情報セキュリティワークショップ in 越後湯沢
～トラストレスなデジタル社会をどう生きるか～

サイバーセキュリティ対策と個人情報保護政策

令和７年10月11日

個人情報保護委員会 事務局 審議官
小川久仁子

自己紹介（略歴）

2011年～2013年
総務省総合通信基盤局消費者行政課企画官
2013年～2016年
電波政策課企画官
移動通信課移動通信企画官

2016年～2018年
個人情報保護委員会事務局参事官

2018年～2020年
総務省総合通信基盤局消費者行政第二課長
2020年～2022年
サイバーセキュリティ統括官付参事官
（総括担当）

2024年7月～
個人情報保護委員会事務局審議官（現職）
個人情報保護法の法制全般、個人情報保護法のいわゆる３年ごと見直しに関する検討
などを担当

個人情報保護委員会
事務局 審議官

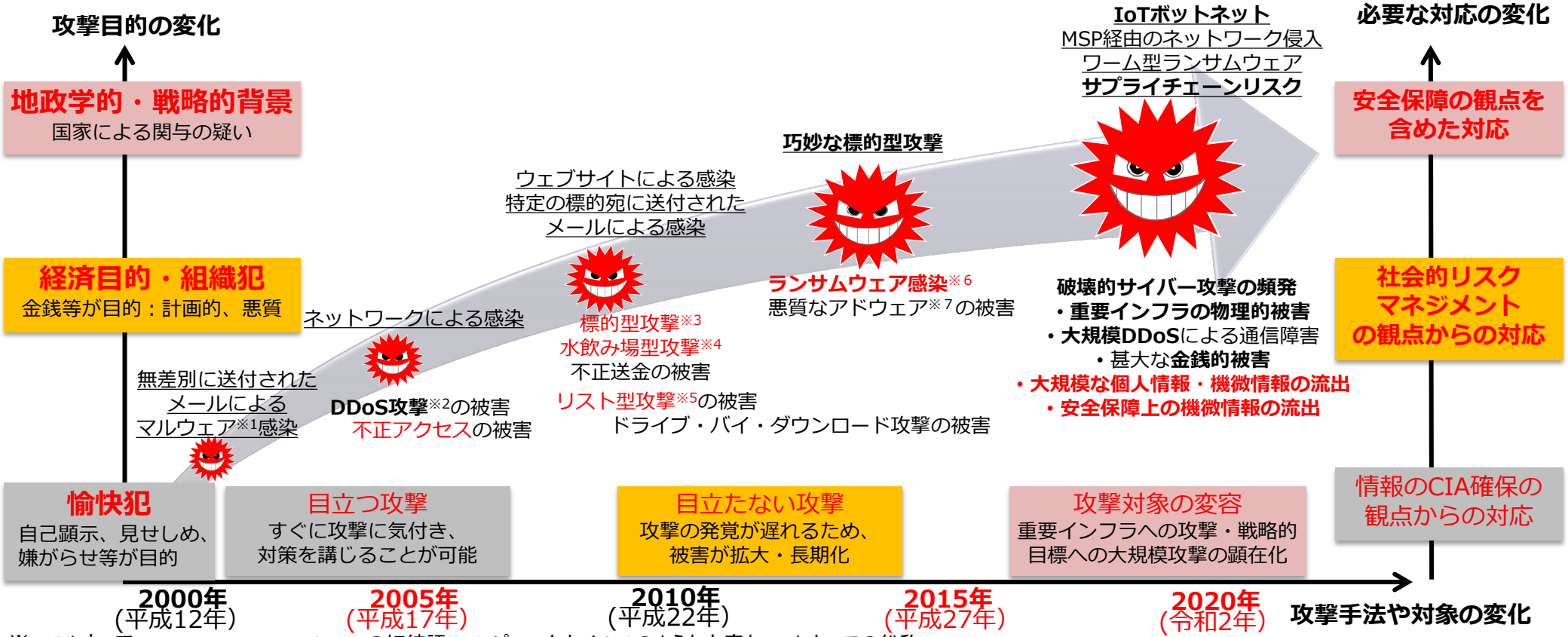
小川 久仁子
（情報処理安全確保支援士、CISSP）

目　次

１．サイバーセキュリティを巡る状況

サイバーセキュリティ上の脅威の増大

- ✓ サイバー空間が社会経済活動の基盤となる一方、**サイバーセキュリティ上の脅威は増大の一途**。
- ✓ サイバー攻撃の主体や目的の変化（愉快犯→金銭目的→地政学的・戦略的背景）、攻撃手法・対象の拡大などにより、サイバー攻撃は**悪質化・巧妙化し、その被害が深刻化**。



※1 マルウェア　Malicious softwareの短縮語。コンピュータウイルスのような有害なソフトウェアの総称。

※2 **DDoS攻撃**　分散型サービス妨害攻撃のこと。多数の端末から一斉に大量のデータを特定宛先に送りつけ、宛先のサーバ等を動作不能にする攻撃。

※3 標的型攻撃　機密情報等の窃取を目的として、特定の個人や組織を標的として行われる攻撃。

※4 水飲み場型攻撃　標的組織が頻繁に閲覧するウェブサイトで待ち受け、標的組織に限定してマルウェアに感染させ、機密情報等を窃取する攻撃。

※5 リスト型攻撃　不正に入手した他者のID・パスワードをリストのように用いてWebサービスにログインを試み、個人情報の窃取等を行う攻撃。

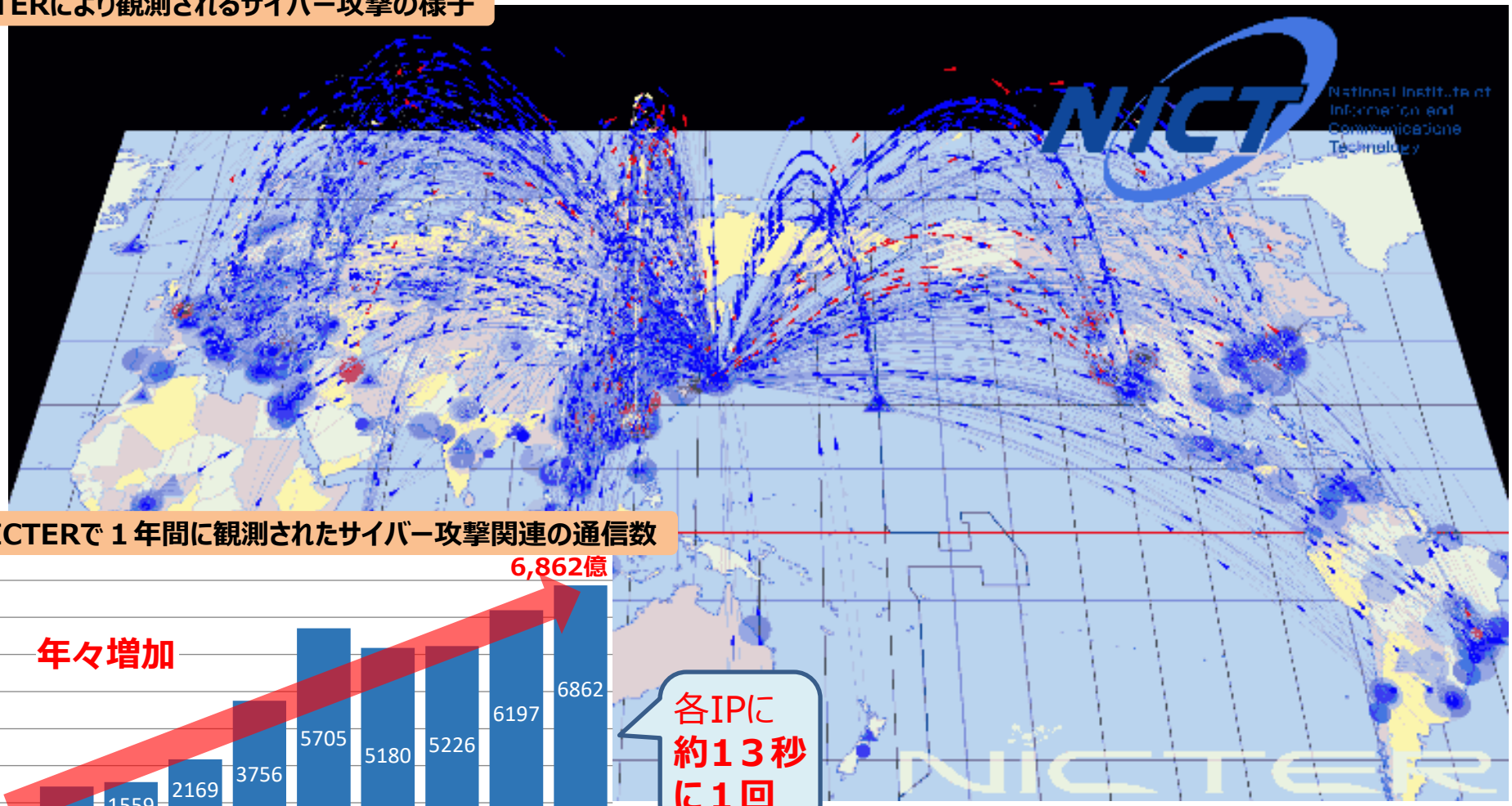
※6 **ランサムウェア**　身代金要求型ウイルスのこと。感染端末上にある文書などのファイルが暗号化され、暗号解除のためには金銭を要求される。

※7 アドウェア　広告表示によって収入を得るソフトウエアの総称。狭義には、フリーウエアと共にインストールされ、ブラウザー利用時に広告を自動的に付加するソフト

IoT機器を狙った攻撃の情勢（NICTERによる観測）

➢ 国立研究開発法人情報通信研究機構（**NICT**）では、大規模サイバー攻撃観測網である**NICTERにおいて、未使用のIPアドレス30万個（ダークネット）を活用**し、グローバルに**サイバー攻撃の状況を観測。**

NICTERにより観測されるサイバー攻撃の様子



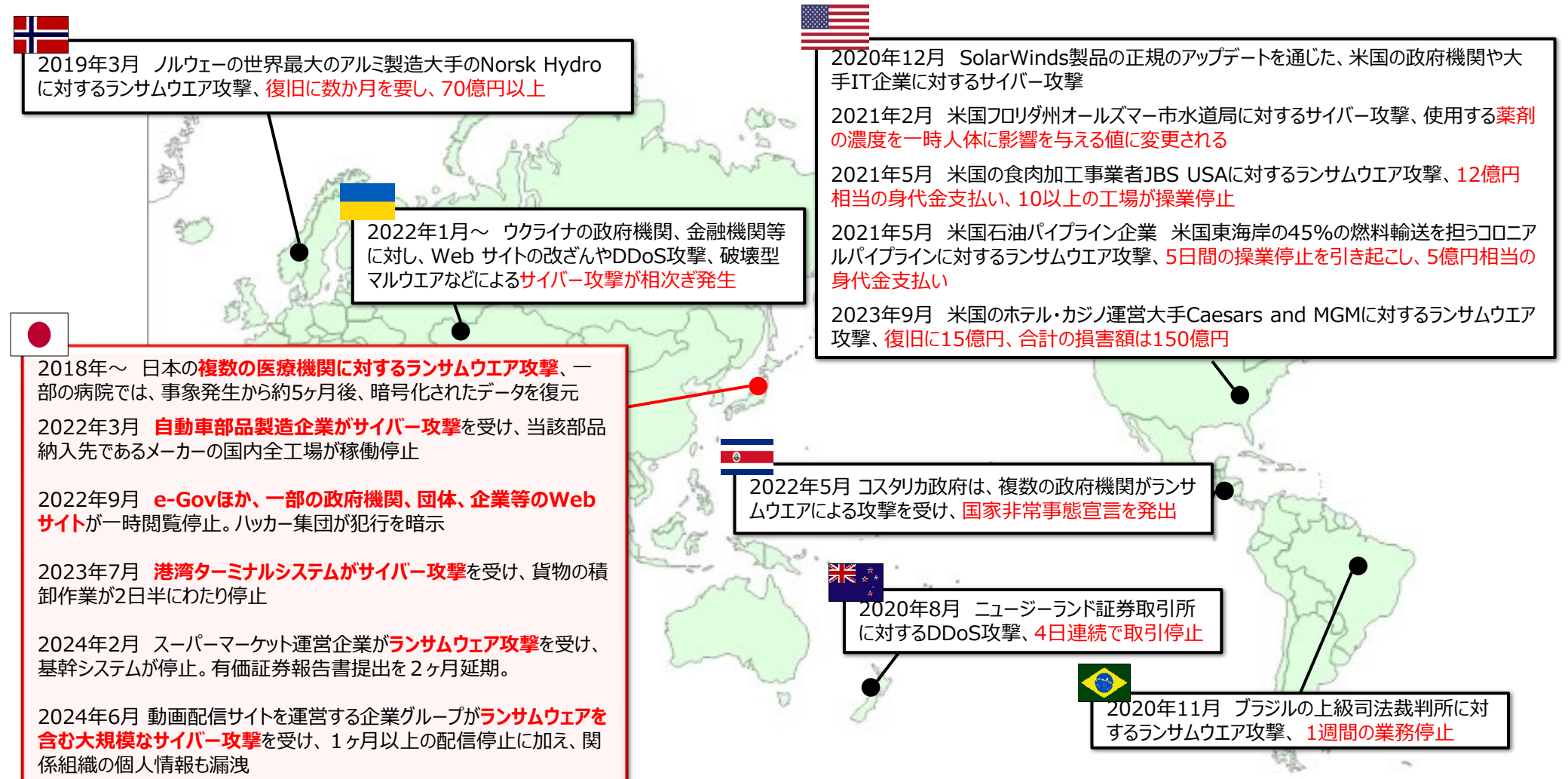
※1IPアドレス当たり
年間約243万パケット

NICTERで１年間に観測されたサイバー攻撃関連の通信数

※2020年は特異的な事象（大規模なバックスキャッタや大量の調査スキャン）が観測されたため、例外的にパケット数が多かったものと推測

（参考）世界における主なサイバー攻撃等

海外のみならず、近年我が国でも深刻なサイバー事案が発生



2019年3月　ノルウェーの世界最大のアルミ製造大手のNorsk Hydroに対するランサムウエア攻撃、復旧に数か月を要し、70億円以上

2022年1月～　ウクライナの政府機関、金融機関等に対し、Web サイトの改ざんやDDoS攻撃、破壊型マルウエアなどによるサイバー攻撃が相次ぎ発生

2020年12月　SolarWinds製品の正規のアップデートを通じた、米国の政府機関や大手IT企業に対するサイバー攻撃

2021年2月　米国フロリダ州オールズマー市水道局に対するサイバー攻撃、使用する薬剤の濃度を一時人体に影響を与える値に変更される

2021年5月　米国の食肉加工事業者JBS USAに対するランサムウエア攻撃、12億円相当の身代金支払い、10以上の工場が操業停止

2021年5月　米国石油パイプライン企業　米国東海岸の45%の燃料輸送を担うコロニアルパイプラインに対するランサムウエア攻撃、5日間の操業停止を引き起こし、5億円相当の身代金支払い

2023年9月　米国のホテル・カジノ運営大手Caesars and MGMに対するランサムウエア攻撃、復旧に15億円、合計の損害額は150億円

2018年～　日本の**複数の医療機関に対するランサムウエア攻撃**、一部の病院では、事象発生から約5ヶ月後、暗号化されたデータを復元

2022年3月　**自動車部品製造企業がサイバー攻撃**を受け、当該部品納入先であるメーカーの国内全工場が稼働停止

2022年9月　**e-Govほか、一部の政府機関、団体、企業等のWebサイト**が一時閲覧停止。ハッカー集団が犯行を暗示

2023年7月　**港湾ターミナルシステムがサイバー攻撃**を受け、貨物の積卸作業が2日半にわたり停止

2024年2月　スーパーマーケット運営企業が**ランサムウェア攻撃**を受け、基幹システムが停止。有価証券報告書提出を２ヶ月延期。

2024年6月 動画配信サイトを運営する企業グループが**ランサムウェアを含む大規模なサイバー攻撃**を受け、１ヶ月以上の配信停止に加え、関係組織の個人情報も漏洩

2024年末～2025年当初　**航空運送事業者・金融機関・通信事業者等に対してサイバー攻撃が行われ、一部のサービスの提供に支障**が出るなどの影響が生じる事例が発生

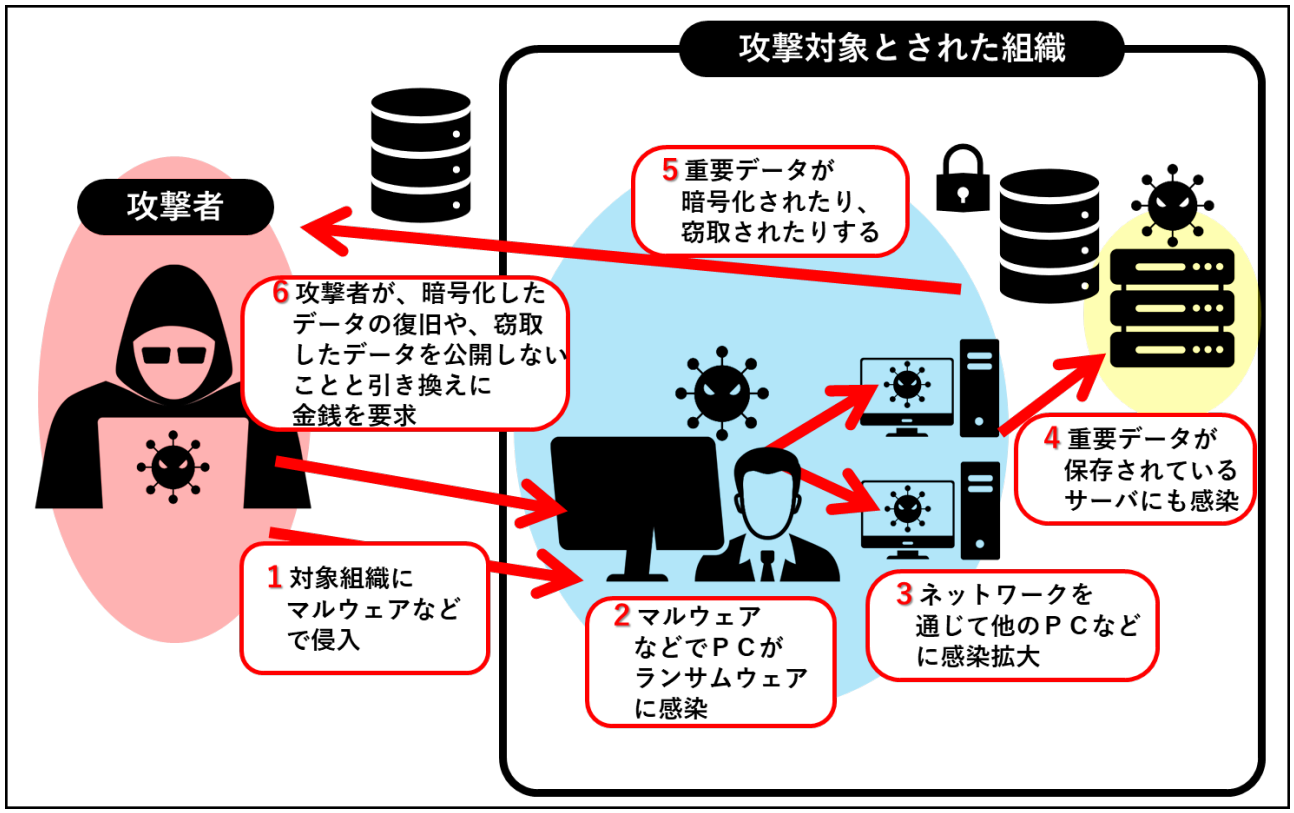
2022年5月 コスタリカ政府は、複数の政府機関がランサムウエアによる攻撃を受け、国家非常事態宣言を発出

