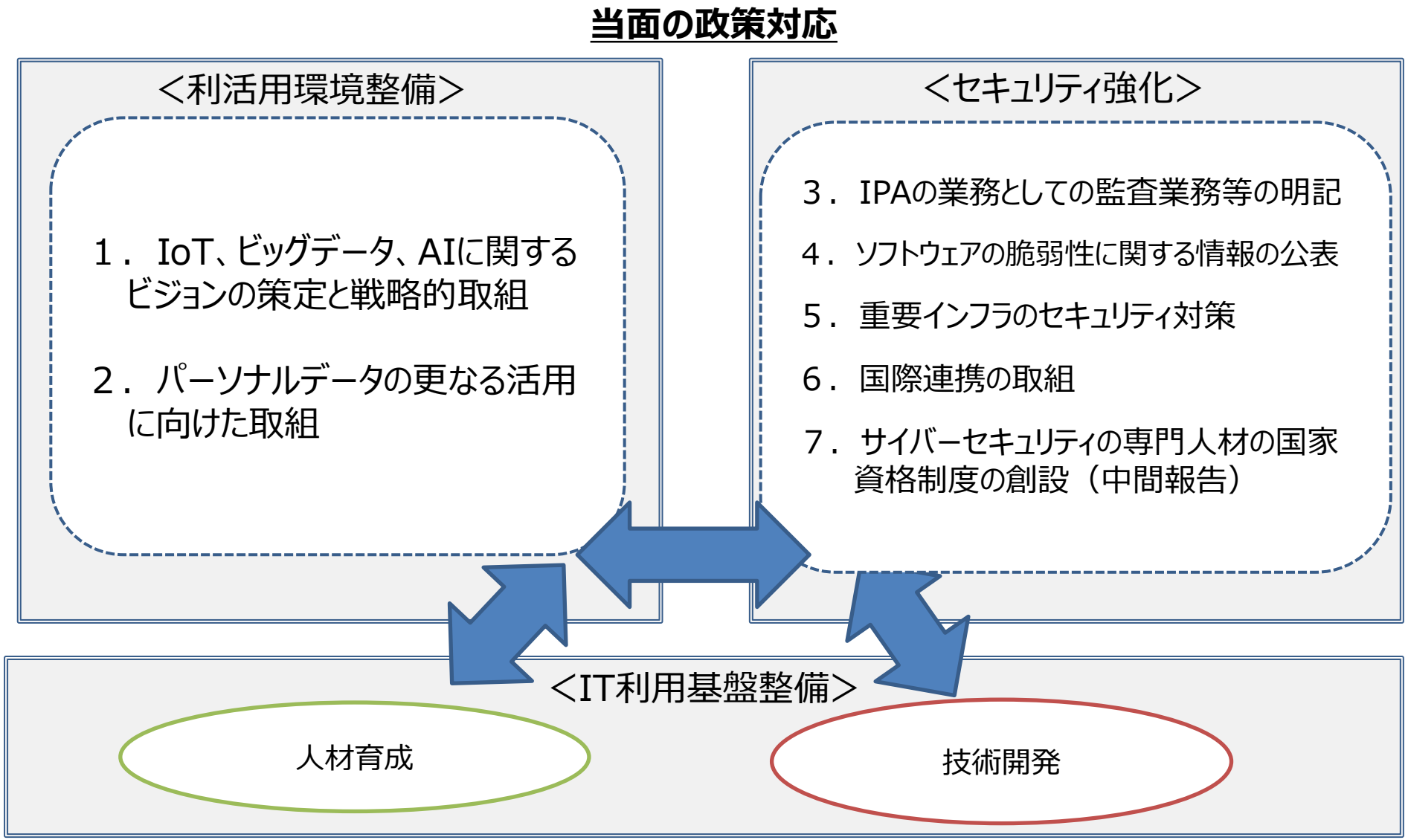
資料2

IoT社会に向けたデータ利活用施策及び
サイバーセキュリティ戦略を受けた今後の対応

2015年9月29日

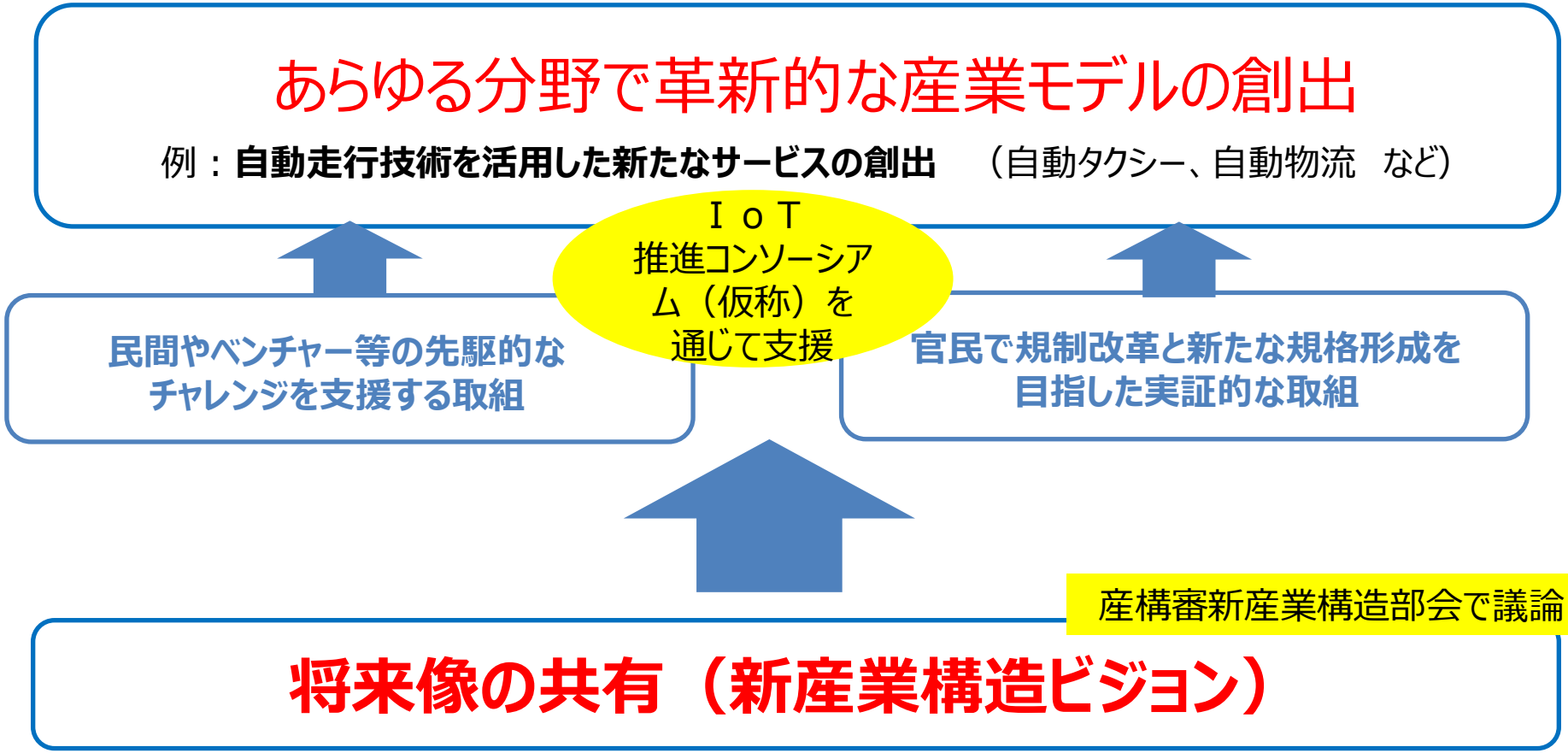
商務情報政策局

０．IoT社会に向けた取組



１．IoT、ビッグデータ、AIに関するビジョンの策定と戦略的取組

- 官民で規制改革と新たな規格形成を目指し、各分野ごとに実証的な取組を推進するとともに、ベンチャー等のＩｏＴを活用したベンチャー等の先駆的なチャレンジを支援。
- このため、官民の羅針盤としてＩｏＴ、ビッグデータ、人工知能の進展を踏まえた2030年の「新産業構造ビジョン」の策定を開始。



参考　IoT推進に向けた研究開発・実証事業

平成２８年度概算要求額　138.6億円（新規）

事業の内容

事業目的・概要

- IoT（モノのデジタル化・ネットワーク化）の進展によって、これまで得られなかった様々なデータの収集が可能となり、こうしたビックデータを人工知能（AI）等によって解析することで、新たな知見・発見を生み、それを実社会にフィードバックすることで新たな価値が創造される社会が現実的になりつつある。
- こうしたIoTの進展は、あらゆる産業において、ビジネスモデルの革新をもたらす可能性があり、諸外国においても国を挙げて環境整備に向けた取組が進められているところ。我が国においても、早急に、（１）分野横断的な共通基盤技術の研究開発、（２）各分野に関する実証事業を通じた新たなビジネスモデルの創出を図り、我が国産業の競争力強化の基盤を整備する。

