイバー官（併）国家安全保障局次長

国家安全保障局

国家安全保障局長

個別のアクセス・無害化措置の執行（現場の指揮と監督責任は警察庁長官及び防衛大臣が負う）

サイバー安全保障担当大臣の下、内閣官房による強力な総合調整

警察・自衛隊（同一の建物で勤務するなど緊密に連携）

措置を承認

独立機関

措置が国際法上許容される範囲内のものかどうか確認

外務大臣

アクセス・無害化のステップ（イメージ）

① アクセス：

攻撃に使用されているサーバー等が持つ脆弱性を利用するなどして、遠隔からログインを実施。

※なお、当該サーバー等が攻撃者によって現に乗っ取られているような場合には、
（攻撃者自身が自ら侵入に利用した弱点を塞ぐことをしていない限り）
非正規の侵入手段が存在するものと想定される。

② 攻撃のためのプログラム等の確認：

インストールされているプログラム一覧、作動している攻撃のためのプログラム等を確認。

③ 無害化：

当該サーバー等が攻撃に用いられないよう無害化。

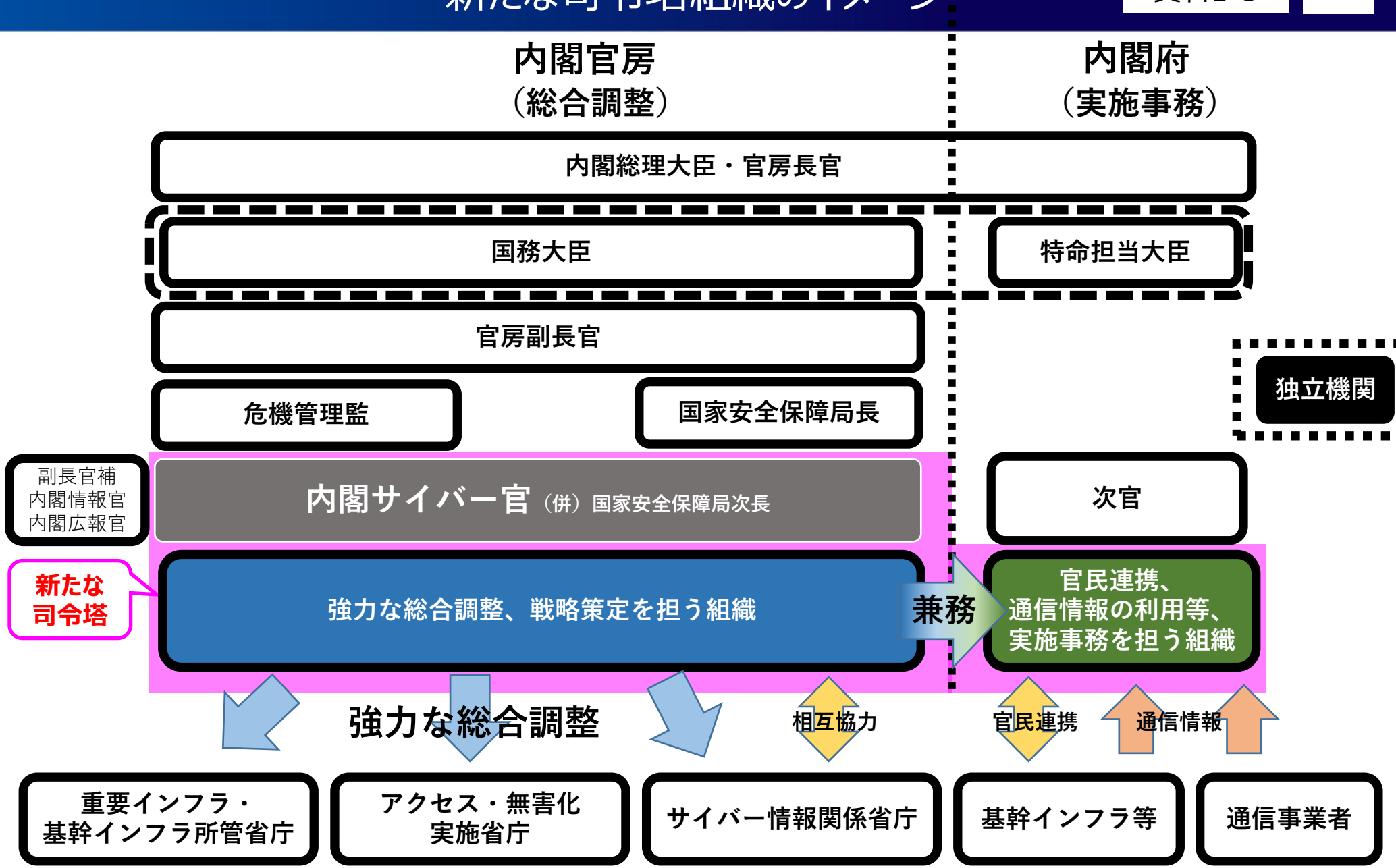
（無害化の方法の例）

- インストールされている攻撃のためのプログラムの停止・削除
- 攻撃者が当該サーバ等へアクセスできないよう設定変更　　など

上記措置を国外にあるサーバ等に対して行う場合、主権侵害に該当するとしても、「緊急状態*」等の国際法上の法理を援用するなどして、国際法上許容される範囲内で実施。

＊：緊急状態（Necessity）
当該措置が、重大かつ急迫した危険から不可欠の利益を守るための唯一の手段であり、相手国等の不可欠の利益を深刻に侵害しないといった一定の要件を満たす場合に、違法性が阻却されるという考え方。

新たな司令塔組織のイメージ



もっと詳しく知りたい方は

能動的サイバー防御

QRリンク先：
https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html