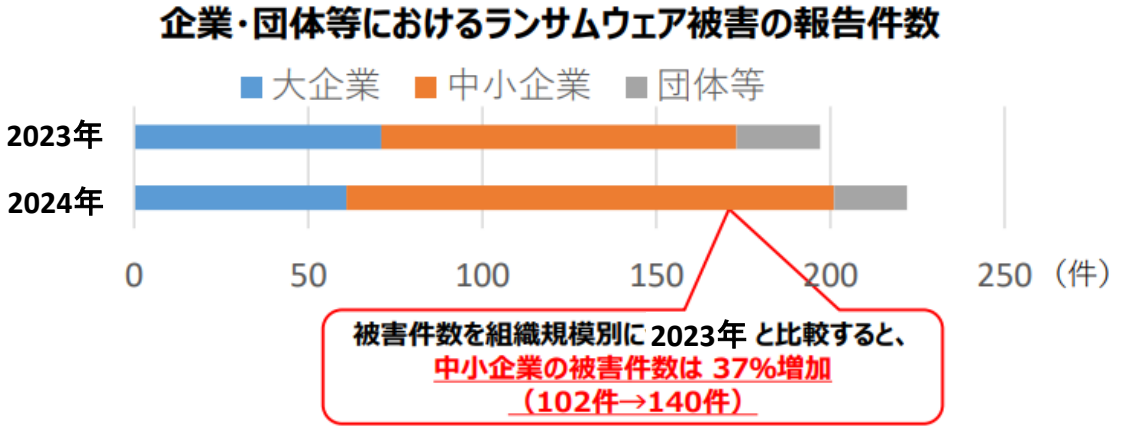
2020年8月　ニュージーランド証券取引所に対するDDoS攻撃、4日連続で取引停止

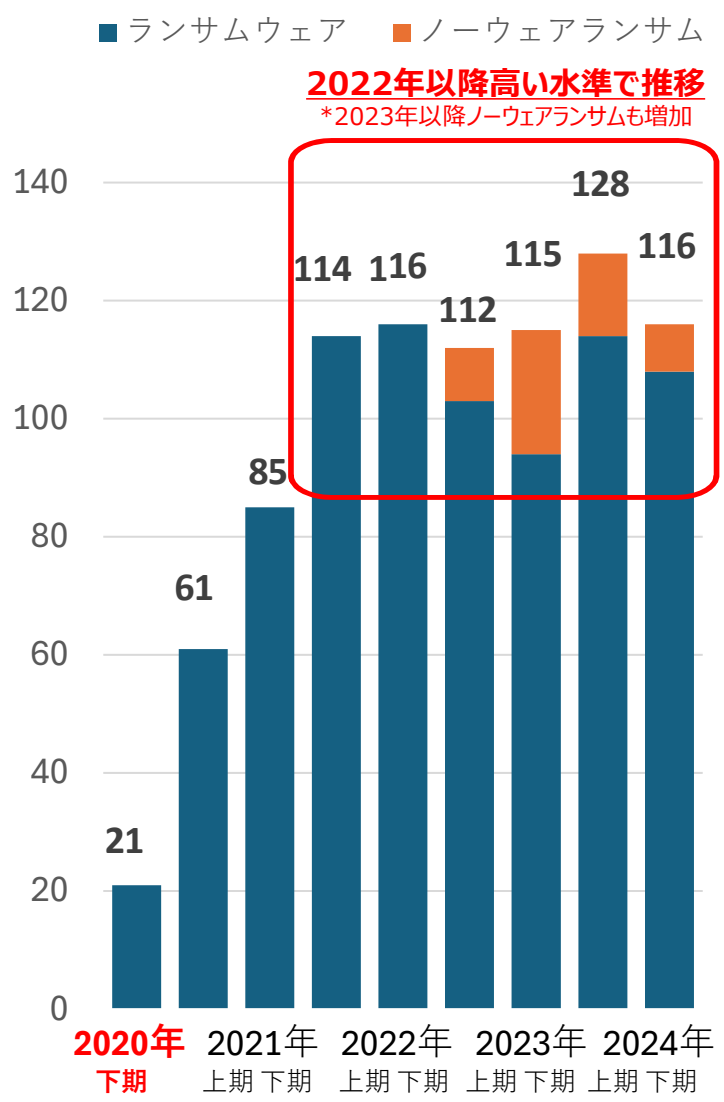
2020年11月　ブラジルの上級司法裁判所に対するランサムウエア攻撃、 1週間の業務停止

2022年2月　米国の衛星通信企業 Viasatがサイバー攻撃を受け、欧州や中東地域で数時間の通信障害が発生、 完全に回復するまでに数日を要し、ドイツの風力発電所が停止する等の影響

サイバー攻撃の動向: ランサムウェア攻撃







出典：警察庁サイバー警察局「令和6年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3月）」、「令和5年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6年3月）」を基に作成

「サイバーセキュリティ」の定義

サイバーセキュリティ基本法（平成26年法律第104号）

（定義）
第2条　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。

国家安全保障戦略（抜粋）（令和４年12月16日 閣議決定）

Ⅵ　我が国が優先する戦略的なアプローチ
２　戦略的なアプローチとそれを構成する主な方策
⑷　我が国を全方位でシームレスに守るための取組の強化
ア　サイバー安全保障分野での対応能力の向上

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。 具体的には、まずは、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。（略）

その上で、**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。
これらの取組は総合的な防衛体制の強化に資するものとなる。

能動的サイバー防御に関する法の全体像

- 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（第10章）　等

→ □ 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

（出典）サイバーセキュリティ戦略本部第1回会合資料3-3（令和7年7月1日） https://www.nisc.go.jp/pdf/council/cs/n01/01document3-3.pdf

（参考）法における組織・体制整備（変更点）

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予定

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

政府全体のサイバーセキュリティ推進体制

※令和７年７月１日時点

内 閣

- 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（サイバー対処能力強化法第３条に基づき今後策定）
- サイバーセキュリティ戦略（令和３年９月28日閣議決定）
- 国家安全保障戦略（令和４年12月16日国家安全保障会議・閣議決定）

サイバーセキュリティ推進専門家会議 ⇄ 意見聴取

サイバーセキュリティ戦略本部
本部長：内閣総理大臣
副本部長：内閣官房長官、サイバー安全保障担当大臣
本部員：全大臣

意見 ← **国家安全保障会議（NSC）**

内閣官房　国家サイバー統括室
内閣サイバー官（併）国家安全保障局次長
〔CS戦略本部事務局、総合調整〕

緊密連携 ⇄ **国家安全保障局（NSS）**

総合調整 ↓

＜全府省庁＞
〔自組織・所管独立行政法人等のセキュリティ確保の推進〕

＜サイバーセキュリティ政策推進省庁＞
〔所掌に基づくサイバーセキュリティ施策の実施〕

- 内閣府（経済安全保障）
- 警察庁（治安の確保）
- デジタル庁（デジタル社会形成）
- 総務省（通信・ネットワーク政策）
  - － NICT（(国研)情報通信研究機構）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
  - － IPA（(独)情報処理推進機構）
- 防衛省（国の防衛）
- 文部科学省（セキュリティ教育）

重要インフラ所管省庁

- 金融庁（金融）
- 総務省（政府・行政サービス、情報通信）
- 厚生労働省（医療）
- 経済産業省（電力、ガス、化学、クレジット、石油）
- 国土交通省（鉄道、航空、物流、水道、空港、港湾）

（出典）サイバーセキュリティ戦略本部第1回会合資料3-3（令和7年7月1日） https://www.nisc.go.jp/pdf/council/cs/n01/01document3-3.pdf

（参考）サイバーセキュリティ戦略（2021年9月閣議決定）

2020年代を迎えた日本を取り巻く時代認識　：　「ニューノーマル」とデジタル社会の到来

- デジタル経済の浸透、**デジタル改革**の推進
- **新型コロナウイルス**の影響・経験 テレワーク、オンライン教育等の進展
- 厳しさを増す**安全保障**環境
- **SDGｓ**への デジタル技術の貢献期待
- **東京オリンピック・パラリンピック**に向けて行ってきた取組

サイバー空間をとりまく課題認識　：　国民全体のサイバー空間への参画

- サイバー空間は、国民全体等**あらゆる主体が参画し公共空間化**
  サイバー・フィジカルの垣根を超えた各主体の相互連関・連鎖の深化
  攻撃者に狙われ得る弱点にも
- 地政学的緊張を反映 **国家間競争**の場に 安全保障上の課題にも
- 不適切な利用は 国家分断、人権の阻害へ
- 官民の取組の 活用

あらゆる主体にとってサイバーセキュリティの確保は自らの問題に
５つの基本原則※は堅持

「Cybersecurity for All」
～誰も取り残さないサイバーセキュリティ～

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進

安全保障の観点からの取組強化

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

「自由、公正かつ安全なサイバー空間」の確保

※情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携

新たなサイバーセキュリティ戦略の方向性

- サイバー空間を取り巻く切迫した情勢や社会全体へのDXの浸透等に対応するとともに、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べく、中長期的に政府が取り組むべきサイバーセキュリティ政策の方向性を広く内外に示すため、５年の期間を念頭に、**新たな「サイバーセキュリティ戦略」を年内を目途に策定。**

深刻化するサイバー脅威に対する防止・抑止の実現	幅広い主体による社会全体のサイバーセキュリティ向上	我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成
• 巧妙化・高度化や、国家背景のキャンペーン等により、サイバー脅威が国民生活・経済活動及び安全保障に深刻かつ致命的な影響を及ぼす恐れ • 被害が生じる前の脅威の未然排除、事案発生後の的確な対処を含め、安全保障の観点も踏まえた実効的な防止・抑止の実現が急務	• DXの浸透により、あらゆる主体がサイバー攻撃の標的となり、直接的な被害にとどまらず、更なる攻撃に悪用される恐れ • 社会全体のサイバーセキュリティ向上に向けて、幅広い主体に対し、リスクや能力を踏まえ、適切な対策を求めていくことで、社会全体のサイバーセキュリティ向上を図る必要	• 人口減少に伴い、官民を通じて、サイバーセキュリティ人材の不足が深刻化する恐れ • AIや量子技術等、技術革新が進展する一方、サイバーセキュリティに関する技術の多くを海外に依存
施策の方向性		
• 新たな司令塔組織（国家サイバー統括室）を中心に、官民連携・国際連携の下、安全保障の観点も踏まえ、能動的サイバー防御を含む多様な手段を組み合わせた総合的な対応方針・体制の確立・実行	• 政府機関等が範となり、地方公共団体・重要インフラ事業者のみならず、製品ベンダー・中小企業・個人等まで様々な主体に求められる対策及び実効性確保に向けた方策の明確化・実施	• 産官学を通じたサイバーセキュリティ人材の確保・育成・裾野拡大 • 研究・開発から実装・運用まで、産官学の垣根を越えた協働による、国産技術を核とした、新たな技術・サービスを生み出すエコシステムを形成
目指すべき姿		

広く国民・関係者の理解と協力の下、国がサイバー防御の要となり、官民一体で我が国のサイバーセキュリティ対策を推進

（出典）サイバーセキュリティ戦略本部第１回会合資料１（令和7年7月1日） https://www.nisc.go.jp/pdf/council/cs/n01/01document1.pdf

「ICTサイバーセキュリティ政策の中期重点方針」（令和6年7月31日公表）

➢ 総務省では、令和６年１月から「**ICTサイバーセキュリティ政策分科会**」（主査：後藤厚宏　情報セキュリティ大学院大学学長）を開催し、総務省が取り組むべき**サイバーセキュリティ政策について、2030年頃も見据えた中長期的な方向性**について検討。

【政府の主な動き】

- **国家安全保障戦略**
- **経済安全保障推進法の施行（特定社会基盤事業者の指定等）　等**

【サイバーセキュリティを巡る主な課題】

- **厳しさを増す国際情勢とサイバー攻撃リスクの高まり**
- **多様化・複雑化するサプライチェーンとアタックサーフェス（攻撃対象領域）の増加**
- **セキュリティ人材の確保**
- **生成AI等の新たな技術への対応**

１．重要インフラ等におけるサイバーセキュリティの確保

- **通信分野（総合的なIoTボットネット対策（新NOTICEの推進やC&Cサーバの検知・対処能力の向上）**、スマートフォンアプリのセキュリティ対策やサプライチェーン対策の推進等）
- 放送分野（安全・信頼性に関する新たな技術基準に基づくセキュリティ対策の着実な推進等）
- 自治体分野（クラウド化・標準化等の環境変化を見据えた人材育成やCSIRT能力向上の取組等）
- クラウドセキュリティの確保やトラストサービス（eシールの認定制度を2024年度中に創設等）の推進

２．サイバー攻撃対処能力の向上と新技術への対応

- **CYNEX・CYXROSSを強力に推進し、国産のサイバーセキュリティ製品・技術による自律的なサイバーセキュリティ情報**の収集・分析力を抜本的に強化
- **CYXROSSとGSOCとの連携により政府システムの一元的な監視体制の構築**に貢献
- **CYDER等を通じた国や地方公共団体等におけるCSIRT対処能力**の抜本的強化
- サイバーセキュリティ研究分野の国際競争力向上を図るため、NICT内に米国等との連携を強化するための結節点を形成
- **生成AI等の新技術への対応**（AIを起因とするセキュリティリスクの回避・低減に向けた取組、AIを活用したサイバーセキュリティ対策の促進、耐量子計算機暗号技術（PQC）等の研究開発等の推進）

３．地域をはじめとするサイバーセキュリティの底上げに向けた取組

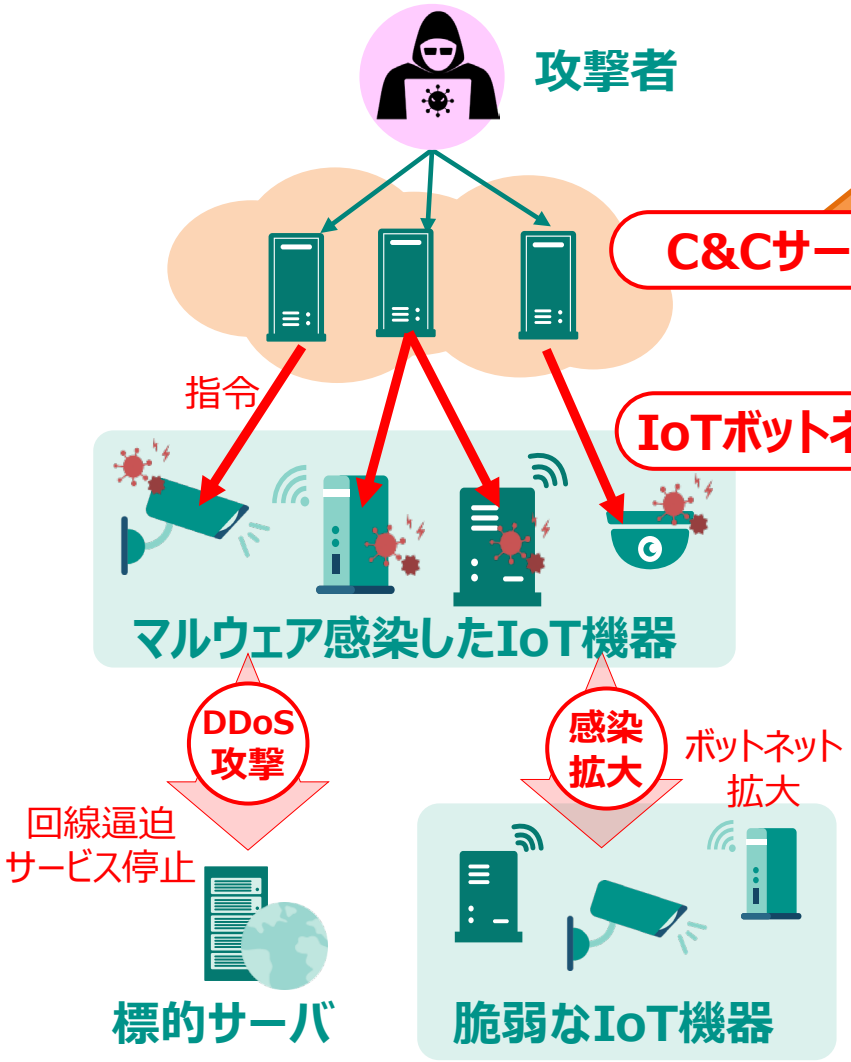
- 地域SECUNITYの活動強化（他機関との更なる連携、持続的な推進体制の整備等）
- 各種ガイドラインの周知啓発等

４．国際連携の更なる推進（国際連携全般、人材育成支援）

- 日ASEANサイバーセキュリティ能力構築センター（AJCCBC）の活動強化（プログラムの拡充、有志国との連携強化等）
- 大洋州島しょ国向け人材育成支援プロジェクトの2025年度以降の本格的な実施

IoT機器を悪用したサイバー攻撃への対策

- IoT機器の急増に伴い、**IoT機器を悪用**した大規模なサイバー攻撃（**DDoS攻撃**等）が発生
- DDoS攻撃は**ネットワーク全体の速度低下**を引き起こしかねないほか、**標的側での対応が難しい**
- 総務省・ISP等が協力して、攻撃指令を行う**C&Cサーバ**と、攻撃役となる**脆弱なIoT機器**の両面から対策



IoTボットネットに対して指令通信を出す C&Cサーバへの対処

電気通信事業者がネットワークの管理のために利用する「**フロー情報**※」を**分析**することで、**C&Cサーバを検知**
→ 対策に活用するための**実証事業を実施中**

※IPアドレス、ポート番号、プロトコル、パケット数などに関する情報
ヘッダー情報のみでペイロード（データの本体部分）は含まない

マルウェアに感染した/感染する危険性が高い 脆弱なIoT機器への対処

サイバー攻撃に悪用されるおそれのある**IoT機器を調査**し、
（サイバーセキュリティに知見のあるNICTにおいて調査を実施）
電気通信事業者を通じ、**IoT機器の利用者に注意喚起**

＜調査＆注意喚起の対象＞

① 既にマルウェアに感染している機器
② ファームウェアの脆弱性等がある機器
③ ID・パスワードの設定に脆弱性がある機器

→「**NOTICE**」プロジェクト NOTiCE

（参考）2025年７月のNOTICE実施状況

みんなで守る、IoT。
NOTiCE

\ あなたのルーターが、乗っ取られる前に。 /

さあ！
ネットにも戸締まりを。

IoT機器観測総数

月**1.24**億件

参加インターネットサービスプロバイダ（ISP）のIPアドレスに対して観測している総数

容易に推測可能なID・パスワードであるIoT機器

月**14,370**件

容易に推測可能なIDやパスワードを使用しているため、攻撃者によって管理権限を乗っ取られたり、サイバー攻撃に加担させられる危険性がある機器

ファームウェアに高リスク脆弱性を有するIoT機器

月**2,865**件

第三者に不正利用される危険性があるファームウェア脆弱性を有するIoT機器

マルウェア感染IoT機器検知数

最大**1,024**件/日

Miraiに既に感染していると推定されるIoT機器。サイバー攻撃に加担させられている可能性がある。

※IPアドレスが変動している場合は、重複して計上している場合があります
※当月1日あたりの最大値を掲載しています

リフレクション攻撃の踏み台にされうるIoT機器

月**15,353**件

リフレクション攻撃の踏み台にされうる可能性のあるIoT機器だと検知した数

政府端末情報を活用した脅威情報の収集・分析『CYXROSS』

- 我が国におけるサイバーセキュリティ対策は海外由来の製品に依存しているため、サイバー安全保障の観点から、国内でセキュリティ製品の創出を行い、国内の製品でサイバー攻撃に対応できる体制を整備する必要がある。
- **安全性や透明性の検証が可能なセンサーを政府端末に導入してサイバーセキュリティ情報を収集し、国立研究開発法人情報通信研究機構（NICT）の能力を活用して分析**する実証事業を実施。
- NICTが開発した様々な技術や観測等で蓄積したデータも活用し、我が国独自のサイバーセキュリティに関する情報を生成。

安全性・透明性を検証可能なセンサー(ソフトウェア)を開発し政府端末に導入

サイバー脅威

サイバー脅威

サイバー脅威

収集した情報をNICTに集約

・検体情報
・アラート情報
・端末情報　等

分析結果を各省庁等に提供

・検体分析結果
・攻撃傾向の統計情報
・サイバー脅威情報(IoC) 等

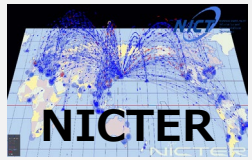
我が国独自のサイバー情勢分析能力を強化
政府システムのセキュリティ対策を強化

NICTの能力強化

NICT
情報通信研究機構

情報分析

NICTが開発したサイバーセキュリティ技術及び蓄積してきたデータ等を活用



サイバー攻撃観測技術

標的型攻撃観測・分析技術

サイバー攻撃情報統合分析技術

AIとサイバーセキュリティ

- あらゆる分野において生成AIの実装が急速に進んでいる一方で、生成AIを巡るリスクとして、偽誤情報の拡散、プライバシーの侵害、知的財産権の侵害等に加えて、サイバー攻撃への悪用等によるサイバーセキュリティのリスクが新たに指摘されている。
- 他方、サイバー攻撃の大規模化・複雑化・巧妙化に伴い、サイバーセキュリティ対策の業務負荷が課題となっている中、サイバー攻撃対策への生成AI等の利活用が期待されている。
- こうした背景を踏まえ、生成AI等のAI技術を巡る最新動向を把握しつつ、AIに起因するセキュリティリスクを可能な限り回避・低減するための「Security for AI」に取り組むとともに、AIをセキュリティ対策に効果的に活用するための「AI for Security」に取り組むことが必要。