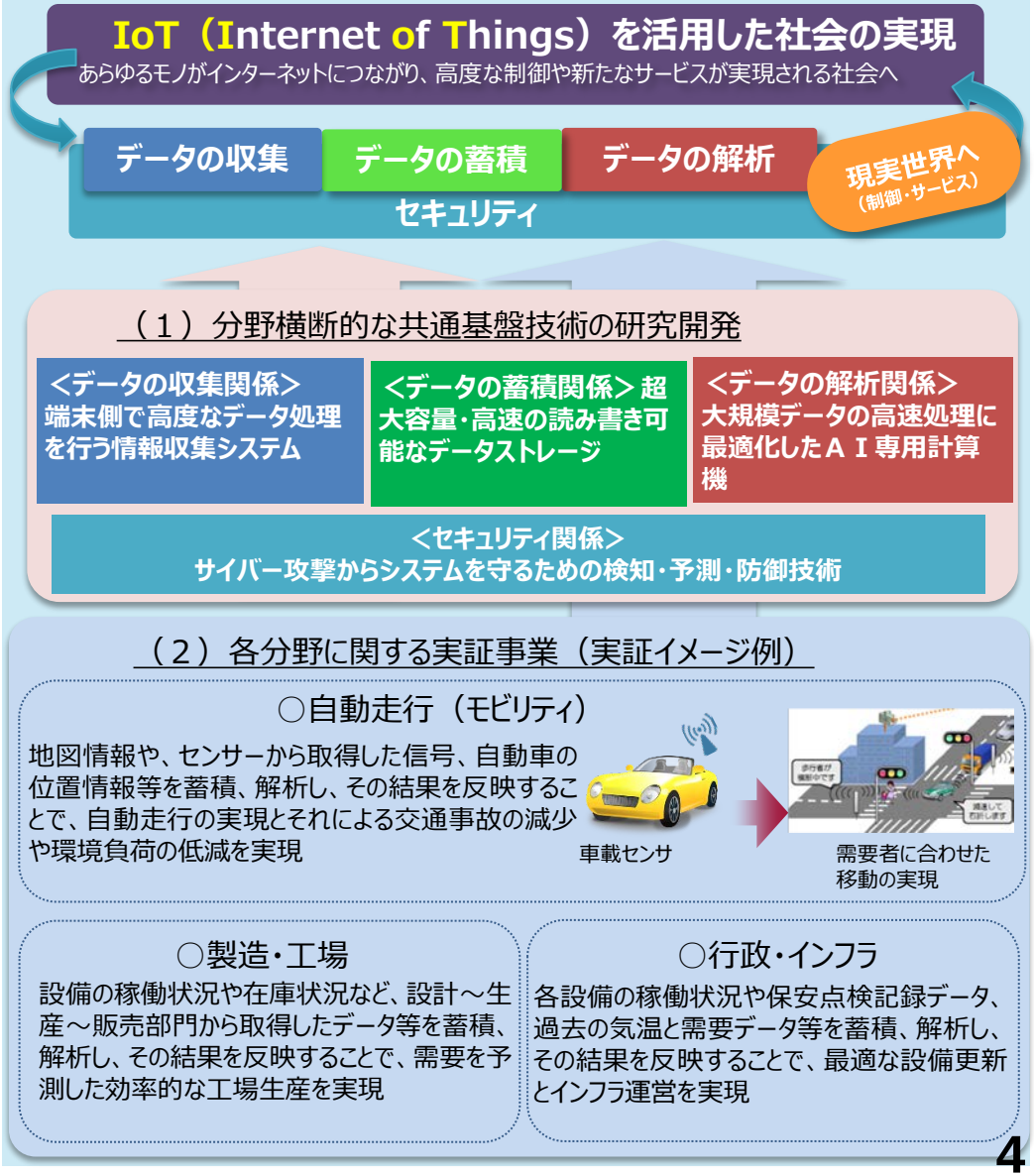
（１）IoT推進のための横断技術開発プロジェクト等

データ収集・蓄積・解析等に係る技術について、従来に比べて格段に省エネルギーで高度なデータ利活用を可能とする次世代技術を産学官連携で開発。

（２）IoT推進のための社会システム推進事業等

製造、モビリティ、医療・健康、流通・宇宙、地域社会インフラ、行政等の各分野におけるビックデータを活用した実証等を行い、新たなビジネスモデルの創出を促す。

事業イメージ



参考　産業構造審議会 「新産業構造部会」の設置

※2015年9月17日第一回開催

産業構造審議会　総会

新産業構造部会

【検討事項】

①［具体的な変革の姿］
　ＩｏＴ・ビッグデータ・人工知能等のもたらす産業構造、就業構造、経済社会システムの変革がどのようなものか。

②［変革のインパクト］
　これらの変革が、どのようなチャンス（リスク）を生み出し、経済社会レベルでどのような課題の解決・制約の克服に寄与するか。

③［海外の動向の把握］
　各国政府や海外のプレーヤーはどのような戦略を持ち、どのような対応を進めていくのか。

④［具体的な処方箋］
　政府や民間企業、さらに個々人はどのような戦略を持ち、どのような対応を進めていくか。

について、**２０３０年における経済社会システムのあるべき姿（「新産業構造ビジョン」）を提示。**

２．パーソナルデータの更なる活用に向けた取組

- 個人情報保護法が改正され、個人情報利活用のための基盤が整備されたところであり、今後具体的な制度設計を進めていく必要。
- 一方、更なる利活用のためには、データを提供する個人と情報を取得する者との信頼関係を構築しつつ、事業者の自主的な取組を推進していくとともに、個人の権利を実質的に侵害する可能性が低いと考えられる場合であって匿名化等が現実的に難しいと考えられるケースについて対応を検討していくことが必要。

分類	課題	対応
①事業者の自主的な対応を促進していくべきもの	データ取得・利活用に当たって、事業者と消費者との信頼関係をどのように構築するか。また、分野による特殊事情にどう対応するか。	• オンライン上の同意取得等ガイドライン策定（昨年１０月） • 今後、分野の特性に応じたルール形成を進めていくことが重要。
	データの提供が可能なデータ流通の知見に乏しい事業者間の取引をどのように促進するか。	• データ取引促進のためのガイドラインを策定
②個人情報保護法上、規程が明確でないため萎縮しているもの	個人情報の種類が明確でない。	• 保護法改正によって対応済み。 • 今後、具体的な運用を明確にしていく必要。
	どこまで処理すれば個人情報でなくなるのか、匿名化の程度が明確でない。	
	利用目的の変更範囲が極めて限定的に解釈されている。	
③更なる個人情報の利活用のために検討すべきもの	個人の権利を実質的に侵害する可能性は低いと考えられるものの、同意取得や匿名化が現実的に難しいと考えられるケース（別紙）がある。	• 今後、同意取得との関係整理などを検討していく必要。

別紙　更なるデータ利活用を検討すべきケース

①不特定多数の人に同意を取ることが現実的ではない場合

＜例＞

- 様々な駐車場の防犯カメラのデータを大量に読み込み、多様な駐車場の駐車枠を識別して、駐車場内で自動駐車を制御する人工知能エンジンの開発を行うケース。

＜例＞

- 大量の顔画像を収集し、読み込み、防犯のための顔画像を認識する人工知能エンジンの開発・高度化を行うケース。

②最終的には匿名加工するが、分析段階では個人情報である方が精度が高い場合

＜例＞

- 別々の機関が保有する、事故車の損傷データと当該事故車のドライバーの負傷状況を掛け合わせることで、車の損傷状況を把握してドライバーの損傷程度を自動的に検証し、救急手段を選択する緊急サービスの改善に用いるケース。

参考　事業者と消費者の信頼関係構築のための取組

ガイドライン策定＋国際標準化

パーソナルデータを利活用したビジネスにおいて、データの取得時に事業者が消費者の理解を十分に得ないままにパーソナルデータの利活用を進めた結果、消費者の不安や混乱を招かないよう、消費者への情報提供・説明を充実させるための指針となる**「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」**を策定。(2014年10月)。2018年を目標に**国際標準化**を進めている。

相談体制の構築

事業者に対して、消費者のよりよいサービス選択に資する情報提供を促す仕組みとして**「事前相談評価」**を構築。（2013年9月）

HEMSにおける取組

ＨＥＭＳデータを利活用してサービスを提供する事業者、および、今後当該サービスへ参入する事業者が、個人情報保護等の観点から留意すべき点について取りまとめたマニュアルを策定予定。（2016年3月末予定）

マルチステークホルダープロセスの活用

マルチステークホルダープロセスとは

事業者・消費者の各代表者及び有識者等の利害関係者が参画するプロセスにおいて、それらの意見を踏まえたルール策定等を行う方法のこと。

改正個人情報保護法における規定

匿名加工情報に係る作成方法等につき、消費者の意見を代表する者その他の関係者の意見を聴いて個人情報保護指針が作成されるよう努めるべきと定められ、マルチステークホルダープロセスの考え方の活用を規定。

試行的検討の実施

同プロセスの有効性と課題を明らかにして実施手法等を検討することを目的として、事業者、消費者代表及び有識者からなる検討会を設置し、2015年1月から3月にかけて、クレジットカード会社及び加盟店が行う各種サービスをユースケースとして、個人情報の匿名加工方法に関し、同プロセスを試行的実施。報告書を取り纏め、公表（同年5月）。

参考 「データに関する取引の推進を目的とした契約ガイドライン」策定

背景・経緯

- 昨今、ビッグデータの分析手法が確立されたことにより、これまで価値が見出されず利活用がなされてこなかったデータについての価値と利活用への期待が高まっている。他方、それらのデータを保有しながらも利活用実績がない事業者は、取引のノウハウを有しないため、事業者間のデータの利活用が期待されるほどには進んでいない。

DDI

- **「データ駆動型ドリブンイノベーション創出戦略協議会」**の中間とりまとめにおいて、契約交渉に要する時間、労力を削減する観点から、データ取引時に参考となる契約雛形の策定を提言(2014年11月)