生成AIの負の影響

サイバー攻撃に悪用される可能性

（例）
- 生成AI利用によるフィッシングメールの巧妙化
- マルウェアの生成、亜種の大量生産

生成AIへのサイバー攻撃・脆弱性内包

（例）
- リスクにつながる悪意のある入力
- LLMの学習データの汚染
- 事業者設定ミスによる安全ではない出力処理

Security for AI

安心安全な利用の促進

① 生成AIの進展によるサイバーセキュリティへの影響に係る調査・検証
- 生成AI等がサイバーセキュリティに与える負の影響の検証・評価
- AIの安心・安全な開発・提供に向けたセキュリティのガイドラインの策定

＜実例検証＞

② 米国専門機関とのAI安全性に関する共同研究事業
- AIの安全性に係る分野の研究開発を推進するため、北米にNICTの研究拠点を構築し、米国等の様々な専門機関との共同研究事業を実施

＜理論研究＞

生成AIの正の影響

サイバー攻撃対策への活用の可能性

（例）
- サイバー防御の自動化
- セキュリティレポート作成の自動化
- 脅威インテリジェンスの精度向上
- 脆弱性のない安全なコード開発の支援
- サイバー攻撃の予見
- インシデント対応の支援

AI for Security

サイバーセキュリティ対策への活用

③ AIを用いたサイバー脅威情報収集・分析の高度化
- 世界中の様々な機関等から発信されるサイバー脅威情報をAIを活用して収集・分析するための技術を開発及び展開

＜平時の分析活動＞

④ 生成AI等を活用した重要インフラ分野におけるサイバーセキュリティ対策強化
- 生成AI等を活用した攻撃インフラ分析の精緻化・迅速化の検証
- 当該情報等を用いた対処オペレーション業務の効率化・迅速化の検証とノウハウの展開

＜攻撃インフラ特定＞

２．安心安全なデータ利活用に向けた個人情報保護政策

(1)個人情報保護法の概要
(2)個人データの安全管理措置
　/漏えい等報告
(3)いわゆる３年ごと見直しについて

個人情報保護法の目的・構成

- **「個人情報」の適正な取扱いに関し、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする法律。**
- **我が国の個人情報保護制度の「基本法」として基本理念、基本方針の策定や国等の責務等を定めるほか、民間事業者や行政機関等の個人情報の取扱いに関する「一般法」として民間部門及び公的部門における必要最小限の規律を定める。**
- **また、個人情報保護委員会の設置根拠や民間部門及び公的部門に対する監視・監督権限についても定める。**

（目的）
第１条　この法律は、デジタル社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、**個人情報の適正な取扱い**に関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにし、**個人情報を取り扱う事業者及び行政機関等についてこれらの特性に応じて遵守すべき義務等を定める**とともに、**個人情報保護委員会を設置する**ことにより、**行政機関等の事務及び事業の適正かつ円滑な運営を図り、並びに個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的**とする。

構成

第１章 総則
第２章 国及び地方公共団体の責務等
第３章 個人情報の保護に関する施策等
第４章 個人情報取扱事業者等の義務等
第５章 行政機関等の義務等
第６章 個人情報保護委員会
第７章 雑則
第８章 罰則

個人情報保護法の成立と改正経緯

2003年（平成15年）　個人情報保護法等※ 成立　2005年（平成17年）4月全面施行

※　その他、行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号。行個法）、独立行政法人等の保有する個人情報の保護に関する法律（同第59号。独個法）、情報公開・個人情報保護審査会設置法（同第60号）、行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律（同第61号）

法施行後約10年が経過。情報通信技術の発展により、制定当時には想定されなかったパーソナルデータの利活用が可能に

2014年（平成26年）　特定個人情報保護委員会　設置

2015年（平成27年）　個人情報保護法 改正※　2017年（平成29年）5月全面施行

2016年（平成28年）　個人情報保護委員会　設置（民間部門の一元化）

３年ごと見直し規定に基づき、国際的動向、情報通信技術の進展、新産業の創出・発展の状況等を勘案して検討・措置

2020年（令和２年）　個人情報保護法 改正　2022年（令和４年）４月全面施行

2021年（令和３年）　個人情報保護制度の官民一元化※　2022年（令和４年）４月一部施行
2023年（令和５年）４月全面施行

※　デジタル社会の形成を図るための関係法律の整備に関する法律（令和3年法律第37号）による個人情報保護法の改正、行個法及び独個法の廃止等

（参考）個人情報保護法制整備の背景

我が国における官・民通ずるIT社会の急速な進展

公的部門
- 電子政府・電子自治体の構築

民間部門
- 電子商取引の進展
- 顧客サービスの高度化　等

国際的な情報流通の拡大・IT化

OECD
　ほとんどの国で民間部門を対象にした法制を整備

情報の自由な流通とプライバシー保護の確保　→　制度間の調和の要請

IT社会の「影」

・プライバシー等の個人の権利利益侵害の危険性・不安感増大

官・民における個人情報保護法制の確立

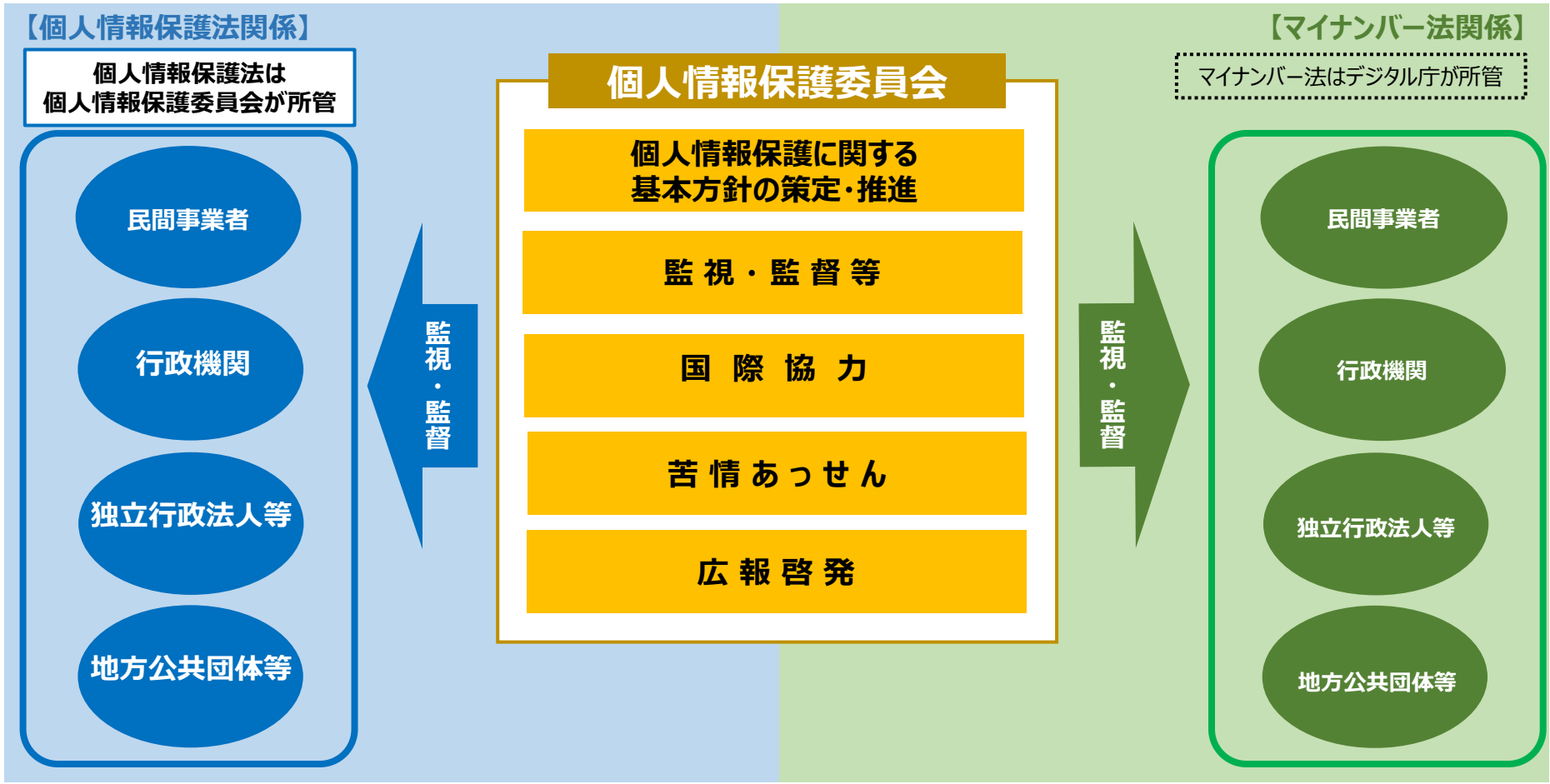
→　保護と利用の調和

- 基本理念
- 国及び地方公共団体の責務、施策
  → 基本法制（第１～３章）
- 民間事業者が遵守すべき規律
  → 基本法制（第４章）
- 公的機関（国・独立行政法人・地方公共団体等）が遵守すべき規律
  → ・行政機関法制
  ・独立行政法人法制
  ・条例

出典：個人情報保護法制整備の背景―内閣府（https://www.cao.go.jp/consumer/doc/100805_shiryou2-1-1.pdf）

個人情報保護委員会とは

- 個人情報保護委員会は、**個人情報の保護に関する法律**（平成15年法律第57号）に基づき、**個人情報の有用性に配慮**しつつ、**個人の権利利益を保護**するため、**個人情報の適正な取扱いの確保**を図ることを任務として設立された合議制の独立機関。
- いわゆる三条委員会であり、権限の行使に当たっては、**高い独立性と政治的中立性が担保**されている。



（参考）個人情報保護法の全体像

憲法・判例
（第13条：個人の尊重等、第21条：通信の秘密等、第35条：住居の不可侵）

個人情報保護法・政令・規則［基本法］
（１～３章：基本理念、国及び地方公共団体の責務等・個人情報保護施策等）

個人情報の保護に関する基本方針
（個人情報保護施策の総合的かつ一体的な推進を図るため、官民の幅広い主体に対し、具体的な実践に取り組むことを要請）

民間部門［一般法］

個人情報保護法・政令・規則
（４・８章ほか：個人情報取扱事業者等の義務等、罰則　等）

【対象】民間事業者　　※一部の独立行政法人等を含む。

ガイドライン

Q&A

公的部門［一般法］

個人情報保護法・政令・規則
（５・８章ほか：行政機関等の義務等、罰則　等）
個人情報保護法施行条例

【対象】行政機関（国）・独立行政法人等・
地方公共団体の機関・地方独立行政法人

ガイドライン・事務対応ガイド

Q&A

注１　個人番号（マイナンバー）や医療分野等においては、上記一般法に優先して適用される特別法も遵守する必要。
注２　金融関連分野、医療関連分野や情報通信分野等の特定分野においては、上記ガイドライン等のほか、当該分野ごとのガイドライン等も遵守する必要。
注３　独立行政法人等、地方公共団体の機関及び地方独立行政法人の一部である国公立の病院・大学等の法人又は業務については、基本的には民間部門の規律が適用されるが、個人情報ファイル、開示等及び匿名加工情報に関する規律については、公的部門の規律が適用。
注４　民間部門においては、対象事業者に対する苦情処理、情報提供や指導等を行う認定個人情報保護団体に対し、対象事業者における個人情報等の適正な取扱いに関する自主的なルール（個人情報保護指針）を作成する努力義務があり、対象事業者は当該指針も遵守する必要。
注５　EU及び英国域内から十分性認定により移転を受けた個人データについては、上記法令及びガイドライン等のほか、補完的ルールも遵守する必要。

民間部門に適用される規律について

【個人情報】

生存する個人に関する情報で、特定の個人を識別することができるもの

① 取得・利用に関するルール

- **利用目的を特定して、その範囲内**で利用する。
- **利用目的を通知又は公表**する。
- 要配慮個人情報の取得は、原則として、あらかじめ本人から**同意**を得る。
- **偽りその他不正の手段**により個人情報を取得しない。
- **違法又は不当な行為を助長し、又は誘発するおそれがある方法**により利用しない。
- 苦情等に適切・迅速に対応する。

【個人データ】

個人情報データベース等を構成する個人情報

個人情報取扱事業者：個人情報データベース等を事業の用に供している者

② 保管・管理に関するルール

- データ内容を正確かつ最新の内容に保つとともに、利用する必要がなくなったときは消去するように努める。
- 漏えい等が生じないよう、**安全に管理**する。従業者・委託先にも安全管理を徹底する。
- 委員会規則で定める漏えい等が生じたときには、委員会に対して報告を行うとともに、本人への通知を行う。

③ 第三者提供に関するルール

- **第三者に提供する場合は、あらかじめ本人から同意**を得る（※**例外規定あり**）。
- **外国にある第三者に提供する場合**は、当該提供について、参考情報を提供した上で、あらかじめ本人から**同意**を得る。
- 第三者に提供した場合・第三者から提供を受けた場合は、一定事項を記録する。

【保有個人データ】

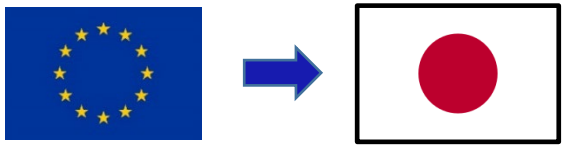
開示、訂正、利用停止、消去等の権限を有する個人データ

④公表事項・開示請求等への対応に関するルール

- 事業者の名称や利用目的、開示等手続などの事項を公表する。
- 本人から**開示等の請求があった場合はこれに対応**する。

日EU　個人データ越境移転規制の制度

GDPR
（一般データ保護規則：General Data Protection Regulation）

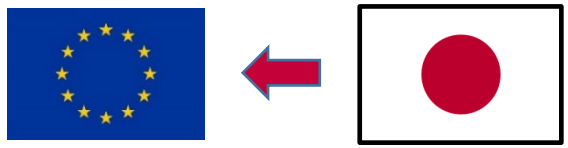


十分性認定
十分な個人情報の保護水準が保証されていることを欧州委員会が認めた場合。

体制整備
企業グループ内の内部行動規範や企業間の契約条項で保護措置を確保している場合。

本人同意
十分性認定等がないことによるリスクについての情報が提供されたうえでの明示的な本人の同意がある場合。

個人情報保護法



国指定
提供先の第三者が個人情報保護委員会の認めた国・地域に所在する場合。

体制整備
提供先の第三者が個人情報保護委員会の規則で定める基準に適合する体制を整備している場合。

本人同意
外国にある第三者へ提供することについて本人の同意がある場合。

十分性認定を得ていることで、本人同意がない場合や企業間契約等がない場合でも、
EUから個人情報を日本に移転することが可能。
DFFT（信頼性のある自由なデータ流通）の観点からも、大きな効果

２．安心安全なデータ利活用に向けた個人情報保護政策

⑴個人情報保護法の概要
⑵個人データの安全管理措置
　/漏えい等報告
⑶いわゆる３年ごと見直しについて

個人データの安全管理措置/漏えい等報告

安全管理措置（第23条）

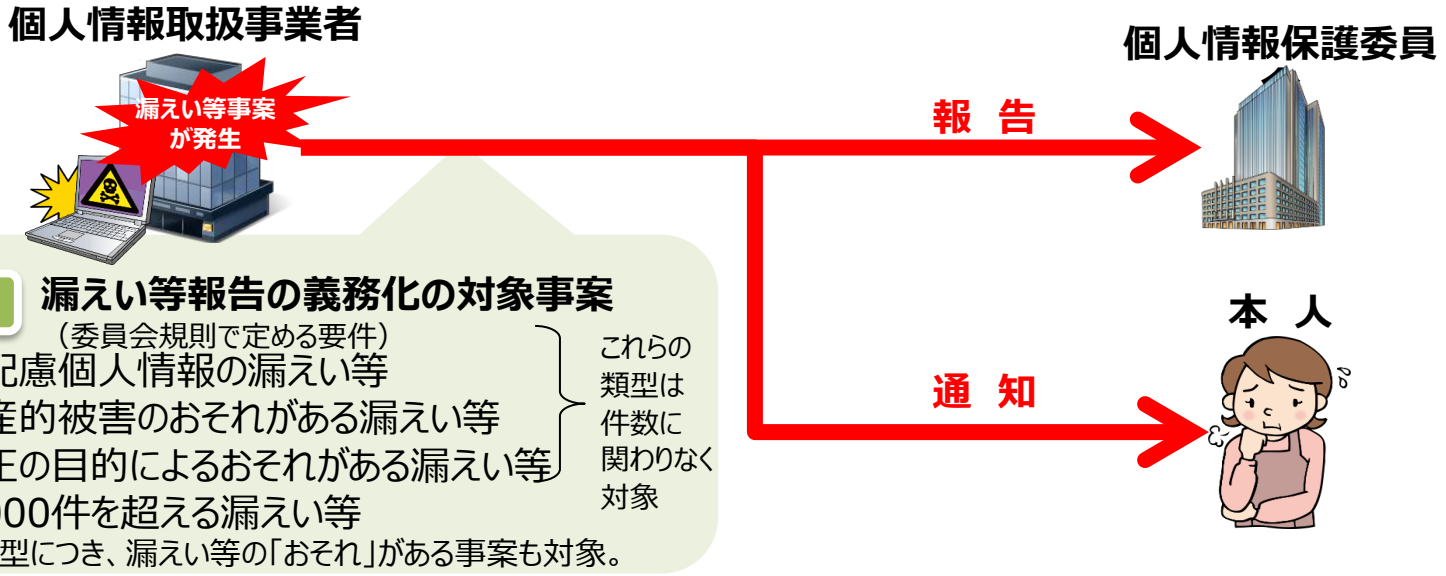
個人情報取扱事業者は、その**取り扱う個人データの漏えい、滅失又は毀損の防止**その他の**個人データの安全管理のために必要なかつ適切な措置**を講じなければならない。

- ✓ 組織的安全管理措置
- ✓ 技術的安全管理措置
- ✓ 人的安全管理措置
- ✓ 物理的安全管理措置

漏えい等の報告（第26条第1項・第2項）

漏えい等が発生し、個人の権利利益を害するおそれが大きい場合、

- **個人情報保護委員会へ報告**
- **本人へ通知**（ただし、本人への通知が困難な場合、これに代わるべき措置をとる）



安全管理措置

個人情報保護法第23条
　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならないが、当該措置は、**個人データが漏えい等をした場合に本人が被る権利利益の 侵害の大きさを考慮**し、**事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容**としなければならない。
　なお、「その他の個人データの安全管理のために必要かつ適切な措置」には、個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、当該個人情報取扱事業者 が個人データとして取り扱うことを予定しているものの漏えい等を防止するために必要か つ適切な措置も含まれる。
　具体的に講じなければならない措置や当該措置を実践するための手法の例等については、**「10（別添）講ずべき安全管理措置の内容」を参照**のこと

講ずべき安全管理措置の内容

個人データの取扱いに係る規律の整備

個人情報取扱事業者は、その取り扱う個人データの漏えい等の防止その他の個人データの安全管理のために、個人データの具体的な取扱いに係る規律を整備しなければならない。

- 取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について定める個人データの取扱規程を策定

組織的安全管理措置

個人情報取扱事業者は、組織的安全管理措置として、次に掲げる措置を講じなければならない。

(1)組織体制の整備
(2)個人データの取扱いに係る規律に従った運用
(3)個人データの取扱状況を確認する手段の整備
(4)漏えい等事案に対応する体制の整備
(5)取扱状況の把握及び安全管理措置の見直し

物理的安全管理措置

個人情報取扱事業者は、物理的安全管理措置として、次に掲げる措置を講じなければならない。

(1)個人データを取り扱う区域の管理
(2)機器及び電子媒体等の盗難等の防止
(3)電子媒体等を持ち運ぶ場合の漏えい等防止
(4)個人データの削除及び機器、電子媒体等の廃棄

人的安全管理措置

個人情報取扱事業者は、人的安全管理措置として、次に掲げる措置を講じなければならない。

〇従業者の教育

(参考)従業者に個人データを取り扱わせる場合には、法第 24 条に基づき従業者を監督

技術的安全管理措置※

個人情報取扱事業者は、技術的安全管理措置として次に掲げる措置を講じなければならない。

(1)アクセス制御
(2)アクセス者の識別と認証
(3)外部からの不正アクセス等の防止
(4)情報システムの使用に伴う漏えい等の防止

※情報システム(PC等を含む。)を使用して個人データを取り扱う場合(インターネット等を通じて外部と 送受信等する場合を含む。)

（参考）漏えい等の報告義務

漏えい等の報告義務（法第26条第１項）

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。

規則第７条１号　要配慮個人情報

- 要配慮個人情報が含まれる個人データの漏えい、滅失若しくは毀損（以下「漏えい等」という。）が発生し、又は発生したおそれがある事態

規則第７条２号　財産的被害

- 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態

規則第７条３号　不正の目的

- **不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為**による**個人データ**（当該個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む。）**の漏えい等が発生**し、又は発生したおそれがある事態

規則第７条４号　本人数1000人超

- **個人データに係る本人の数が 1000 人を超える漏えい等が発生**し、又は発生したおそれがある事態

（参考）漏えい等報告が必要な場合（事例）

不正アクセスにより個人データが漏えいした場合

- 個人データを格納しているサーバー等において、外部からの不正アクセスによりデータが窃取された場合
- マルウェアに感染したコンピュータに不正な指令を送り、IPアドレス等への通信が確認された場合
- 不正検知を行う専門家等の第三者から漏えいのおそれについて連絡を受けた場合

ランサムウェア等により個人データが暗号化され、復元できなくなった場合

ECサイトからクレジットカード番号を含む個人データが漏えいした場合

※クレジットカード番号の下4桁のみとその有効期限の組合せの漏えいであれば、直ちに報告対象事態には該当しない。

送金や決済機能のあるウェブサービスのログインIDとパスワードの組み合わせを含む個人データが漏えいした場合

漏えい等事案が発生した場合に講ずべき措置・体制整備

漏えい等事案が発覚した場合に講ずべき措置<ガイドライン3-5-2>

（1）事業者内部における報告及び被害の拡大防止

責任ある立場の者に直ちに報告するとともに、漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる。

（2）事実関係の調査及び原因の究明

漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講ずる。

（3）影響範囲の特定

上記（2）で把握した事実関係による影響範囲の特定のために必要な措置を講ずる。

（4）再発防止策の検討及び実施

上記（2）の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を講ずる。

（5）個人情報保護委員会への報告及び本人への通知

安全管理措置の一内容として、個人情報取扱事業者は、**漏えい等事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備**しなければならない。
＜ガイドライン10-3(4)漏えい等事案に対応する体制の整備＞

漏えい等報告の種類（速報・確報）

速　報

個人情報取扱事業者は、法第26条第1項本文の規定による報告をする場合には、前条各号に定める事態を知った後、**速やかに※**、当該事態に関する次に掲げる事項(報告をしようとする時点において把握しているものに限る。次条において同じ。)を報告しなければならない。＜規則８条１項＞

※個別の事案によるものの、個人情報取扱事業者が当該事態を知った時点から**概ね3～5日以内**である。＜ガイドライン3-5-3-1＞

確　報

個人情報取扱事業者は、**当該事態を知った日から 30 日以内(当該事態が前条第３号に定めるものである場合にあっては、60 日以内)**に、当該事態に関する前項各号に定める事項を報告しなければならない。
＜規則８条２項＞

※　確報を行う時点（報告対象事態を知った日から 30 日以内又は 60 日以内）において、合理的努力を尽くした上で、**一部の事項が判明しておらず、全ての事項を報告することができない場合には、その時点で把握している内容を報告し、判明次第、報告を追完**することができる。
＜ガイドライン３－５－３－４＞

（参考）漏えい等報告の報告事項

報告書

個人情報の保護に関する法律第 26 条第 1 項の規定により、次のとおり報告します。

令和●年 5 月 15 日

個人情報保護委員会　殿

報告者の氏名又は名称　　株式会社〇〇工業
住所又は居所　　〇〇県△△市××－××

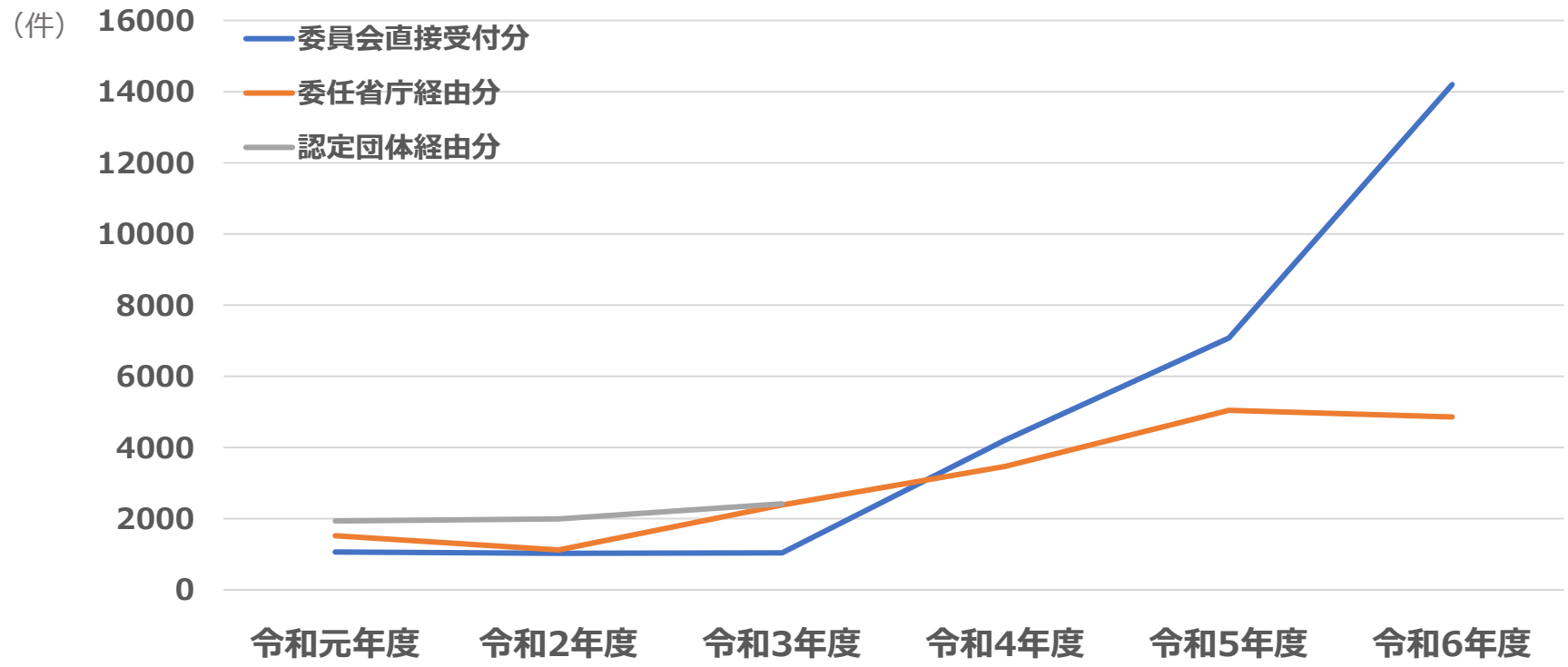
1．報告種別（該当する□に印を付けること。）
新規又は続報の別：□ 新規　☑ 続報　前回報告：令和●年 4 月 2 日
速報又は確報の別：□ 速報　☑ 確報

2．報告をする個人情報取扱事業者（以下「報告者」という。）の概要

報告者の氏名又は名称	（フリガナ）カ）●●●●コウギョウ 株式会社〇〇工業
法人番号（13 桁）	● ● ● ● ● ● ● ● ● ● ● ● ●
業種・業種番号	●●●●業　● ● ● ●
報告者の住所又は居所	〇〇県△△市 ××－××
代表者の氏名（報告者が法人等の場合に限る。）	（フリガナ）コジョウイ　イチロウ 代表取締役 個情委　一郎
事務連絡者の氏名	（フリガナ）カ）●●●●コウギョウ　ソウムブ　〇〇カ　ホゴホウ　ジロウ 株式会社〇〇工業 所属部署　総務部〇〇課　保護法　二郎 電話　●●●●（　●●　）　●●●● E-mail　●●●●@●●.jp

３　報告事項
(1)事態の概要
※発生日／発覚日
発生事案（漏えい、滅失　等）
規則第７条各号該当性
データ委託先の有無
事案経過
※　概要、発覚の経緯・発覚後の事実経過
外部機関による調査の実施状況
（規則第７条第３号に該当する場合）
(2)漏えい等が発生し又は発生したおそれがある個人データの項目
(3)漏えい等が発生し又は発生したおそれがある個人データに係る本人の数
(4)発生原因
(5)二次被害又はそのおそれの有無及びその内容
(6)本人への対応の実施状況
(7)公表の実施状況
(8)再発防止のための措置
(9)その他参考となる事項

（参考）漏えい等報告の件数の推移（提出経路別）



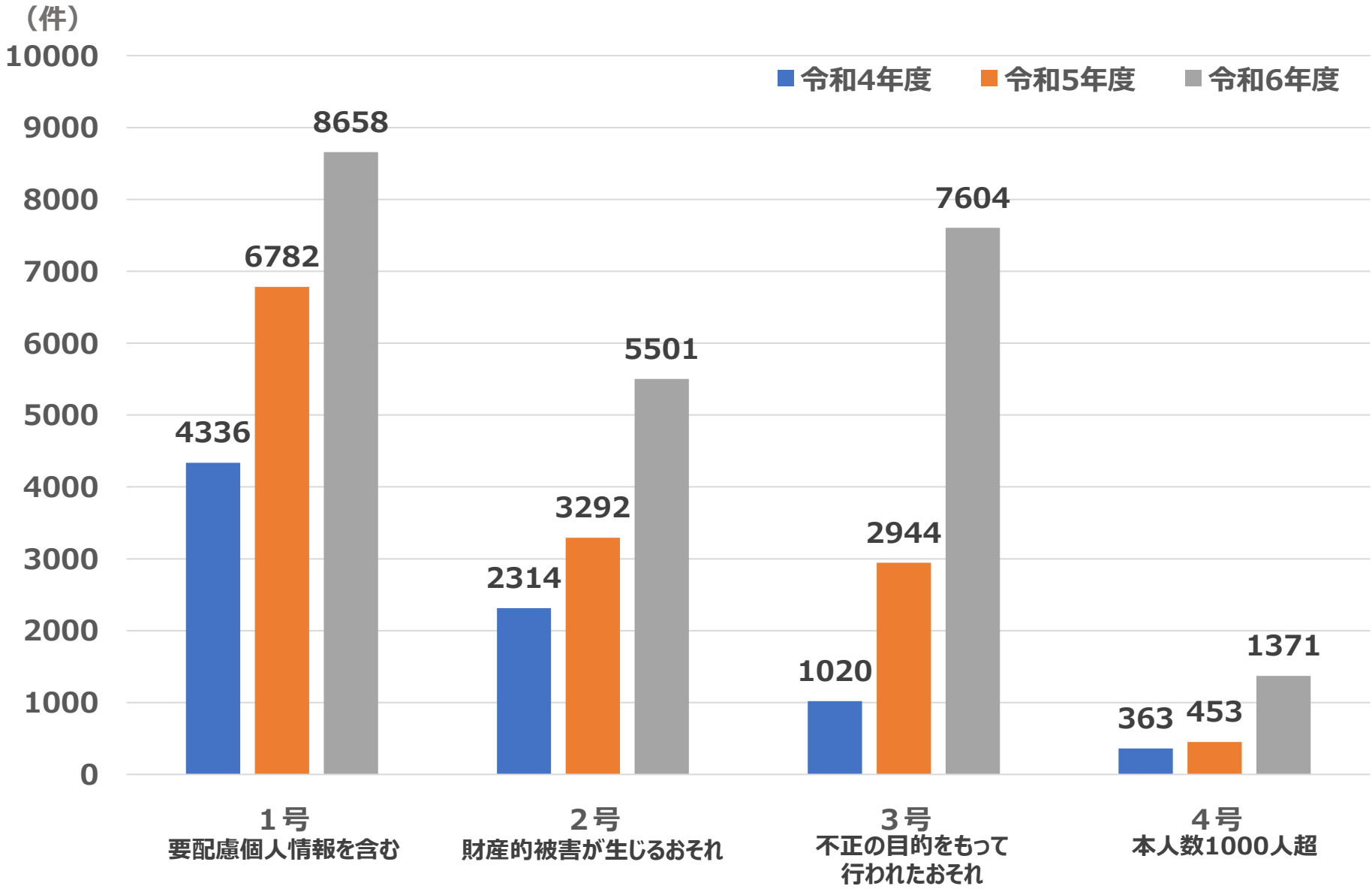
	令和元年度		令和2年度		令和3年度		令和4年度		令和5年度		令和６年度	
委員会直接受付分	**1066**	**23.6%**	**1027**	**24.8%**	**1042**	**17.8%**	**4217**	**54.9%**	**7075**	**58.4%**	**14198**	**74.5%**
委任先省庁経由分	**1519**	**33.6%**	**1122**	**27.1%**	**2386**	**40.8%**	**3468**	**45.1%**	**5045**	**41.6%**	**4858**	**25.5%**
認定団体経由分	1935	42.8%	1992	48.1%	2418	41.4%	－		－			
総数	**4520**		**4141**		**5846**		**7685**		**12120**		**19056**	

※1　令和元年度～令和６年度個人情報保護委員会年次報告より
　　令和２年改正法が令和４年４月１日に施行されたことに伴い、認定団体を経由した漏えい等事案の報告制度は廃止された。
※2　令和6年度の件数にはSaaSを提供する事業者のサーバーが不正アクセスを受けたことにより、同社SaaSを利用していた多数の個人情報取扱事業者に影響が及んだ事案に係る漏えい等報告2,745件が含まれています（以下の令和６年度の件数についても同じ）。

（参考）漏えい等報告実績：人数別

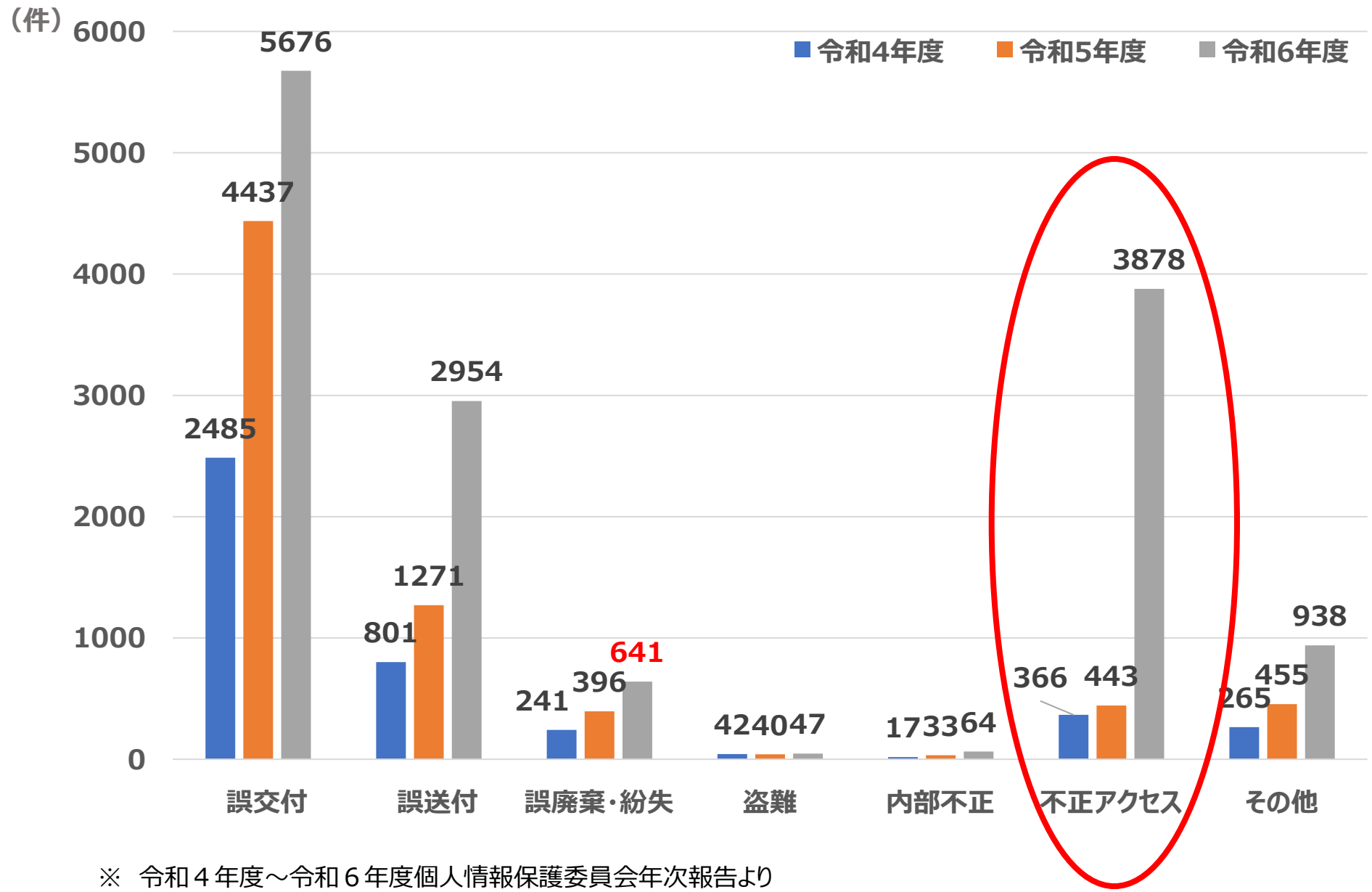
※　令和４年度～令和６年度個人情報保護委員会年次報告等より

（参考）漏えい等報告実績：報告義務該当事由別



※　令和４年度～令和６年度個人情報保護委員会年次報告等より

（参考）漏えい等報告実績：原因別（※委員会直接受付分）

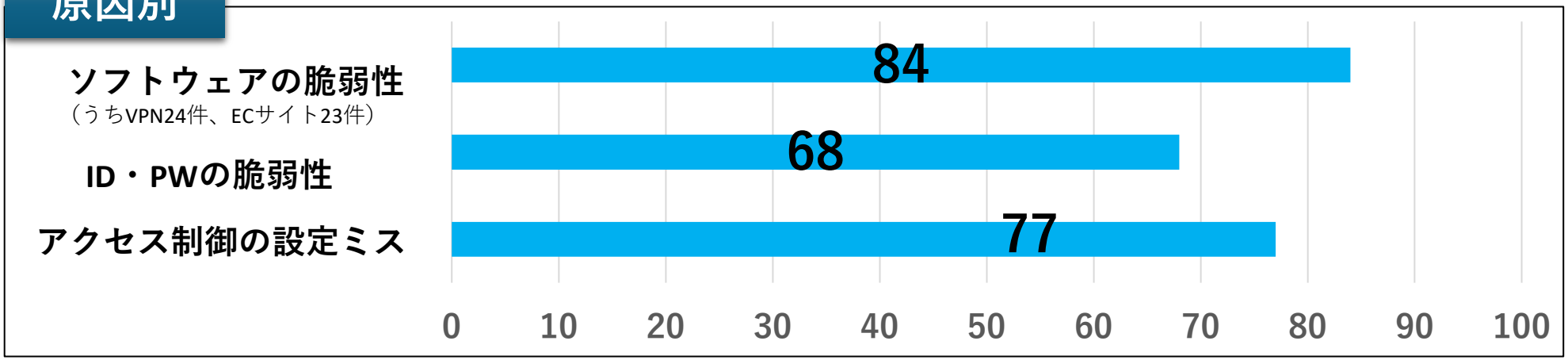


※　令和４年度～令和６年度個人情報保護委員会年次報告より

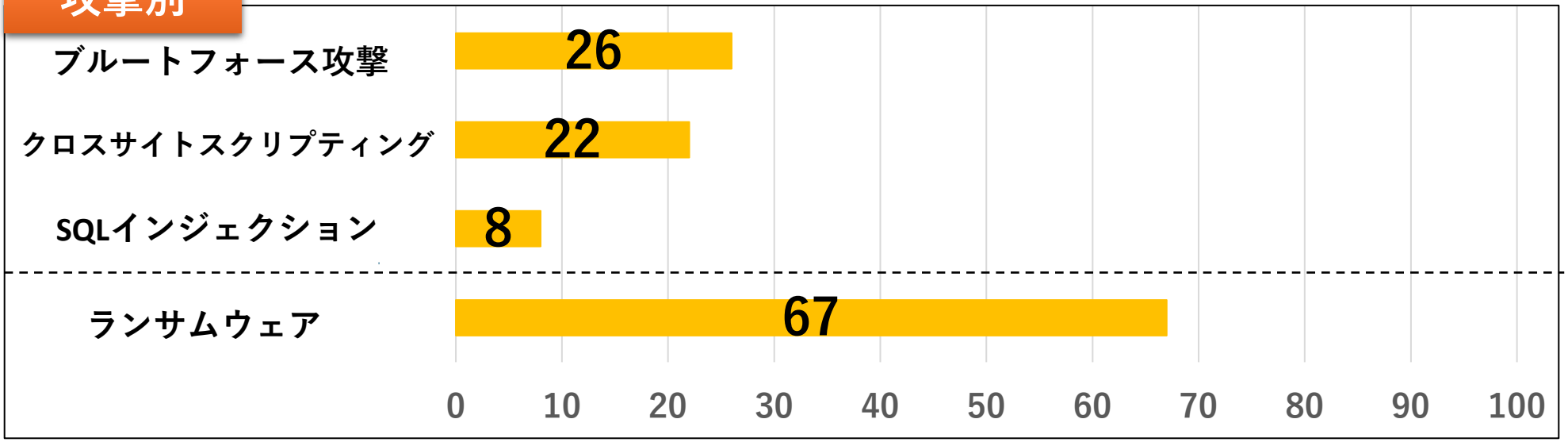
令和６年度指導・助言案件の要因分析

（全体件数　198）

原因別



攻撃別



（※1）個人情報保護委員会における民間事業者に対する指導案件のうち、不正アクセスが原因となっている事案（198件）を抽出して分析したもの。なお、原因別・攻撃別の項目は、主なものに限り記載している。