成長戦略

- **「日本再興戦略』改訂2015」**においても契約モデルの必要性を記載
  『大量のパーソナルデータやサプライチェーンの各工程間の取引情報等のビッグデータを活用した新たなビジネスモデルの創出等に向け、**企業間データ連携・共有を促進するための標準契約モデルを本年度内に策定する**（2015年6月)』

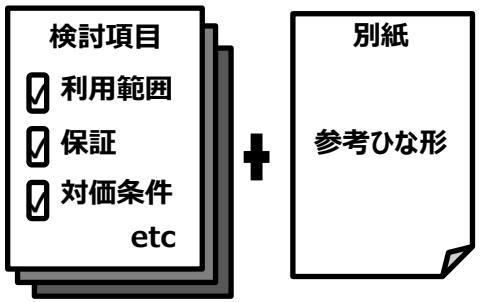
目的、概要

◆目的

① データに関する取引における事業者の契約検討、契約交渉労力の軽減
② 契約交渉の負担軽減による、データに関する取引の活性化
③ 取引開始後の予期せぬトラブルの抑止

◆概要

・データに関する取引に係る契約の検討項目と参考ひな形で構成
・検討項目では、**「データの利用範囲」、「保証」、「対価条件」**等、データに関する取引に係る契約において留意すべきポイントを整理



参考　個人情報の保護に関する法律（現行）の概要

- 2003年5月に成立、2005年4月に施行。
- 個人情報とは、「生存する個人に関する情報で、特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」をいう。
- 5,000人分を超える個人情報を取り扱う事業者が法律に基づく義務の対象。一般私人や小規模取扱事業者は規制の対象外。

主要な義務規定

○　利用目的に関する規律

・ 個人情報の利用目的の特定（§15）、目的外利用の禁止（§16）
　個人情報を取り扱うに当たっては、利用目的をできるだけ特定し、原則として、あらかじめ本人同意を得ないで、その目的の達成に必要な範囲を超えて個人情報を取り扱ってはならない。

・ 適正な取得（§17）、取得時の利用目的の通知等（§18）
　偽りその他不正な手段によって個人情報を取得してはならず、取得時は本人へ速やかに利用目的を通知又は公表しなければならない。また、本人から直接書面で取得する場合は、あらかじめ本人に利用目的を明示しなければならない。

○　第三者提供の制限

・ 第三者提供の制限（§23）
　あらかじめ本人の同意を得ないで本人以外の者にデータを提供してはならない(ただし、例外規定あり)。
※委託、事業承継及び共同利用の場合は相手方は第三者に該当しない。

○　事故防止のための措置

・ 安全管理措置（§20）、従業者・委託先の監督（§21-22）
　データの漏えいや滅失を防ぐため、必要かつ適切な技術的・組織的な保護措置を講じなければならず、また安全にデータ管理するため、従業者や委託先へ必要・適切な監督を行わなければならない。

参考　改正個人情報保護法の概要(本年９月成立)

背景

- 情報通信技術の進展により、膨大なパーソナルデータが収集・分析される、ビッグデータ時代が到来。
- 他方、個人情報として取り扱うべき範囲の曖昧さ（グレーゾーン）等のために、企業は利活用を躊躇。
- また、国境を越えて大量のデータが移転される機会が増大し、円滑な移転のために国際整合的な制度の整備が必要に。
- 一方で、いわゆる名簿屋問題等により、個人情報の取り扱いについて一般国民の懸念も増大。

改正のポイント（平成２７年９月から２年以内に全面施行）

１．個人情報の定義の明確化	・個人情報の定義の明確化（身体的特徴等が該当） ・要配慮個人情報に関する規定の整備
２．適切な規律の下で個人情報等の有用性を確保	・匿名加工情報に関する加工方法や取扱い等の規定の整備
３．個人情報の保護を強化（名簿屋対策等）	・トレーサビリティの確保（第三者提供に係る確認及び記録の作成義務） ・不正な利益を図る目的による個人情報データベース提供罪の新設
４．個人情報保護委員会の新設及びその権限	・個人情報保護委員会を新設し、現行の主務大臣の権限を一元化 ・個人情報保護指針の作成や届出、公表等の規定の整備
５．個人情報の取扱いのグローバル化	・国境を越えた適用と外国執行当局への情報提供に関する規定の整備 ・外国にある第三者への個人データの提供に関する規定の整備
６．その他改正事項	・本人同意を得ない第三者提供(オプトアウト規定)の届出、公表等厳格化 ・利用目的の変更を可能とする規定の整備 ・取り扱う個人情報が5,000人分以下の小規模取扱事業者への対応

参考 サイバーセキュリティ戦略（平成27年9月4日閣議決定）を踏まえた主な取組

政府機関を守る取組

予算 制度 国による監視・監査・調査の対象を、独立行政法人・府省庁と一体となり公的業務を行う特殊法人等に拡大

重要インフラを守る取組

予算 **情報共有体制の強化**：IPAが企業から収集した攻撃情報を解析、迅速に共有することにより被害拡大を防止

予算 **サイバーレスキュー隊の派遣**：事業者が攻撃の発生を通報した場合、政府が支援・実態解明を進める。得られた情報は、関係者間で積極的に共有。

ガイドライン **制御系対策（技術基準や保安規定の整備）**
制御システムやスマートメーターのセキュリティリスクに対応するため、新たな対策ガイドライン等を策定

企業を守る取組

ガイドライン **経営ガイドラインの策定**：
最新の攻撃情報を踏まえた対策等の重要性を経営層に認識してもらうためのガイドラインの策定、同ガイドラインに基づく第三者認証を実施予定

予算 **IoTシステムのセキュリティに係る制度整備・技術開発**：
エネルギー・自動車・医療分野等に活用できるセキュリティに係る総合的な基準整備及び技術開発

広報 **普及啓発活動の実施**：各種セミナーの実施等。最新の攻撃手口の共有体制提供等の支援

基盤整備のための取組

人材の育成：
予算 若年層の優秀なセキュリティ人材の早期発掘イベントの拡充
予算 独創的なアイディアと技術を活用する突出した能力を持つ若年層の人材を発掘・育成
制度 情報処理技術者試験を活用し、実践的能力を適時適切に評価できる資格制度の創設

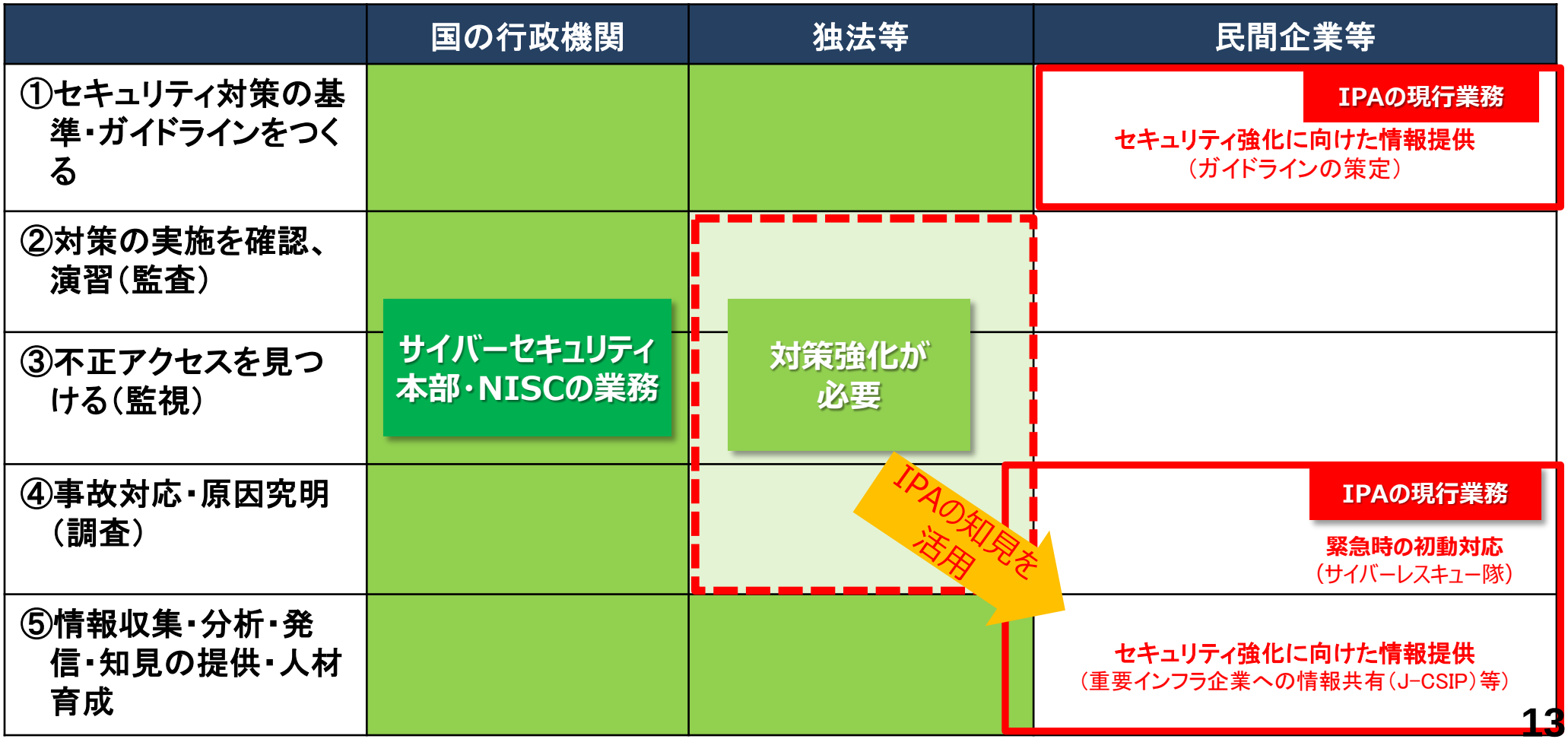
脆弱性情報の収集・公表：制度 ソフトウェアの脆弱性に関し、開発者の同意がない場合も、必要に応じ公表