（※2）１つの事態で複数の原因別・攻撃別の項目に該当する場合には全てに計上しているため、原因別、攻撃別の各項目の件数の合計は、全体件数を超えることがある。

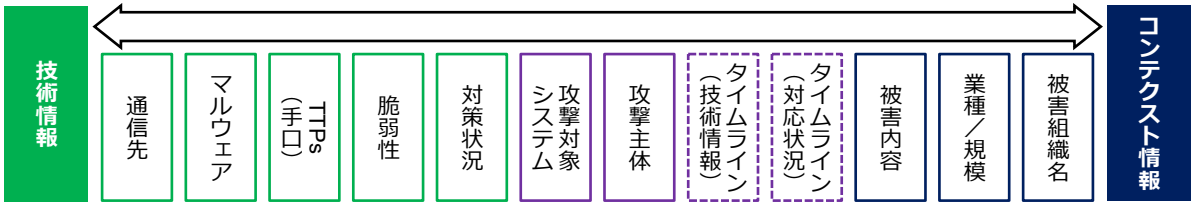
（参考）サイバー攻撃被害に係る情報の共有・公表ガイダンス

- サイバー攻撃被害を受けた組織がサイバーセキュリティ関係組織（例：NISC、警察、所管省庁、JPCERT、ISACなど）と被害に係る情報を共有することは、被害組織自身にとっても社会全体にとっても有益。一方、被害組織においては、どのような情報を、どのタイミングで、どのような主体と共有すべきか、必ずしも十分な理解が進んでいない。
- このため、被害組織の担当部門（例：システム運用部門、法務・リスク管理部門等）を想定読者として、被害組織の立場にも配慮しつつ、サイバー攻撃被害に係る情報を共有する際の実務上の参考となるガイダンス文書を策定し、普及を図ることで、円滑かつ効果的な情報共有を促進していく。
- このガイダンス文書策定のため、サイバーセキュリティ協議会(※)運営委員会の下に、2022年4月、内閣官房・警察庁・総務省・経済産業省を事務局として、有識者からなる「サイバー攻撃被害に係る情報の共有・公表ガイダンス」検討会（座長：星周一郎東京都立大学法学部教授）を設置して検討。2023年3月8日にガイダンスを公表。

※サイバーセキュリティ基本法に基づき、平成31年4月に組織された法定の官民の情報共有体制。関係省庁で運営委員会を構成。

https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00160.html

- **どのような情報を？**（様々な種類・性質の情報が存在）



- **どのタイミングで？**（サイバー攻撃への対処の時系列を意識）

- **どのような主体と？**（様々なサイバーセキュリティ関係組織が存在）

- **想定読者**（被害組織）

CSIRT
システム運用部門

法務・リスク管理・
企画・渉外・広報部門

個人情報保護法サイバーセキュリティ連絡会の開催

○ 個人情報取扱事業者等は取り扱う個人データ等につき安全管理措置を講じなければならず、組織的・人的・技術的安全管理措置等を適切に講ずることにより、情報システムに対する外部からの不正アクセス等を防止することが期待されている。

○ しかしながら、近年、個人情報取扱事業者等からの機密情報等の窃取・破壊等を企図したサイバー攻撃は一層高度化・複雑化・巧妙化し、攻撃対象も拡大し続けており、個人データ等の漏えい等の大きな要因となっている。

○ このような情勢の中で、個人情報保護委員会が、データ関係省庁等との連携を強化し、個人情報保護法上求められる各種の安全管理措置として講じ得る方策等について検討・把握するとともに、個人情報取扱事業者等に対する効果的な普及啓発の在り方等を検討する観点から、「個人情報保護法サイバーセキュリティ連絡会」を令和６年12月から開催。

１．開催目的等

・個人情報保護法上求められる各種の安全管理措置として講じ得る方策等について検討・把握するとともに、個人情報取扱事業者等に対する効果的な普及啓発の在り方等を検討するため、四半期ごとに行う。

２．検討事項

・直近の漏えい等報告や指導の状況（四半期公表内容。不正アクセスによる個人データ等の漏えい等事例を含む。）を説明し、専門的見地から個人データ等の漏えい等の対策や留意すべき点等について、助言を得る。
・その他、安全管理措置の実施方策や効果的な普及啓発の方法に係る情報交換を実施。

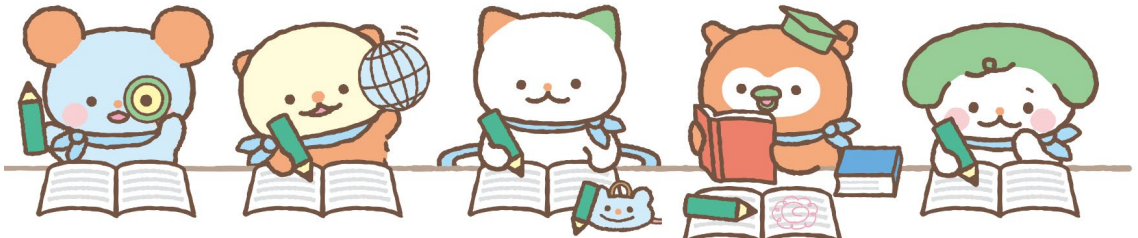
３．参加機関

・内閣官房　国家サイバー統括室（NCO）
・警察庁サイバー警察局
・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（JPCERT/CC）
・個人情報保護委員会事務局
（JPCERT/CC以外は、当委員会との覚書締結機関）

※「個人情報保護法サイバーセキュリティ連携会議」及び「特定個人情報セキュリティ関係省庁等連絡協議会」は、上記以外の省庁・機関も幅広く含む連携会議/連絡協議会として今後も開催（年1回開催）

２．安心安全なデータ利活用に向けた個人情報保護政策

⑴個人情報保護法の概要
⑵個人データの安全管理措置
　/漏えい等報告
⑶いわゆる３年ごと見直しについて



いわゆる３年ごと見直し規定に基づく検討

いわゆる3年ごと見直し規定（令和2年改正法）

○個人情報の保護に関する法律等の一部を改正する法律
（令和2年法律第44号）

※令和4年4月1日全面施行

附　則

第十条　政府は、この法律の施行後三年ごとに、個人情報の保護に関する国際的動向、情報通信技術の進展、それに伴う個人情報を活用した新たな産業の創出及び発展の状況等を勘案し、新個人情報保護法の施行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。

いわゆる３年ごとの見直しこれまでの検討経緯

令和５年

９～10月	「改正個人情報保護法の施行状況について」公表
11月15日	「個人情報保護法　いわゆる３年ごと見直し規定に基づく検討」公表
11月下旬～	関係団体等ヒアリングを順次実施

令和６年

２月21日	「個人情報保護法　いわゆる３年ごと見直し規定に基づく検討項目」公表
４月上旬～	有識者ヒアリングを順次実施
６月27日	**「中間整理」公表**（～7月29日までパブコメ実施）
９月　４日	「中間整理」に関する意見募集の結果・今後の検討の進め方　公表
10月16日	**「個人情報保護法のいわゆる３年ごと見直しの検討の充実に向けた視点」公表**
12月17日	事務局ヒアリング（有識者 、経済団体・消費者団体）の状況報告
12月25日	**「個人情報保護法のいわゆる３年ごと見直しに関する検討会 報告書」公表**

令和７年

１月22日	**「「個人情報保護法　いわゆる３年ごと見直しに係る検討」の今後の検討の進め方について」公表**
２月　５日	「個人情報保護法の制度的課題に対する考え方（案）について（個人データ等の取扱いにおける本人関与に係る規律の在り方）」公表
２月19日	「個人情報保護法の制度的課題に対する考え方（案）について（個人データ等の取扱いの態様の多様化等に伴うリスクに適切に対応した規律の在り方）」公表
３月　５日	**「個人情報保護法の制度的課題に対する考え方について」公表、意見の概要①**
４月16日	**意見の概要②**
６月13日	**デジタル重点計画、データ利活用制度の在り方に関する基本方針、経済財政運営と改革の基本方針2025、新資本実行計画2025等閣議決定**

（参考）個人情報保護制度の基本的在り方に関する事務局ヒアリング

「個人情報保護法のいわゆる３年ごと見直しの検討の充実に向けた視点」に基づき、個人情報保護委員会事務局において、個人情報保護制度の基本的在り方に関するヒアリングを実施。

個人情報保護政策を考える上で注目すべき環境変化、重視すべきリスク・政策目的、実態を踏まえた規制の在り方といった制度の基本的在り方に関わる次元の論点について、改めて、幅広いステークホルダー等の間で再確認するもの。

【ヒアリング対象】

（有識者：11名）

・石井夏生利氏　・板倉陽一郎氏　・佐藤一郎氏　・宍戸常寿氏　・新保史生氏
・鈴木正朝氏　・曽我部真裕氏　・高木浩光氏　・高橋克巳氏　・森亮二氏　・山本龍彦氏

（経済団体・消費者団体等：17団体）

・一般社団法人AIガバナンス協会
・一般社団法人全国消費者団体連絡会
・一般社団法人電子情報技術産業協会
・一般社団法人日本インタラクティブ広告協会
・一般社団法人日本DPO協会
・一般社団法人MyDataJapan
・公益社団法人全国消費生活相談員協会
・サステナビリティ消費者会議
・プライバシーテック協会
・一般社団法人新経済連盟
・一般社団法人データ社会推進協議会
・一般社団法人日本IT団体連盟
・一般社団法人日本経済団体連合会
・一般社団法人日本ディープラーニング協会
・一般社団法人モバイル・コンテンツ・フォーラム
・国立研究開発法人情報通信研究機構
・主婦連合会

適正な個人データの取扱い確保のための規律

※民間部門に適用される規律について述べたもの

適正な個人データの取扱いを通じて個人の権利利益を保護するために、個人情報保護法において、次のような規律を整備。

これらは**全ての事業者に適用される最低限のルール**ともいえ、取り扱われる個人データ、利用目的の性質及び事業活動の態様に応じて、特別法、ガイドライン、認定個人情報保護団体や業界の自主基準、運用等により**必要に応じて上乗せ**される。

（１）個人データに着目した規律

✓**「個人情報データベース等」による個人データの取扱いの危険性**に着目し、それを**事業の用に供している個人情報取扱事業者**に対し、その適正な取扱いを担保するための義務等を規律。

（２）個人情報取扱事業者による適正な取扱い

①　本人の関与による適正な取扱いの確保

✓ 個人情報取扱事業者自身のガバナンスにより法律に定める義務が適切に履行され、当該個人情報取扱事業者から本人への通知・公表・同意取得等（※）により**本人による適切な関与・監視を受け**つつ、適正な取扱いの実現を期待するという**当事者間での自主的な規律を重視**する構造。

（※）●取得・利用に関するルール：利用目的を特定し原則としてその範囲内で利用し、取得時に本人に利用目的を通知・公表する。
●第三者提供に関するルール：第三者提供時には、原則として本人の同意を得る。
●公表事項・開示請求等への対応に関するルール：本人から開示・訂正・利用停止等の請求があった場合にはこれに対応する。

②　事業者内における適正な取扱いの確保

✓偽りその他**不正の手段により個人情報を取得**すること、あるいは、違法又は不当な行為を助長し又は誘発するおそれがある方法により**不適正な利用**を行うことは、個人の権利利益の保護を脅かすおそれが大きい。

✓利用目的が妥当であっても、正確性が保たれていなければ、本人に望まぬ影響を与えかねないことから**正確性確保**を義務付け。

✓個人データが個人情報取扱事業者や本人の関与不可能な領域に流出することで本人の権利利益を損なうリスクが増大することから、必要な**安全管理措置、従業員や委託先の監督**を義務付け。

ヒアリングから得られた視点：（１）保護法益について

考慮すべきリスク

(A)評価・選別及びこれに基づく影響を与えるリスク　(B)直接の働きかけを行うことのリスク
(C)秘匿領域が他人に知られるリスク　(D)自身のデータを自由意思に従って制御できないリスク

リスクの優先順位等には、いくつかの異なる考えが示されたが、**バランス良く対応を検討すべきという指摘が大半**。
このほか、次の主張・指摘があった。

- (D)は本人に関わる情報の取扱いを本人が決定する権利に関わるリスクであり、位置付けが異なる。
- データ保護法制たる個人情報保護法が考慮すべきは(A)が主であり、他は副次的、間接的。

→「個人の権利利益の保護」の意味合いに関しては、その権利利益の外延や、特に規律すべき取扱いなどについて様々な考え方があることの表れと考えられる。

保護を要する局面

①本人の知らぬ間に本人の情報を取得すること
②データ分析等を通じて評価・選別を行うこと
③評価の結果を利用して本人に働きかけること

など、様々な段階があることから、**それぞれの段階を念頭においた検討**を行うことで、より適切な規律となり得るのではないか。

保護の対象、規律対象

法目的・理念に即した適切な規律の在り方については、**様々な観点からの検討の余地**があり得るのではないか。

- 保護の対象については、その取扱いによる本人へのリスク（差別的な取扱いの助長、追跡性、脆弱性、本人到達性等）を惹起し得る情報を幅広く対象とすべきとの考え
- 規律する取扱いの態様についても、評価・分析などの「取扱いの類型」や「その目的」を規律対象とすべきとの考え

プロファイリング

プロファイリングをはじめとする個人情報の処理内容についても何らかの規律が必要との指摘も多い。

具体的には、プロファイリング実行のためのプログラム作成に係る元データの利用目的やその関連性、プログラムそのものに関わる論点、プロファイリングによって得られた結果の取扱いなど、様々な視点が示された。

ヒアリングから得られた視点：（2）本人の関与について

本人の関与

本人の関与の趣旨として大きく２つの考え方

①事業者におけるガバナンスを確保するための手段

個人の認知限界や、個人と事業者との情報・交渉力等の非対称性などが存在するとの前提の上で、次のa)、b)の考えがあり、どのような場合をb)の領域とするか様々な考えが示された。

a)個人の選択権であり本人の関与が当然認められるべきという考え

b)合理的な基準を設けて、その適合性を規制当局が監視することが必要であるという考え

②本人に関わる情報の取扱いを本人が決定する権利

この中でも、次のa)、b)を両端として、その間で様々な見解が示された。

a)個人データは本人の所有物であり本人はあらゆる利用について許諾又は拒否の権限を持つべきとの考え

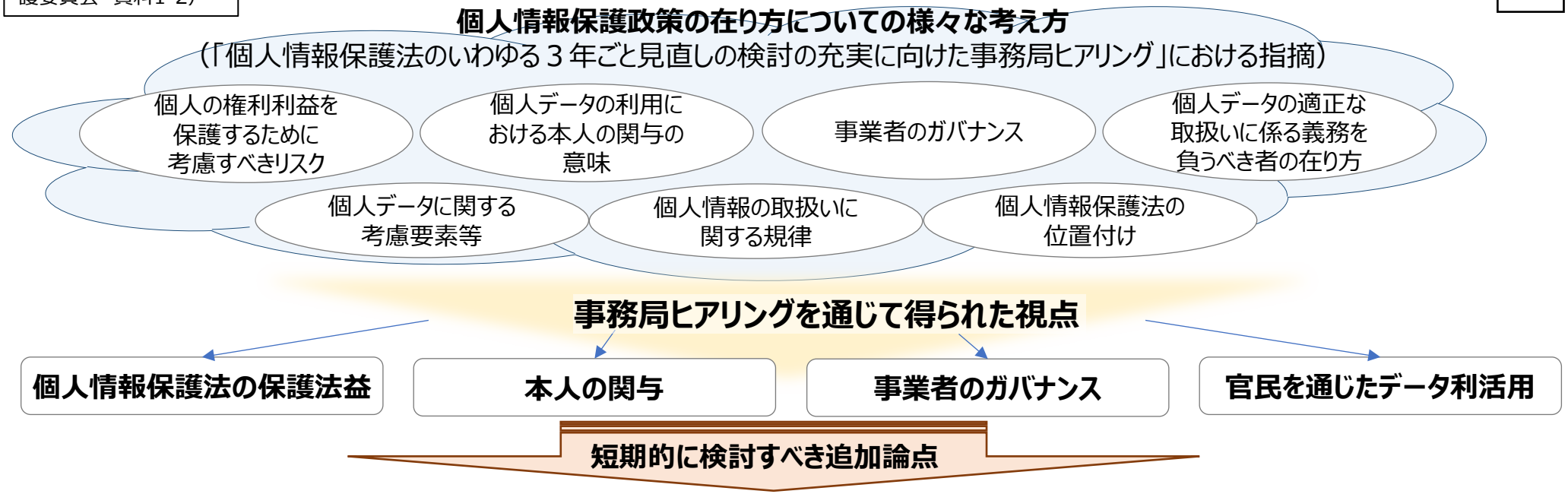
b)社会的なニーズ・手続負担等を踏まえた現実性・具体的な個人の権利利益とのけん連性等との関係で自ずと制限が課されるとの考え

①の観点からは、**本人に直接の影響がない取扱いについては、本人の関与を担保する必要が必ずしもないのではないか**との視点が得られた。ただし、**その場合においても②については**別途、その要否や程度、手法等について**検討する必要**があるものと考えられる。

特に**生成AI**については、学習結果が（個人情報を含まない）パラメータとなることを念頭において「個別の個人の権利利益への直接的な影響が想定されない個人データの利用」であるとして、**本人の関与は必要ないとする指摘が大半**であったが、②の観点から、**自分の情報のAI学習利用について関与できることが必要との考えも**見られた。

②の権利には、現状の開示等の請求等に加えて、能動的に自らの情報を活用する観点からの**データポータビリティも含まれるのではないか**という視点も得られた。ただし、**事業者の負担や事業分野ごとの必要性・妥当性等についての議論が必要**であると考えられる。

事務局ヒアリングを踏まえて短期的に検討すべき追加論点について



個人データ等の取扱いにおける本人関与に係る規律の在り方

「本人の権利利益への直接の影響の有無等」を切り口とした規律の内容を検討

- **同意規制の在り方**

  個人の権利利益の侵害が想定されない統計作成等であると整理できるAI開発等、以下の場合は同意不要と整理できるのではないか

  ① 統計作成等、特定の個人との対応関係が排斥された一般的・汎用的な分析結果の獲得と利用のみを目的とした取扱いを実施する場合
  ② 取得の状況からみて本人の意思に反しない取扱いを実施する場合
  ③ 生命等の保護又は公衆衛生の向上等のために個人情報を取り扱う場合であって本人同意を得ないことに相当の理由があるとき

- **漏えい等発生時の対応（本人通知）の在り方**

  本人への通知が行われなくても本人の権利利益の保護に欠けるおそれが少ない場合は本人通知不要と整理できるのではないか

個人データ等の取扱いの態様の多様化等に伴うリスクに適切に対応した規律の在り方（ガバナンスの在り方）

- **個人データの適正な取扱いに係る義務を負うべき者の在り方**

  個人情報の取扱いに関わる実態（個人データ等の取扱いについて、実質的に第三者に依存するケースが拡大、委託先の管理等を通じた安全管理措置に係る義務の適切な遂行が困難）を踏まえ、個人情報取扱事業者等からデータ処理等の委託を受けた事業者に対する規律の在り方を検討すべきではないか