政府系ファンド等の活用：その他 政府系ファンドの活用により、セキュリティ企業の競争力強化

国際連携の強化：その他 幅広い分野で国際協力体制を確立し、サイバー空間の安全を確保

3．サイバーセキュリティ対策強化に係るIPAの業務

- サイバーセキュリティ戦略では、現在、国の行政機関に対して実施している監視・監査・原因究明調査業務の対象範囲を、独立行政法人や一部の特殊法人等に拡大すること、その推進体制において、IPAをはじめとした専門機関の知見を活用することが明記された。
- IPAは、現在、民間企業等を中心として実施しているセキュリティ対策強化に向けた業務を、今後、強化していく予定。



４．ソフトウェア製品の危険性に関する情報の公表

- 現在は、IPAを窓口として、ソフトウェア製品の脆弱性については情報を収集し、開発者と調整の上、公表してユーザーへの注意喚起を行っているが、開発者との調整で同意が得られないケースや、脆弱性に当てはまらない危険性情報の取扱いは定められていない。
- ソフトウェア製品における脆弱性等の危険性情報に関し、公表手続等の取扱いを明確化することが必要。

○近年、ソフトウェア製品の危険性に起因する情報漏洩や不適切作動等のリスクが深刻化。
今後、IoTが進む中で、その社会的影響は更に増大。

例1：（2013年12月）バイドゥ（株）の日本語入力システムが、ユーザに無断で入力情報を外部に送信していることが判明。

例2：（2015年 7月）クライスラーの自動車に搭載されたシステムに脆弱性が発見され、ブレーキやエンジンのオン/オフが遠隔から操作できることが発覚。47万台超に影響が及んだ。

5．重要インフラのセキュリティ対策

● NISCが策定した第３次行動計画に基づく取組を推進。また、当省の取組として、標的型攻撃の情報共有、制御機器の認証、研究開発等、対策を複合的に推進。更なるJ-CSIPの体制強化が必要。

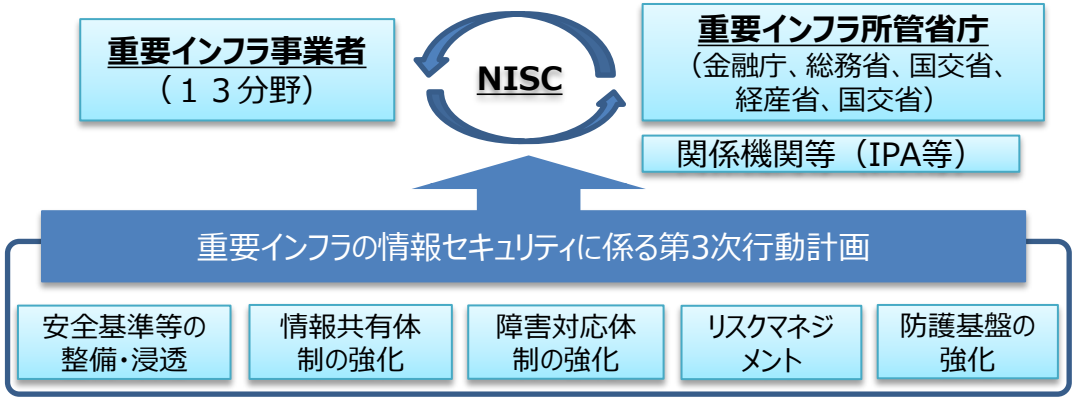
＜NISCが策定した第３次行動計画に基づく取組＞
電力・ガス・石油・化学・クレジット等１３の重要インフラ分野に関して、安全基準等の整備・浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化等を実施。

＜サイバー情報共有イニシアティブ（J-CSIP）＞
独立行政法人情報処理推進機構（IPA）が、重要インフラ分野等（電力、化学、ガス、石油、重工、資源開発の６業種（６１組織））における情報共有網を構築。各社と秘密保持契約を結び、情報収集、解析、共有等を実施。

＜制御システムセキュリティの対策の推進＞
技術研究組合制御システムセキュリティセンター（CSSC）が、昨年度より、インフラを制御する制御機器のセキュリティ認証を開始。

＜研究開発支援＞
戦略的イノベーション創造プログラム（SIP）のテーマの一つに、「重要インフラ等におけるサイバーセキュリティの確保」が選定され、今後研究開発を実施。

【第３次行動計画の枠組み】



【サイバー攻撃情報共有体制（J-CSIP）】

重要インフラ等企業（重工、電気、ガス、化学、石油、資源開発（今年２月に追加））

６．国際連携の取組

● 政府、民間機関等のあらゆるレベルでの国際連携を推進。

＜政府機関間の連携＞

北米：日米サイバー対話等による緊密な連携・対応
アジア大洋州：日ASEAN情報セキュリティ政策会議等による、協力関係の更なる深化・拡大
その他：欧州（英、仏、エストニア、EU）、アジア（日中韓）、豪、ロシアと政府間サイバー協議を実施。

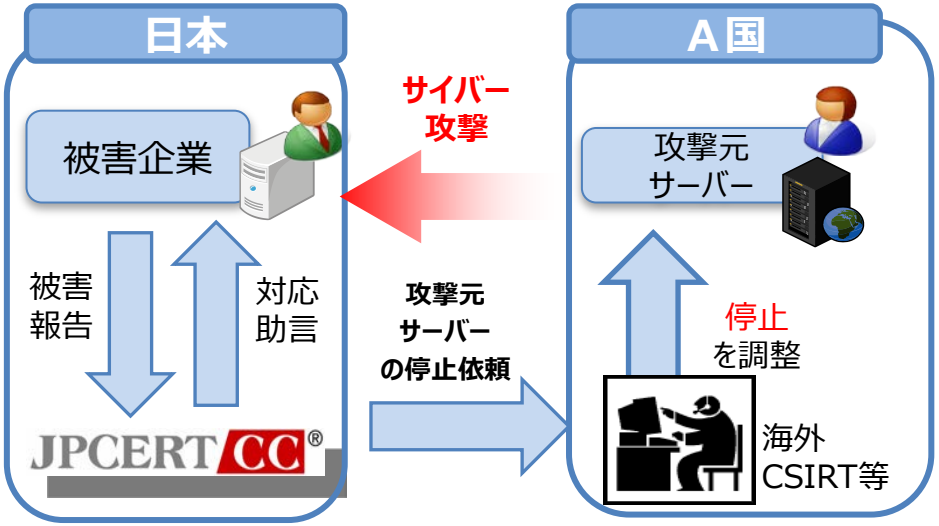
＜民間専門機関間の連携（一般社団法人JPCERTコーディネーションセンター（JPCERT/CC））＞

JPCERT／CCが日本の窓口CSIRT（※）となり、世界約１００カ国の窓口CSIRTと連携、サイバー攻撃に対して共同対処を実施。また、ASEANを中心に、現地指導やOJT等によるCSIRT構築も支援。
（※）Computer Security Incident Response Team

【日ASEAN情報セキュリティ政策会議】

(出典）NISC「サイバーセキュリティ戦略本部第４回会議資料

【国際連携によるサイバー攻撃対処】



７．情報セキュリティ人材の育成確保について（中間報告）

- 「実践的な能力を適時適切に評価できる試験制度の充実を図る」（「日本再興戦略」改訂2015）を踏まえ、良質な情報セキュリティ人材の供給のために、情報セキュリティスペシャリスト試験をベースとした登録制度の創設を目指す。
- 登録制度では、更新制度や登録簿公開等により、実践的な能力など質を担保するとともに、実務経験者や過去の試験合格者などへの門戸拡大により量も確保。
- 主としてユーザ企業を対象に、情報セキュリティマネジメント試験を新たに導入予定。

今後必要となる情報セキュリティ人材像と育成確保

- **ホワイトハッカーのような高度セキュリティ技術者**
  → 人材の発掘・育成に関する取組を継続・改善
- **ユーザ企業の事業部門や情報システム部門において、自社の情報セキュリティ技術者と連携して情報セキュリティの確保を管理する人材**
  → 情報セキュリティマネジメント試験
- **ユーザ企業やベンダ企業の情報システムを設計、開発、運用する担当者として必要な情報セキュリティに関する高度な知識・技能を身に付けた人材**
  → 情報セキュリティスペシャリストの登録制度

登録制度の概要

- **主な対象者**
  情報セキュリティスペシャリスト試験合格者
- **更新制度**
  - 目的：最新の専門的な知識・技能の習得や資質の維持・向上
  - 規模：２０２０年に３万人超
  - ３年ごとに更新
  - 登録者の活用に関する施策の実施
  - 主な要件：情報セキュリティスペシャリスト試験の一部再受験
    最新の知識や技能に関する講習の受講
- **登録簿公開**
  業務経歴による検索機能
- **登録者コミュニティ**
  - 最新のインシデント情報の提供
  - コミュニティ参加者同士の切磋琢磨