個人情報保護法の制度的課題の再整理

個人情報保護法の目的（第1条）

「・・・**個人情報の有用性**に配慮しつつ、**個人の権利利益を保護**することを目的とする。」

事務局ヒアリングを通じて得られた視点

個人情報保護法の保護法益 | **本人の関与** | **事業者のガバナンス** | **官民を通じたデータ利活用**

個人データ等の取扱いにおける本人関与に係る規律の在り方

- **同意規制の在り方**
  - 統計作成等(※)、特定の個人との対応関係が排斥された一般的・汎用的な分析結果の獲得と利用のみを目的とした取扱いを実施する場合の本人の同意の在り方
    ※　統計作成等であると整理できるAI開発等を含む
  - 取得の状況からみて本人の意思に反しない取扱いを実施する場合の本人の同意の在り方
  - 生命等の保護又は公衆衛生の向上等のために個人情報を取り扱う場合における同意取得困難性要件の在り方
  - 病院等による学術研究目的での個人情報の取扱いに関する規律の在り方
- **漏えい等発生時の対応（本人通知等）の在り方**
- **子供の個人情報等の取扱い**（※）

※心身の発達過程にあり本人による実効性ある関与が必ずしも期待できない

個人データ等の取扱いの態様の多様化等に伴うリスクに適切に対応した規律の在り方

- 個人情報取扱事業者等からデータ処理等の委託を受けた事業者に対する規律の在り方
- 特定の個人に対する働きかけが可能となる個人関連情報に関する規律の在り方
- 身体的特徴に係るデータ（顔特徴データ等）（※）に関する規律の在り方
  ※本人が関知しないうちに容易に取得することが可能であり、一意性・不変性が高いため、本人の行動を長期にわたり追跡することに利用できる
- オプトアウト届出事業者に対する規律の在り方

個人情報取扱事業者等による規律遵守の実効性を確保するための規律の在り方

- 勧告・命令等の実効性確保
- 刑事罰の在り方
- 経済的誘因のある違反行為に対する実効的な抑止手段（課徴金制度）の導入の要否
- 団体による差止請求制度・被害回復制度の導入の要否
- 漏えい等報告等の在り方

個人データ等の取扱いにおける本人関与に係る規律の在り方①

1　個人の権利利益への影響という観点も考慮した同意規制の在り方

(1)統計作成等、特定の個人との対応関係が排斥された一般的・汎用的な分析結果の獲得と利用のみを目的とした取扱いを実施する場合の本人の同意の在り方

- **統計情報等の作成**（注１）**のために複数の事業者が持つデータを共有し横断的に解析するニーズが高まっている**こと、特定の個人との対応関係が排斥された統計情報等の作成や利用はこれによって個人の権利利益を侵害するおそれが少ないものであることから、このような**統計情報等の作成にのみ利用されることが担保されていること等**（注２）(注３）**を条件**に、**本人同意なき個人データ等の第三者提供**（注４）(注５）**及び公開されている要配慮個人情報の取得**を可能としてはどうか（注６）。

  注1：統計作成等であると整理できるAI開発等を含む。
  注2：本人同意なき個人データ等の第三者提供については、当該個人データ等が統計情報等の作成にのみ利用されることを担保する観点等から、個人データ等の提供元・提供先における一定の事項（提供元・提供先の氏名・名称、行おうとする統計作成等の内容等）の公表、統計作成等のみを目的とした提供である旨の書面による提供元・提供先間の合意、提供先における目的外利用及び第三者提供の禁止を義務付けることを想定している。
  注3：本人同意なき公開されている要配慮個人情報の取得については、当該要配慮個人情報が統計情報等の作成又は本規律に基づく本人同意なき個人データ等の第三者提供にのみ利用されることを担保する観点等から、公開されている要配慮個人情報の取得者における一定の事項（取得者の氏名・名称、行おうとする統計作成等の内容又は本規律に基づく本人同意なき個人データ等の第三者提供を行う目的である旨等）の公表、取得者における目的外利用及び第三者提供（本規律に基づく本人同意なき個人データ等の第三者提供を行う目的である場合における当該第三者提供を除く。）の禁止を義務付けることを想定している。
  注4：法第17条の規定により特定された利用目的の達成に必要な範囲を超える第三者提供を含む。
  注5：当該提供により提供先が本人同意なく要配慮個人情報を取得することも可能とすることを想定している。
  注6：具体的な対象範囲や公表事項等は、制度が円滑に運用されるよう、改正の趣旨を踏まえつつ、個人情報保護委員会規則（以下「委員会規則」という。）等で定めることを想定している。

- 行政機関等の取り扱う保有個人情報についても同様に、利用目的以外の目的のための提供に係る「統計の作成」の例外規定の対象を、統計情報等の作成に拡大してはどうか。

個人データ等の取扱いにおける本人関与に係る規律の在り方②

1　個人の権利利益への影響という観点も考慮した同意規制の在り方

(2) 取得の状況からみて本人の意思に反しない取扱いを実施する場合の本人の同意の在り方

- **個人データの第三者提供等が契約の履行のために必要不可欠な場合**を始め、目的外利用、要配慮個人情報取得又は第三者提供が本人の意思に反しないため本人の権利利益を害しないことが明らかである場合（注７）について、**本人の同意を不要**としてはどうか。

注7：例えば、本人が、事業者Aの運営するホテル予約サイトで事業者Bの運営するホテルの宿泊予約を行ったため、事業者Aが事業者Bに当該本人の氏名等を提供する場合や、金融機関が海外送金を行うために送金者の情報を送金先の金融機関に提供する場合等が想定される。具体的な対象範囲は、制度が円滑に運用されるよう、改正の趣旨を踏まえつつ、委員会規則等で定めることを想定している。

(3) 生命等の保護又は公衆衛生の向上等のために個人情報を取り扱う場合における同意取得困難性要件の在り方

- **人の生命、身体又は財産の保護のための例外規定及び公衆衛生の向上又は児童の健全な育成の推進のための例外規定**について、現行制度においては「本人の同意を得ることが困難であるとき」という要件が付されているが、事業者・本人の同意取得手続に係る負担を軽減し、個人情報のより適正かつ効果的な活用及びより実効的な個人の権利利益の侵害の防止につなげる観点から、**「本人の同意を得ることが困難であるとき」のみならず、「その他の本人の同意を得ないことについて相当の理由があるとき」（注８）についても、上記例外規定に依拠**できることとしてはどうか。

注8：例えば、（公衆衛生の向上のために特に必要である一方で、）本人のプライバシー等の侵害を防止するために必要かつ適切な措置（氏名等の削除、提供先との守秘義務契約の締結等）が講じられているため、当該本人の権利利益が不当に侵害されるおそれがない場合等が想定される。具体的な事例については、制度が円滑に運用されるよう、改正の趣旨を踏まえつつ、ガイドライン等において明確化することを想定している。

(4) 病院等による学術研究目的での個人情報の取扱いに関する規律の在り方

- 医学・生命科学の研究においては、研究対象となる診断・治療の方法に関する臨床症例の分析が必要不可欠であり、病院等の医療の提供を目的とする機関又は団体による研究活動が広く行われている実態があることから、目的外利用規制、要配慮個人情報取得規制、第三者提供規制に係るいわゆる学術研究例外に依拠することができる主体である**「学術研究機関等」に、医療の提供を目的とする機関又は団体**（注９）**が含まれることを明示**することとしてはどうか。

注９：例えば、病院や、その他の医療の提供を目的とする機関等（診療所等）が含まれることが想定される。具体的な対象範囲は、制度が円滑に運用されるよう、改正の趣旨を踏まえつつ、ガイドライン等において明確化することを想定している。

漏えい等の発生時の規律について

個人データ等の取扱いにおける本人関与に係る規律の在り方

2　本人への通知が行われなくても本人の権利利益の保護に欠けるおそれが少ない場合における漏えい等発生時の対応の在り方

- 現行法上、個人情報取扱事業者は、漏えい等報告の義務を負うときは、本人への通知が困難な場合を除き、一律に本人への通知義務を負うこととなるが、**本人への通知が行われなくても本人の権利利益の保護に欠けるおそれが少ない場合（注10）について、本人への通知義務を緩和**し、代替措置による対応を認めることとしてはどうか。

  注10：例えば、**サービス利用者の社内識別子（ID）等、漏えいした情報の取得者において、それ単体ではおよそ意味を持たない情報のみが漏えいした場合**などが想定される。具体的な対象範囲は、制度が円滑に運用されるよう、改正の趣旨を踏まえつつ、委員会規則等で定めることを想定している。

- 行政機関等についても同様の改正を行うこととしてはどうか。

個人情報取扱事業者等による規律遵守の実効性を確保するための規律の在り方

5　漏えい等発生時の体制・手順について確認が得られている場合や違法な第三者提供が行われた場合における漏えい等報告等の在り方

- 委員会規則で定めるところによる、報告対象事態（規則第７条）が発生した場合の委員会への報告（法第26条第１項）について、体制・手順に係る認定個人情報保護団体などの第三者の確認を受けること等を前提として、一定の範囲で速報を免除することを可能としてはどうか。さらに、漏えいした個人データに係る本人の数が１名である誤交付・誤送付のようなケースについては、委員会への報告のうち確報を、一定期間ごとに取りまとめた上で行うことを許容してはどうか。
- また、違法な個人データの第三者提供についても報告対象事態にすることとしてはどうか。
- 違法な第三者提供については、行政機関等についても同様の改正を行うこととしてはどうか。

デジタル行財政改革会議　データ利活用制度・システム検討会

目 的

データ利活用による社会課題の解決が重要な課題となる中、医療、金融、産業等の分野における**データ利活用に係る制度及びシステムの整備について包括的な検討を行う**ため、デジタル行財政改革担当大臣の下に、データ利活用制度・システム検討会（以下「検討会」という。）を開催する。

構 成 員

	阿部 淳	株式会社日立製作所代表執行役 執行役副社長
	安中 良輔	日本製薬工業協会産業政策委員会健康医療データ政策 GL
	生貝 直人	一橋大学大学院法学研究科教授
	依田 高典	京都大学大学院経済学研究科教授
	稲谷 龍彦	京都大学大学院法学研究科教授
	岩村 有広	一般社団法人日本経済団体連合会常務理事
	上野山 勝也	株式会社 PKSHA Technology 代表取締役
	岡田 淳	森・濱田松本法律事務所外国法共同事業パートナー弁護士
	落合 孝文	渥美坂井法律事務所・外国法共同事業プロトタイプ政策研究所所長・シニアパートナー弁護士
	越塚 登	東京大学大学院情報学環教授
	宍戸 常寿	東京大学大学院法学政治学研究科教授
	巽 智彦	東京大学大学院法学政治学研究科准教授
	丹野 美絵子	公益社団法人全国消費生活相談員協会消費者情報研究所消費生活専門相談員
（座長）	**森田 朗**	**一般社団法人次世代基盤政策研究所所長・代表理事**

開催実績

第１回	令和6年12月26日	総論（１）
第２回	**令和7年 1月21日**	**総論（２）**
第３回	１月24日	アーキテクチャとシステム
第４回	**２月13日**	**金融分野**
第５回	２月26日	医療分野
第６回	３月 ４日	教育分野
第７回	３月12日	産業分野
第８回	**４月 １日**	**官民のデータ利活用**
第９回	４月15日	重要論点についての議論（医療分野、モビリティ、金融分野）
第10回	**４月24日**	**重要論点についての議論**
第11回	５月13日	データ利活用制度の在り方に関する基本方針素案について
第12回	６月18日	「データ利活用制度の在り方に関する基本方針」報告

EUと日本におけるデジタル関係の法制度の整備状況

個人データ（Personal Data）に関して、EUではGDPR（2016年）、日本では個人情報保護法が一般法。
一般法を前提とした上で、各分野におけるデータ利活用の政策やルールが検討されている。

	データ関係		競争政策関係	AI関係		サイバーセキュリティ関係
	データ保護の法的強化 各分野における データ利活用に影響	**データ利活用の法的強化** ①個人起点（一次利用）、②社会起点（二次利用） 等でのルール整備が進展 ※GDPRと整合的な形でEHDS法等は整備				
EU	GDPR（2016）	データスペース構想（2020） 国や組織を超えてデータを連携できる空間に関するルールや仕組みを整備する構想。ヘルスケア、産　業・製造等の９分野を指定 データガバナンス法（2021） オープンデータ以外の政府のデータ共有促進 データ法（2023） 民間の非個人データ（IoT等）の共有促進 EHDS法（医療・2024） ・ヘルスデータ基盤の構築 ・ヘルスデータ(仮名化・匿名化済)の第三者提供に同意不要 ・医療機関からのデータ提出義務 PSD3（金融決済・検討中）※PSD2は2015に成立 金融データアクセスの枠組と連携したPSD2の改正		デジタル市場法（2022） 競争可能で公正な市場の確保 デジタルサービス法（2022） 消費者と企業へ安全なオンライン環境を創出 EU AI法（2024） 人間中心のAI開発政策の具体化		サイバーレジリエンス法（2024） デジタル要素を含む製品への水平的なサイバーセキュリティ要件の整備
日本	個人情報保護法	日本では、一部の対応※にとどまる。 ※次世代医療基盤法・銀行法等	PF透明化法 スマホ競争促進法	電気通信事業法等で一部対応 検討中		サイバーセキュリティ基本法をはじめ、各種ガイドライン等で対応 （IoTセキュリティ適合性評価制度（JC―STAR）※2025.3制度開始予定）

（出典）第１回データ利活用制度・システム検討会 資料３（表部分）

（参考）デジタル行財政改革会議における議論

第10回　デジタル行財政改革会議
資料５　抜粋

データ利活用の加速（１）

データの利活用を最大限に進め、地域の抱える問題を含めた社会課題の解決を実現するための制度及びシステムの整備について、新たな法制度の構築を含め、包括的に検討。６月に基本的な方針をとりまとめ予定。

視　点

1．データ利活用による価値創出
・新たな価値の創出
・円滑なアクセス
・自由で信頼性がある国際的なデータ流通

2．リスクに対処しつつAIの最大活用

3．透明性、信頼性確保
・データガバナンス
（「データ主権」の尊重、プライバシー、知的財産、安全保障・経済安全保障）

論点①：データ利活用を促す仕組みの整備

・データ政策の司令塔としてデジタル庁の任務を明確化（領域ごとの戦略策定、共通機能の整備）

・トラスト基盤の整備（データ提供者・データ真正性の確認を担保する共通基盤）

・データのデジタル化・標準化・構造化の推進（分野内、分野間の低コストで迅速なデータ連携）

・データ連携プラットフォームの信頼性確保（データ（個人データ、知財等）を安心して預けられる仕組み）

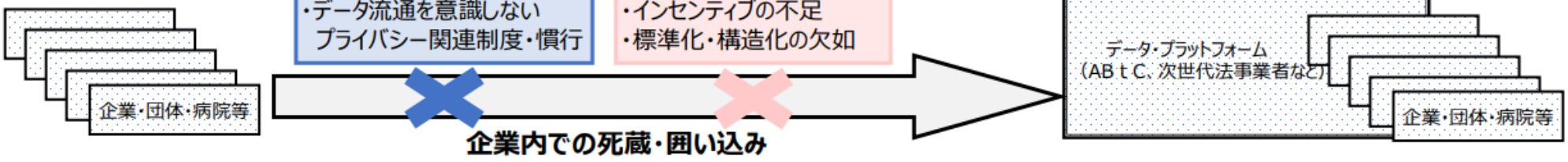
・行政データのオープンデータ化（機械可読データ化等）、デジタル公共財の整備

・リスク（プライバシー、知財）に応じたデータガバナンスの確保（匿名化・仮名化・本人関与・アクセス制限等）

論点②：個人情報保護法のアップデート

・個人データ等の取扱いにおける本人関与に係る規律の在り方
・個人データ等の取扱いの態様の多様化等に伴うリスクに適切に対応した規律の在り方
・個人情報取扱事業者等による規律遵守の実効性を確保するための規律の在り方

整合性の確保



データ利活用制度の在り方に関する基本方針

第11回　デジタル行財政改革会議　資料１　抜粋

データ利活用制度の在り方に関する基本方針（案）（概要）

将来像　データとAIが好循環を形成するデータ駆動社会を構築するため制度・システム・運用全体を再設計→人口減を克服しWell-Beingを実現。

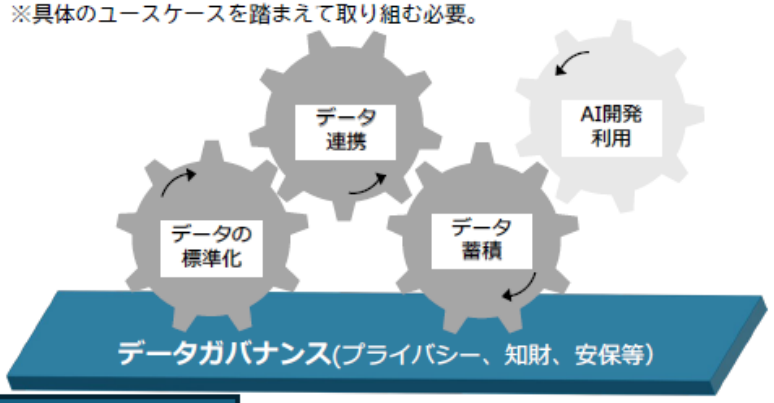
（検討の視点）

- A　データ利活用による新たな価値の創造
- B　リスクにも適切に向き合いつつ AI-Poweredな社会実現
- C　透明性・信頼性の確保（プライバシー、知財、安保等）

※データ利活用と個人情報の適切な保護は不可分一体の関係。

分野横断の取組　① AI活用にも資する円滑なデータ連携を実現するデータ利活用制度構築、②AI開発を含めた統計作成等の場合における同意にとらわれない本人関与の在り方等を含む個情法改正、③官民協働によるユースケース創出の取組を一体的に推進し、データとAIの好循環を形成。
（今後、官民データ活用推進基本法の抜本的な改正、新法などの必要な検討を行い、次期通常国会への法案提出を目指す）

※具体のユースケースを踏まえて取り組む必要。



主な検討事項

データの標準化	○ データ連携を円滑化するため、国が重要分野のユースケースについて標準規格を策定
データ連携の推進	○「データ連携プラットフォーム」制度の構築（個人情報や知財等が含まれるデータを安心して預けられるガバナンス（公平性、競争条件等）を確保） ○ トラスト基盤の整備（事業者の真正性、実在性を確認するため公的な法人認証も対応検討（国際的な相互運用性確保））
データ蓄積・アクセスの円滑化	○ 質の高いデータ収集（社会経済的に重要なユースケースについて義務的手法や補助金誘導等） ○ デジタル公共財の整備
データガバナンス	○ 個人情報保護の適正な取扱い確保（個人の権利利益に対する直接の影響が想定されない取扱いと評価される場合における同意にとらわれない本人関与と必要なガバナンスの在り方、事後的規律の整備など、バランスの取れた早期の個人情報保護法改正）

先行分野の取組

行政保有データの利活用
- 政府におけるデータ利活用の分野横断的な統括機能の確立
- 分野間におけるデータ連携の推進、識別子

医療データ
EHDSを参考にした創薬、医学研究などの二次利用を進めるための包括的・体系的な法制度、情報システムの整備等（来年夏目途に議論、法改正が必要な場合は令和９年通常国会提出を目指す）

金融データ
- 家計の収支管理等の設計・点検を容易に行うために必要な金融情報の見える化に向けた取組を推進
- クレカについて令和7年度中にAPI接続に向けた対応の方向性・工程のとりまとめ

教育データ
自治体を越えた教育データの連携を可能とする認証基盤をGビズIDやJPKIを活用して整備（令和７～８年度に認証基盤の整備に向けた調査・技術実証等）

モビリティデータ
- 標準化や活用事例のベストプラクティス創出推進
- 官民のデータ連携・共有スキームとして「モビリティデータスペース」確立（令和7年度に先行自治体において取組開始）

3．（4）信頼性の高いデジタル空間の構築
①社会全体でのデータガバナンスの構築

- 事業者等においては、その取り扱うデータの価値が最大化されるため、データを適切に利活用する取組や法令遵守はもちろんのこと、プライバシーなど個人の権利利益や自他の知的財産を尊重する取組、データセキュリティのための防護策を講じるなどの取組を総合的に行う**データガバナンス[13]を確保する必要**がある。これは、個人を始めとする関係者の**信頼を確保し、持続的に円滑なデータ利活用を社会的に確立するために必須の課題**であり、全てのデータ保有者、仲介者又は利用者（以下「データ関係主体」という。）におけるデータガバナンスを確保することによって、**データの価値を最大化しつつ、リスクを社会的に受容可能な程度にとどめる**ことが可能となる。

- また、データ連携が拡大し、さらに、多数の AI が協働することも考えられる中、社会全体においても、データの価値を最大化しつつ、リスクを低減していくためには、各データ関係主体におけるデータガバナンスの取組に加え、データのライフサイクルにおいてデータがクラウド事業者による場合などデータ関係主体の制御を離れてアクセスされる可能性があることも想定し、**データの性質等に応じて必要な場合には、秘密計算[14]その他のプライバシー強化技術（PETs）などの技術的手法によって、適切なデータ関係主体によって防護されることが有用**であり、制度面を含めて対応を検討する。その際、PETs 技術の発展に応じて、アジャイルな対応が必要となることに留意する。加えて、AI に関わるガバナンスについては総合科学技術・イノベーション会議、統合イノベーション戦略推進会議、AI 戦略会議などと連携をしながら推進する。

- このような**データガバナンスの取組においては、データの性質や利用目的に応じたリ スクベースの対応を基本**とすることに留意する。一律な規制によってデータ利活用を萎縮させるのではなく、リスクの大きさに応じた制度・技術・運用の柔軟な措置を講ずることにより、安全性と利便性のバランスを確保しつつ、データ駆動型社会の持続 的発展を支えていく。また、その際、データ関係主体の内部においても様々な関係者が存在し、例えば、現場、リスク管理部門又はマネジメント層などそれぞれが**データによる価値創造とリスクの関係について共通の正確な理解**を持つことで、リスクに対する過剰反応でデータ活用を過少としたり、逆に、リスクを正確に共有しないといった事象が発生しないことが必要であることに留意して、取組を進める。

13 文脈によっても多義的であり、例えば、経営者によるガバナンスや、それをコーポレートガバナンスとして推進す る施策を指すこともある。企業等の個々の主体データに係る各種取組を統合的にバランスよく進めるためには、**デ ータを使いこなす能力を高める取組、データに係るリスクに対応するための取組**（法令遵守のための業務プロセス 構築、データセキュリティのためのデータ防護策等）を適切に組み合わせることで効率よく目的を達成する必要が あり、**経営者が経営問題として取り組むことが不可欠となるため、データガバナンスとして一連の取組を促す**もの。

14 データの処理中においても暗号化・秘匿化を行うことが可能なTEE（Trusted Execution Environment）など復号 鍵がチップ内にのみ存在するハードウェア型の秘密計算が世界的に AI 処理にも活用され始めている

3．（4）信頼性の高いデジタル空間の構築 ④データ利活用の前提としての個人情報の適正な取扱いの確保

- データ利活用は、当該データに含まれる個人情報の適正な取扱いを確保することで、個人の権利利益の保護を図りつつ行う必要がある。**個人情報については、我が国 では、個人情報保護法が、いわゆる「一般法」として、その適正な取扱いを通じ、個人の権利利益の保護**を図ってきたが、その在り方については、**情報通信技術の急速な進展や国際的動向、高度化・複雑化し国境をまたぐことも多いデータ利活用の実態等に応じ、不断に見直す必要**がある。
- 例えば、現行法では、個人情報取扱事業者のガバナンスと本人関与による自主的な規律が重視されているが、技術進展等により生まれる従来の想定にない新たな取扱いは、個人の権利利益に対する侵害となる場合だけでなく、それに必ずしも影響しない場合等があり得る。AI の活用が急速に社会全体に広がる現状を踏まえ、**AI開発を含めた統計作成等、特定の個人との対応関係が排斥された一般的・汎用的な分析結果の獲得と利用のみを目的とした取扱いを実施する場面**などのように、**個人の権利利益に対する直接の影響が想定されない取扱いと評価される場合については、そのリスクに応じ、同意にとらわれない本人関与の在り方と必要なガバナンスの在り方について具体的検討**を進める。
- あわせて、データ処理が高度化・複雑化することでその実態が本人からも見えにくく なること等を踏まえ、**個人が安心してデータを提供できる制度とその運用に対する「信頼」が醸成されるよう、個人情報保護法の確実な遵守を担保するため、適切な事後的規律を上記見直しと一体的に整備する必要**があることから、**課徴金、命令、罰則等の様々な手法について、個人の信頼を確保するとともに実効性や経済活動への不当な萎縮効果を避ける観点を含めた全体としてバランスの取れた形[19]での個人情報保護法の改正案について、早期に結論を得て提出**することを目指す。
- 時代により変化する国内外における個人情報の保護・利活用の動向や関連の技術の動 向等について今後とも的確に把握していくため、個人情報保護委員会において、**より包括的なテーマや個人情報保護政策全般について、「個人情報保護政策に関する懇談会」**を通じて有識者やステークホルダーと継続的に意見交換を行う。
- 各府省庁は、その所管分野において、社会的課題の解決や行政事務の効率化等の観点 から、個人情報を含めた多様なデータの利活用に関する政策を企画立案・実施する際 には、**「個人情報等の適正な取扱いに関係する政策の基本原則」**（2022 年 5 月 25 日個人 情報保護委員会。以下「基本原則」という。）を引き続き踏まえるとともに、個人情報 保護委員会においては、**新たに作成した基本原則を解説したガイダンスも活用し、各府省庁に適切な助言を行うことにより、各府省庁との連携を強化**する。

19 2025 年1月 22 日に個人情報保護委員会が決定した**『「個人情報保護法 いわゆる3年ごと見直しに係る検討」の 今後の検討の進め方について』**において、一般法としての個人情報保護法の基本的な在り方の観点から検討すべき 制度的な論点として、**「個人データ等の取扱いにおける本人関与に係る規律の在り方」、「個人データ等の取扱いの態 様の多様化等に伴うリスクに適切に対応した規律の在り方」**及び**「個人情報取扱事業者等による規律遵守の実効性 を確保するための規律の在り方」の各項目が整理**されている。

（参考）デジタル社会の実現に向けた重点計画（抜粋）

（令和７年６月13日　閣議決定）

デジタル社会の実現に向けた重点計画

（２）AI-フレンドリーな環境の整備（制度、データ、インフラ）

① デジタル行財政改革の推進

急激な人口減少に対応するため、利用者起点で我が国の行財政の在り方を見直し、デジタルを最大限に活用して公共サービスの維持・強化と地域経済活性化を進め、社会変革を実現するため「デジタ ル行財政改革取りまとめ 2025[30]」に基づき取組を実行する。国民生活に密着し社会・経済的な重要性が高い分野（教育、子育て、医療、介護、モビリティ、インフラ、防災等）について、利用者起点で規 制・制度の見直しやデジタル活用を進めるとともに、国・地方の共通基盤の整備を推進する。**「データ利活用制度の在り方に関する基本方針[31]」**に基づき取組を加速し、**データとAIの好循環を確立するとともに、横断的な法制度について**官民データ活用推進基本法[32]の抜本的改正、新法など必要な検討を行い、**次期通常国会への法案提出を目指す。これを下支えする個人情報の保護に関する法律（以下「個人情報保護法」という。）**[33]の**改正案についても、早期に結論を得て提出を目指す**。

30 2025 年６月13 日デジタル行財政改革会議決定。
31 2025 年６月13 日デジタル行財政改革会議決定。
32 平成28 年法律第103 号。
33 平成15 年法律第57 号。

（参考）経済財政運営と改革の基本方針2025 （抜粋）

（令和７年６月13日　閣議決定）

経済財政運営と改革の基本方針2025

３．「投資立国」及び「資産運用立国」による将来の賃金・所得の増加

（２）ＤＸの推進

（デジタル行財政改革）

急激な人口減少に対応するため、利用者起点で我が国の行財政の在り方を見直し、デジタルを最大限に活用して公共サービスの維持・強化と地域経済活性化を進め、社会変革を実現するため「デジタル行財政改革取りまとめ2025」[90]に基づき取組を実行する。国民生活に密着し社会・経済的な重要性が高い分野（教育、子育て、医療、介護、モビリティ、インフラ、防災等）について、利用者起点で規制・制度の見直しやデジタル活用を進めるとともに、国・地方の共通基盤の整備を推進する。**「データ利活用制度の在り方に関する基本方針」に基づき取組を加速し、データとＡＩの好循環を確立**するとともに、**横断的な法制度について**官民データ活用推進基本法[91]の抜本的改正、新法など必要な検討を行い、**次期通常国会への法案提出を目指す。これを下支えする個人情報保護法[92]の改正案についても、早期に結論を得て提出を目指す。**

90 令和７年６月13日デジタル行財政改革会議決定。

91 官民データ活用推進基本法（平成28年法律第103号）。

92 個人情報の保護に関する法律（平成15年法律第57号）。

（参考）新しい資本主義のグランドデザイン及び実行計画2025年改訂版（抜粋）

（令和７年６月13日　閣議決定）

新しい資本主義のグランドデザイン及び実行計画2025年改訂版

３．ＧＸ・ＤＸの着実な推進

（２）ＤＸ

⑤データ利活用の推進

データ駆動社会を実現するため、欧米の制度も踏まえつつ、また、プライバシーや知的財産保護、安全保障といった観点にも留意し、横断的な法制度の在り方、個人情報保護法のアップデートの在り方、デジタル公共財の整備について６月に基本的方針をまとめる。また、**横断的な法制度**については、官民データ活用推進基本法の抜本的な改正、新法など必要な検討を行い、**次期通常国会に法案を提出することを目指す。これを下支えする個人情報保護法の改正案についても、早期に結論を得て提出することを目指す。**

医療データについて、創薬等に円滑に利用できる法体系構築に向け検討年限、役割分担等を具体化するとともに、適切な監督やガバナンスの確保、患者本人の関与の在り方（同意の要・不要、患者本人の同意に依存しない在り方を含む。）、二次利用を可能とする情報の範囲等を検討する。金融データについて、個人が自らの家計のストック・フローを容易かつ安全に把握できるよう、利用者起点で取組を推進する。教育データについて、既存の認証基盤を活用し、標準化を進める。産業データを始めとしたデータ連携に必要なトラスト確保等に取り組むとともに、官民協議会を設立し、ユースケースの創出を通じデータ連携エコシステム形成を進める。

デジタル社会形成を担うデジタル庁に、データ政策の司令塔の役割を担わせる。必要な人材の集結など体制を強化し、データ利活用を促進する制度・アーキテクチャ等の検討や各府省庁への規律付け等を通じて、戦略的にデータ政策を推進する。

（参考）統合イノベーション戦略2025（抜粋）（令和７年６月６日閣議決定）

２．第６期基本計画の総仕上げとしての取組の加速
（１）先端科学技術の戦略的な推進
①重点分野の戦略的な推進

（ＡＩ活用の推進）
・統計作成等と整理できるＡＩ開発等における本人同意の在り方や、課徴金等による規律遵守の実効性確保等について検討し、**「個人情報の保護に関する法律（平成15 年法律第57 号）」の改正案を早期に提出**する。

別添 Society 5.0の実現に向けた科学技術・イノベーション政策

４．官民連携による分野別戦略の推進
（１） ＡＩ技術
（戦略的に取り組むべき基盤技術）
≪ＡＩ利活用の促進≫
【実施状況・現状分析】
・個人情報保護法のいわゆる３年ごと見直し規定に基づき、個人の権利利益の保護と個人情報の利活用のバランスを図りつつ検討を進め、 令和７年１月に、制度的な論点の整理を実施。本整理において、ＡＩ開発等を含む統計作成等のみを目的とした取扱いを実施する場合の本人同意の在り方や、経済的誘引のある違反行為に対する実効的な抑止手段である課徴金の導入の要否等の論点を整理。
【今後の取組方針】
・制度的な論点の整理を踏まえ、関係者との対話も重ねながら検討を継続。【個情委】

（参考）規制改革推進に関する答申（抜粋）（令和7年5月28日規制改革推進会議決定）

Ⅲ　投資大国　　1　健康・医療・介護
イ　医療等データの包括的かつ横断的な利活用法制等の整備

我が国においては、令和 22 年（2040 年）頃に向けて、85 歳以上の高齢者の増加や人口減少が更に進む見通しである中、全ての地域・世代の患者等が 適切に医療、介護等のサービスを受けながら自立して日常生活を営めるよう、 地域の実情に応じた効果的かつ効率的な医療提供体制・介護サービス提供体制等を確保することが一層重要であること、また、**患者等本人からの同意取得原則という入口規制が医療等データの利活用の大きな制約になっている との指摘**があること、医療等データの利活用の議論においては、本来実現させるべき姿と制度等の設計とを整合させ、個々の医療等データの最終的な提供主体たる国民の理解を得ることにもつなげることが重要であるとの指摘 があること**、医療等データの利活用法制等の整備等の検討に当たっては基本理念及び制度枠組みを示すことが重要**であるとの指摘があること、ＥＵにおいては令和７年３月に European Health Data Space 規則（以下「ＥＨＤＳ」という。）が発効され、今後数年間かけて戦略的かつ計画的かつ段階的に所要の制度整備、システム整備等が進む見通しであることなども踏まえ、**患者等本人からの同意取得原則という入口規制を、プライバシー等の個人の権利 利益の適切な保護を前提としつつ医療等データの利用者の利活用の段階で 対応するという出口規制の考え方に転換することを含め**、医療等データの包括的かつ横断的な利活用に関する制度及び運用の整備並びに情報連携基盤の構築等の具体化に向けた検討を速やかに進めていく必要があるため、以下の措置を講ずる。

（略）

b 個人情報保護委員会は、個人情報保護法が、いわゆる**「一般法」として、医療等データを含めた個人情報の適正な取扱いを通じ個人の権利利益の 保護**を図ってきたが、情報通信技術の進展、国際動向、利活用の実態等を踏まえて、同法を不断に見直す必要があることを踏まえ、**以下の事項を検討し、結論を得次第、速やかに同法の改正法案を国会に提出**する。

・同法における、**①統計作成等、特定の個人との対応関係が排斥された一般的・汎用的な分析結果の獲得と利用のみを目的とした取扱いを実施す る場合の本人同意**の在り方、**②公衆衛生の向上等のために個人情報を取 り扱う場合**における同意取得困難性要件の在り方、**③病院等による学術研究目的**での個人情報の取扱いに関する規律の在り方を含む、**本人からの同意取得規制の在り方と必要なガバナンスの在り方**。

・同法の**確実な遵守を担保するため、必要とされる事後的な規律を一体的に整備し、全体としてバランスの取れた法制度**とすること。

３．今後に向けて

個人情報保護法サイバーセキュリティ連絡会の開催(再掲)

○ 個人情報取扱事業者等は取り扱う個人データ等につき安全管理措置を講じなければならず、組織的・人的・技術的安全管理措置等を適切に講ずることにより、情報システムに対する外部からの不正アクセス等を防止することが期待されている。

○ しかしながら、近年、個人情報取扱事業者等からの機密情報等の窃取・破壊等を企図したサイバー攻撃は一層高度化・複雑化・巧妙化し、攻撃対象も拡大し続けており、個人データ等の漏えい等の大きな要因となっている。

○ このような情勢の中で、個人情報保護委員会が、データ関係省庁等との連携を強化し、個人情報保護法上求められる各種の安全管理措置として講じ得る方策等について検討・把握するとともに、個人情報取扱事業者等に対する効果的な普及啓発の在り方等を検討する観点から、「個人情報保護法サイバーセキュリティ連絡会」を令和６年12月から開催。

１．開催目的等

・個人情報保護法上求められる各種の安全管理措置として講じ得る方策等について検討・把握するとともに、個人情報取扱事業者等に対する効果的な普及啓発の在り方等を検討するため、四半期ごとに行う。

２．検討事項

・直近の漏えい等報告や指導の状況（四半期公表内容。不正アクセスによる個人データ等の漏えい等事例を含む。）を説明し、専門的見地から個人データ等の漏えい等の対策や留意すべき点等について、助言を得る。
・その他、安全管理措置の実施方策や効果的な普及啓発の方法に係る情報交換を実施。

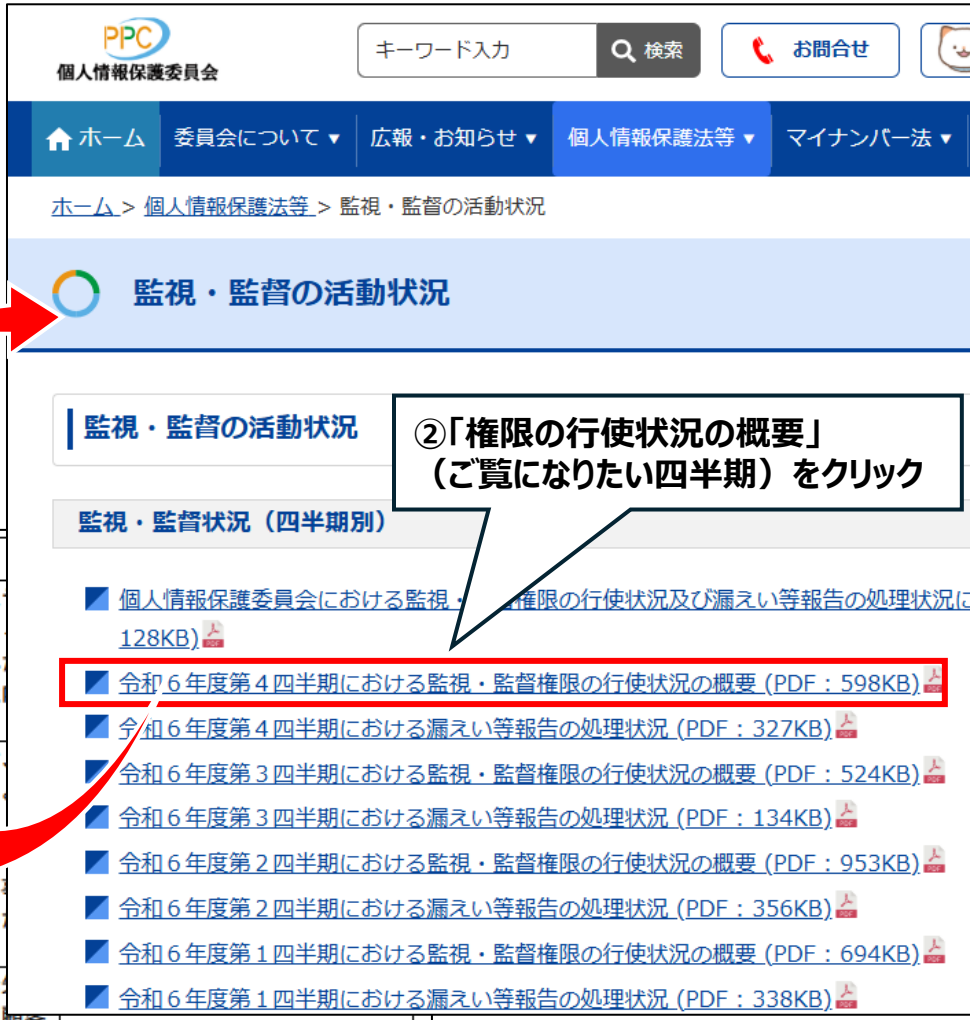
３．参加機関

・内閣官房　国家サイバー統括室（NCO）
・警察庁サイバー警察局
・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（JPCERT/CC）
・個人情報保護委員会事務局
（JPCERT/CC以外は、当委員会との覚書締結機関）

※「個人情報保護法サイバーセキュリティ連携会議」及び「特定個人情報セキュリティ関係省庁等連絡協議会」は、上記以外の省庁・機関も幅広く含む連携会議/連絡協議会として今後も開催（年1回開催）

（参考）四半期毎の状況公表

○個人情報保護委員会ホームページ（https://www.ppc.go.jp/index.html）



	事案の概要	
1	事業者が利用していたITインフラが不正アクセスを受け、事業者の顧客、従業者及び取引先の個人データについて漏えいのおそれが生じた事案。当該ITインフラのアクセス検証の際に用いたセキュリティ脆弱な検証用アカウントが削除されず残置され、当該アカウントから当該ITインフラに侵入され、と、事業者が当該ITインフラの利用のため使用しているNAS（Network Attached Storage）が、社内ネットワーク内ではユーザ認証を経ずにアクセス可能な状態であったこと等が原因と考えられる。	
2	事業者が運営している施設のウェブサイトがSQLインジェクション攻撃による不正アクセスを受け、データベース内の個人データが窃取され、顧客の個人データについて漏えいが生じた事案。事業者にSQLインジェクション攻撃への対策が不十分であったことが原因と考えられる。	
3	事業者が提供するクラウドサービスを構成するサーバが不正アクセスを受け、当該サーバに保いた、委託元である事業者の従業者及び顧客の個人データについて漏えいのおそれが生じた事案。者のファイアウォールの通信設定に不備があり、外部から制限なくアクセス可能な設定となっていと等が原因と考えられる。	
4	事業者が販売する商品の発送業務及びそれに伴う個人データの取扱いを委託していたところ、委託ある事業者の倉庫管理システムが、不正アクセスを受け、ランサムウェアに感染した結果、事業者の顧客の個人データについて漏えいのおそれが生じた事案。事業者は、約７年間、委託先である事業者に個人データの取扱いを委託していたところ、発送に使用した顧客の個人データの保持状況（廃棄状況）について定期的な確認を一切しておらず、その結果、多数の顧客の個人データについて漏えいのおそれが生じたため、委託先の監督について不備が認められた。	委託先の監督
5	事業者のサーバがVPN経由で不正アクセスを受け、ランサムウェアに感染した結果、ファイルが暗号化され、従業者及び顧客の個人データについて毀損及び漏えいのおそれが生じた事案。サポート切れのVPN	技術的安全管理措置（外部からの不正アクセス等の

③委員会が指導した個別の事案の概要をとりまとめて公表

WARNING

不正アクセスによる個人データ
漏えい防止のための注意喚起

令和６年12月11日

PPC 個人情報保護委員会
Personal Information Protection Commission

1

発生事例から学ぶセキュリティ対策

個人情報保護委員会には、これらの手口によって発生した個人データの漏えい等事案が複数報告されている状況です。
報告された事案を分析したところ、以下８つの事例に類型化できる問題点が挙げられ、これら問題への措置が十分でない場合、安全管理措置（法第23条）、従業者の監督（法第24条）及び委託先の監督（法第25条）の違反と判断される可能性があります。
これらの事例の多くは、委託先等を含め、個人情報取扱事業者内外における複数の組織・部署が関係することから、その問題点を克服するためには、単純な技術的問題への対応にとどまらず、経営層を交えた組織的な対応が必要となります。個人情報取扱事業者におかれては、今回紹介する事例の原因及び対策も参考にし、必要なセキュリティ対策を行っていただくよう、お願いします。

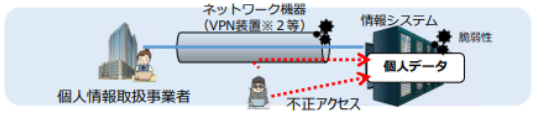
<事例>

- 事例１　脆弱性が放置された事例
- 事例２　脆弱性への対応が遅れた事例
- 事例３　不正ログインの事例
- 事例４　グループ会社や海外拠点が狙われた事例
- 事例５　グループ会社間のアクセス制御不備があった事例
- 事例６　個人領域に保存していたデータの漏えい事例
- 事例７　グループ会社への監督が不十分な事例
- 事例８　利用するクラウドサービスからの漏えい事例

3

事例１　脆弱性が放置された事例

個人情報取扱事業者が個人データを取り扱うために導入した情報システムについて、定期的にソフトウェア等を最新状態に保つための措置を適切に行わず、さらに、脆弱性が公開され対処方法がリリースされていたにもかかわらず、対策を放置していたことで、不正アクセスによる個人データの漏えい等を防ぐことができなかった。



原因

- ✓ システム業者との間で、情報システム導入の業務委託契約しか締結しておらず、セキュリティ対策に関するシステム保守の業務委託契約を締結していなかった。
- ✓ グループ会社の間で脆弱性対策を行う役割分担が明確化されておらず、結果的に放置してしまった。
- ✓ 特に、VPN 装置等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多い。

対策例

- ✓ 適切なシステム業者を選定し、情報システムの脆弱性対策等のセキュリティ対策も含めたシステム保守の業務委託契約を締結する。
- ✓ (1)管理対象となるIT資産の洗い出し、(2)脆弱性情報の収集・分析、(3)脆弱性への対処といった脆弱性対策プロセスを確実に行う。
- ✓ VPN 装置は、それ自体が意識的に利用・管理されるサーバ等と異なり、ネットワークサービスの一部として提供されるケースもあり、運用体制や脆弱性対応の責任が不明瞭なケースも多く、グループ会社内及び外部委託先との役割分担を明確化することが重要である。

※２　仮想プライベートネットワーク（Virtual Private Network）の略称であり、離れた拠点間を仮想的な専用線でネットワークでつないで通信できるようにするための仕組み。

4

事例８　利用するクラウドサービスからの漏えい事例

クラウドサービス提供事業者が提供する業務システムが不正アクセスを受け、クラウド環境で管理されていた多数のクラウドサービス利用者である顧客企業の個人データが暗号化され、大量の個人データの漏えいのおそれが生じた事案。

原因

- ✓ クラウドサービスの外部からの不正アクセス等の防止のための措置等の技術的安全管理措置に問題があった。
- ✓ 業務の委託ではないクラウドサービス利用は個人データの取扱いの委託には該当しないと考えていたため、委託先に対する個人データの取扱状況の監督を実施していなかった。

対策例

- ✓ 顧客企業は、利用しようとするクラウドサービスにて適切なセキュリティ対策が講じられているか、サービス利用規約やクラウドサービスの安全性評価に関する資料等により確認し、適切なサービスを選定する。
- ✓ クラウドサービス利用が個人データの取扱いの委託となる場合、利用する顧客企業が適切に取扱状況を把握できるよう、クラウドサービス提供事業者は積極的にセキュリティレポート等の必要な情報を公開することが望ましい。

11

出典：https://www.ppc.go.jp/files/pdf/241211_warning.pdf

中小企業・小規模事業者・個人事業主の皆さま

不正アクセスによる個人情報の漏えい等にご注意ください!!

●漏えい等の少なくない割合が、不正アクセスによるものです。
※個人情報保護委員会への漏えい等報告の約30%（令和6年度上半期）

●不正アクセスは中小企業でも発生しています。
※サーバやサイト等に不正アクセスを受けた経験のある中小規模事業者は約2%
（令和6年度中小規模事業者における個人情報等の安全管理措置に関する実態調査）

●不正アクセスの被害は甚大です。
▶いざ漏れたら、お客様の大切な個人情報が危険にさらされます。
▶事業者としても、様々な緊急の対応が求められます。
（原因究明、被害者への連絡、二次被害の防止、再発防止策）

しかし、小さな注意で防げることも多々あります

パスワードを強化しよう！

パスワードは、「長く」「複雑に」「使いまわさない」ように強化しましょう！名前、電話番号、誕生日や簡単な英単語等をパスワードには使わないようにしましょう！

OSやソフトウェアは、常に最新状態にしよう！

古いバージョンのまま放置していると、セキュリティ上の問題が解決されず、脆弱性を悪用した不正アクセスの危険性があります！

ウィルス対策ソフトウェアを導入しよう！

ウィルス対策ソフトウェアを導入するとともに、ウィルス定義ファイルを常に最新の状態にしましょう！

以上の3つから始めてみませんか！

PPC 個人情報保護委員会
Personal Information Protection Commission
TEL 03-6457-9849（個人情報保護法相談ダイヤル） URL https://www.ppc.go.jp/

※令和4年4月より、漏えい等報告・本人通知の義務化が始まっています。
一度個人情報保護委員会のホームページを確認しておきましょう！▶

令和6年12月時点

令和6年度に実施した調査からこんなことが分かっています

中小規模事業者の個人情報保護対策はまだまだ不十分！

【社内での課題】
- 何をしてよいかわからない・・・40%
- 情報セキュリティ対策・・・19%
- 個人情報保護法等の理解不足・・・27%
- 電子化による管理の難易度上昇・・・17%

不正アクセスにより、こんな被害が生じています

- システム等の停止・・・34%
- 顧客・取引先情報の漏えい・・・9%
- クレジットカード情報等の漏えい・・・17%
- データの改ざん・・・7%

対応の未実施や不注意が不正アクセスを招いています

- OSやソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生するサイバーセキュリティ上の欠陥（脆弱性）を放置していた・・・26%
- 実在のサービスや企業を騙ったフィッシングサイト（偽サイト）へ誘導する電子メールのURLにアクセスし、アカウント情報（ID・パスワード）等を入力してしまった・・・24%
- セキュリティ対策ソフト等を導入していなかった・・・4%
- パスワードの設定に不備があった・・・2%

一方で！ 安全管理措置に関して取り組んでいただいている事業者もみられます

- ウィルス対策ソフトウェアの導入・・・42%
- ウィルス対策ソフトウェアの自動更新などによる最新状態の維持・・・44%
- 個人データが記録された媒体（紙・USB・パソコンなど）を復元不可能な手段で廃棄・・・34%

個人情報保護の意識の向上、体制の整備、安全管理措置の取組をよろしくお願いします

参照コンテンツ

漏えい等報告・本人への通知の義務化について
https://www.ppc.go.jp/news/kobetsu_feature/roueitou_houkoku_gimuka/

お役立ちツール 中小企業向け
https://www.ppc.go.jp/personalinfo/legal/

はじめての個人情報保護法 シンプルレッスン
https://www.ppc.go.jp/files/pdf/simple_lesson_2022.pdf

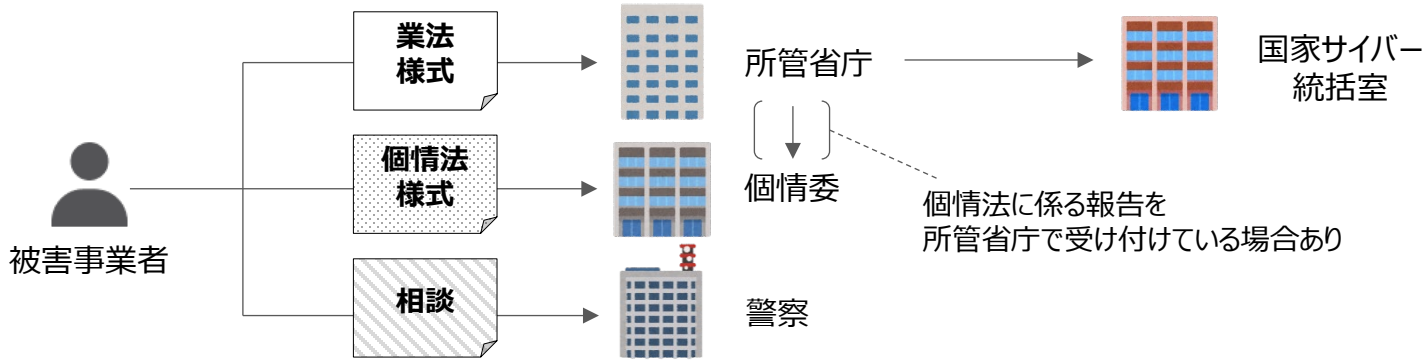
令和6年度中小規模事業者における個人情報等の安全管理措置に関する実態調査結果
https://www.ppc.go.jp/news/survey_report/

出典：https://www.ppc.go.jp/files/pdf/241205_chuushou_leaflet.pdf

報告一元化の実現に向けたタイムライン

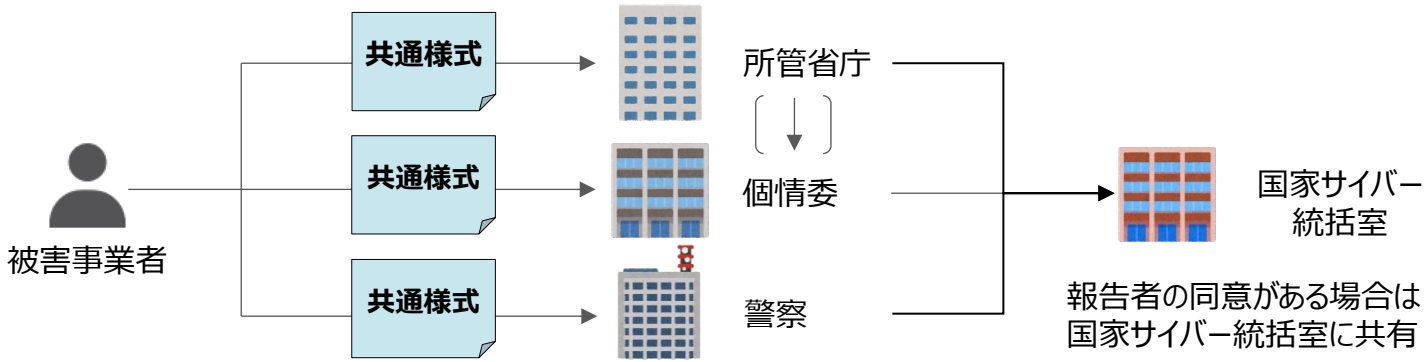
現状

関係政府機関に対して、
個別の様式で
それぞれ報告等を行う必要



DDoS攻撃・ランサムウェア
報告様式の統一
（周知期間等を経て
本年10月1日から実施）

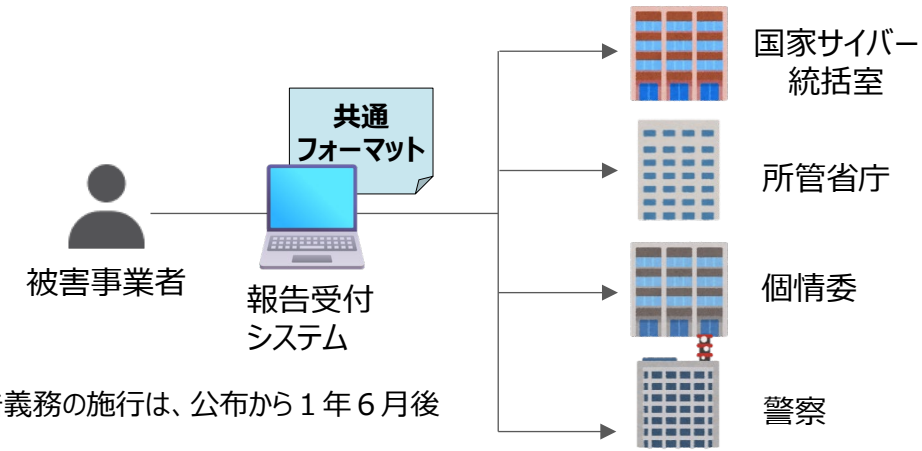
DDoS攻撃・ランサム事案発生時の
関係省庁への**報告様式を統一**



報告窓口の一元化

（システム整備を進め
新法の報告義務施行に併せ実施）

システムを活用し、
新法の報告窓口を一本化。
関係省庁への共有も可能に。



※　報告義務の施行は、公布から１年６月後

今後に向けて考慮していくべき点

より包括的なテーマや個人情報保護政策全般について、中間整理に対する意見募集の結果や、検討会報告書、事務局ヒアリングの結果等を踏まえ、今後ともステークホルダーと継続的に議論を行うとともに、業務の遂行にあたり、例えば、以下のような点を考慮していくことが必要である。

⑴ デジタル化に対応した個人情報取扱事業者のガバナンスの向上
適切なデータ利活用を推進できる体制整備
（PIA（個人情報保護評価）実施・DPO（データ保護責任者）設置等を含む）
人材育成等）

⑵ 個人・消費者と事業者との信頼（トラスト）の醸成・向上

⑶ 官民を通じたデータ利活用の推進、適切な企業・組織間連携

⑷ 民間の自主的取組へのインセンティブ、認定個人情報保護団体に関する取組

⑸ 本人関与の在り方という観点からの更なる整理
（プロファイリング、データポータビリティ等）

⑹ 保護法益に応じた個人情報・個人データの範囲や規律の対象となる行為

「個人情報保護政策に関する懇談会」の開催

1　開催趣旨

個人情報の保護及びその利活用のバランスの在り方は国民各層にとって重要な課題であり、その重要性は以前にも増して高まっている。そのようなバランスの在り方を考え、時代に即した個人情報保護制度の運用や見直し等を行うに当たっては、委員会として、**デジタル社会の進展やAIの急速な普及を始めとした技術革新、技術の社会実装に関する動向、国内外における個人情報の保護・利活用に関する動向等について的確に把握**していく必要がある。

このため、**広く各界の有識者やステークホルダーと透明性のある形で継続的に意見を交換**し、併せて**個人情報保護政策に関し相互理解を促進**することにより、**実情に即した、より包括的なテーマや個人情報保護政策全般についての検討**に資する。

2 想定されるテーマ

・個人情報保護政策全般について
・個人情報保護・利活用に関する技術の動向
・監視・監督活動の在り方
・国際連携の強化 等

3 会　員

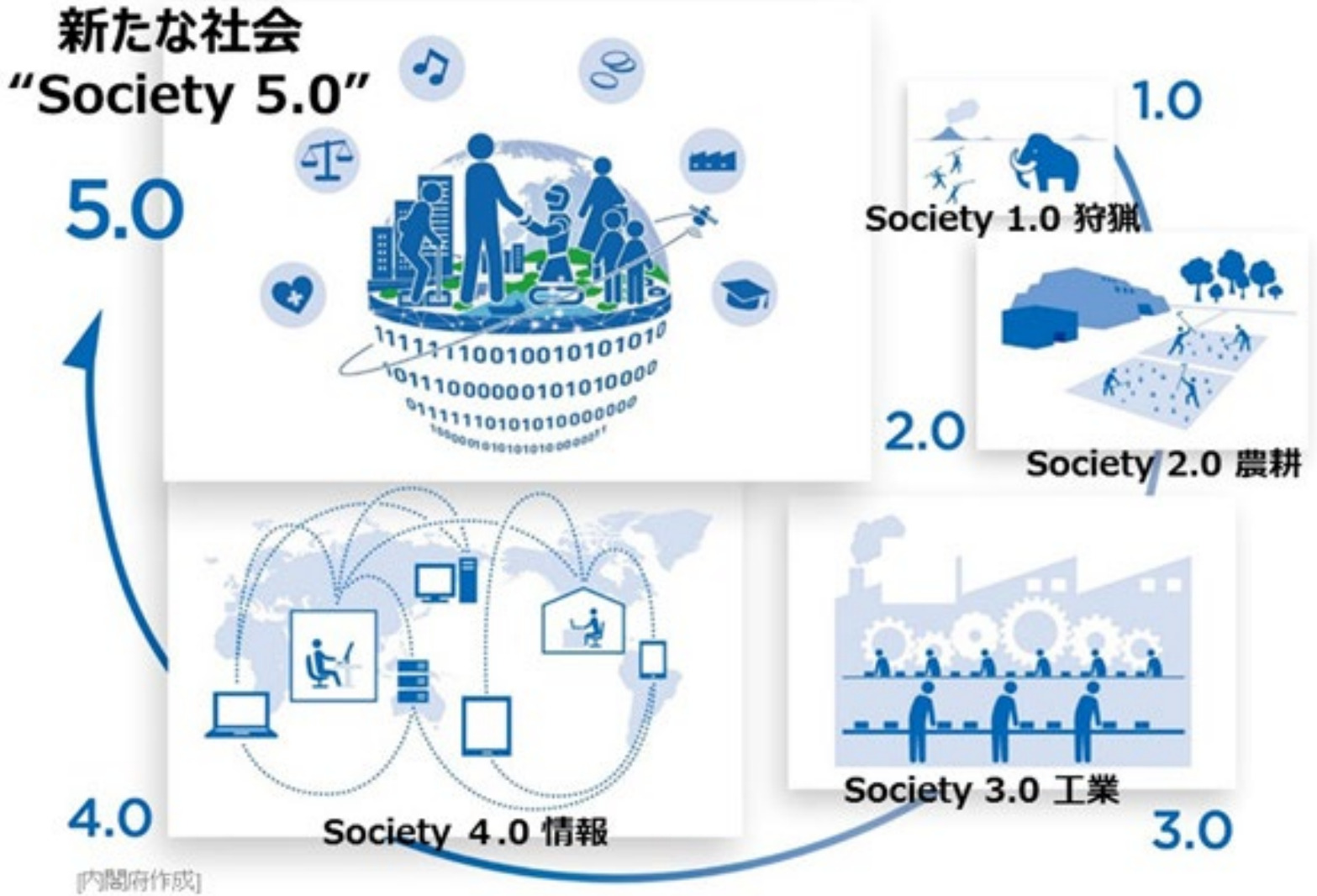
・有識者、法曹、経済団体、消費者団体、地方公共団体

4　開催状況

第1回　令和7年9月19日（事業者等の自主的取組とそれへのインセンティブについて）

Society 5.0を支える適正なデータの利活用

サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）



出典：http://www8.cao.go.jp/cstp/society5_0/index.html

Thank you !

Kuniko Ogawa