総務省における情報セキュリティに関する取組について

平成２５年６月

情報流通行政局 情報流通振興課
情報セキュリティ対策室
調査官　村上　聡

目　次

「情報セキュリティ」から「サイバーセキュリティ」へ

NISC 戦略

第1次情報セキュリティ基本計画
第2次情報セキュリティ基本計画
国民を守る情報セキュリティ戦略

→ サイバーセキュリティ戦略
（2013.06.10）

自由民主党 提言

情報セキュリティに関する提言
（2012.02.24）

→ 新たなICT戦略に関する提言
（2013.05.21）
第二部
サイバーセキュリティと経済成長
～サイバー空間の国家安全保障～

- 情報セキュリティ (information security) : 情報の「Confidentiality＝機密性」、「Integrity＝完全性」、「Availability＝可用性」を維持すること、とは、違ってきている？

- サイバー空間って何？　定義は？

- □ はじめに
- ☑ 情報セキュリティに関する脅威の変遷
- □ 政府全体における情報セキュリティ政策の動向
- □ 総務省における情報セキュリティ政策の概要
- □ パーソナルデータの利用・促進に向けて
- □ 終わりに

情報セキュリティに関する脅威の変遷

ICTは社会経済活動の基盤であると同時に我が国の成長力の鍵であるが、昨今、情報セキュリティ上の脅威の多様化・悪質化により、その被害が深刻化している。

危険度

経済犯・組織犯
金銭等の目的
計画的・悪質

愉快犯
自己顕示欲、見せしめ、嫌がらせ

メールによる感染

ネットワークによる感染

ウェブサイトによる感染

トロイの木馬

ワーム

ボット
（ロボットの略から命名）

ガンブラー

標的型
サイバー攻撃

高度化
複雑化

特定の組織や個人になりすましメールを送りつけるなどして、情報窃取などを行う。

感染したPCは、遠隔操作され迷惑メール、攻撃の踏み台などに悪用。

ウェブサイトの閲覧で感染し、データの窃盗などに悪用。

一昔前のウィルス

★目立つ→駆除しやすい

★目立たない→駆除しにくい
感染ユーザは「少し調子がおかしいかな？」程度で、特段の不具合を感じない。

2000年　2005年　2010年

情報セキュリティに関する事案

分散型サービス妨害(DDoS)攻撃

2009年7月・・・韓国、米国の金融機関や政府機関等のシステムが攻撃を受け、数日間に亘りウェブサイトへのアクセス不能な状態に陥ったことに加え、推定で27～41億円の経済的な被害が発生。

2010年9月・・・中国のハッカー組織が、日本政府機関のウェブサイトを攻撃すると表明した後、防衛省及び警察庁等のウェブサイトが攻撃を受け、3日間に亘りアクセスしづらい状態が継続。

2012年6月・・・国際ハッカー集団アノニマスが、ネット上の違法ダウンロード行為に刑事罰を導入する改正著作権法の成立に反発し、日本政府等に攻撃予告。**財務省、国交省**のウェブサイトが改ざんされたほか、最高裁、自民党、民主党のウェブサイトが一時アクセスしづらい状態が発生。

2012年9月・・・中国からのサイバー攻撃により、**最高裁判所、文化庁**等のウェブサイトが改ざん。

クラウドサービスの障害事例

2012年6月・・・ファーストサーバ(ヤフー子会社のレンタルサーバ事業者)が保有する共有サーバ・クラウドサーバにおいて、保守作業で使用した更新プログラムの不備により、約5000の企業・団体顧客のメールデータ等が消失

不正アクセス

2011年4月・・・**ソニーの子会社**(ソニー・コンピュータエンタテイメント及び米国法人)のシステムに対する不正アクセスにより、個人情報(氏名・住所、電子メールアドレス、クレジットカード番号等)約1億人分が窃取。

2012年9月・・・ウイルスに感染したPCが第三者により**遠隔操作**され、掲示板に違法な書込みが行われたことから、当該PCの所有者が誤認逮捕。

2012年10月・・ウイルス感染により、ネットバンキングにログインした利用者のPCの画面に偽画面が表示され、ID・パスワードが窃取。これにより、数百万円の不正送金が発生。

2013年4月・・・**NTTレゾナント**が運営するポータルサイト「goo」が不正アクセスを受け、約3万人のアカウントに不正ログインがあったとの報道。

2013年5月・・・**ヤフー**のポータルサイト「Yahoo!JAPAN」が不正アクセスを受け、最大約2200万人のユーザIDが流出した可能性があったとの報道。

標的型サイバー攻撃

2010年9月・・・イランの原子力発電所の制御システムにおいて、USB経由でスタックスネットと呼ばれるマルウェア感染が確認されたとの報道。(我が国のパソコンでも、スタックスネット感染パソコンが発見された旨の報道。)

2011年8月・・・**三菱重工業**の社内サーバやパソコン約80台が情報収集型のウイルスに感染し、コンピュータのシステム情報が流出したおそれ。

2011年10～11月・・・**衆参両院**のサーバやパソコンが情報収集型のウイルスに感染していたことが報道、ID・パスワードが流出したおそれ。

2011年11月・・**総務省**のパソコン23台が情報収集型のウイルスに感染していたことが判明、個人情報、業務上の情報が流出したおそれ。

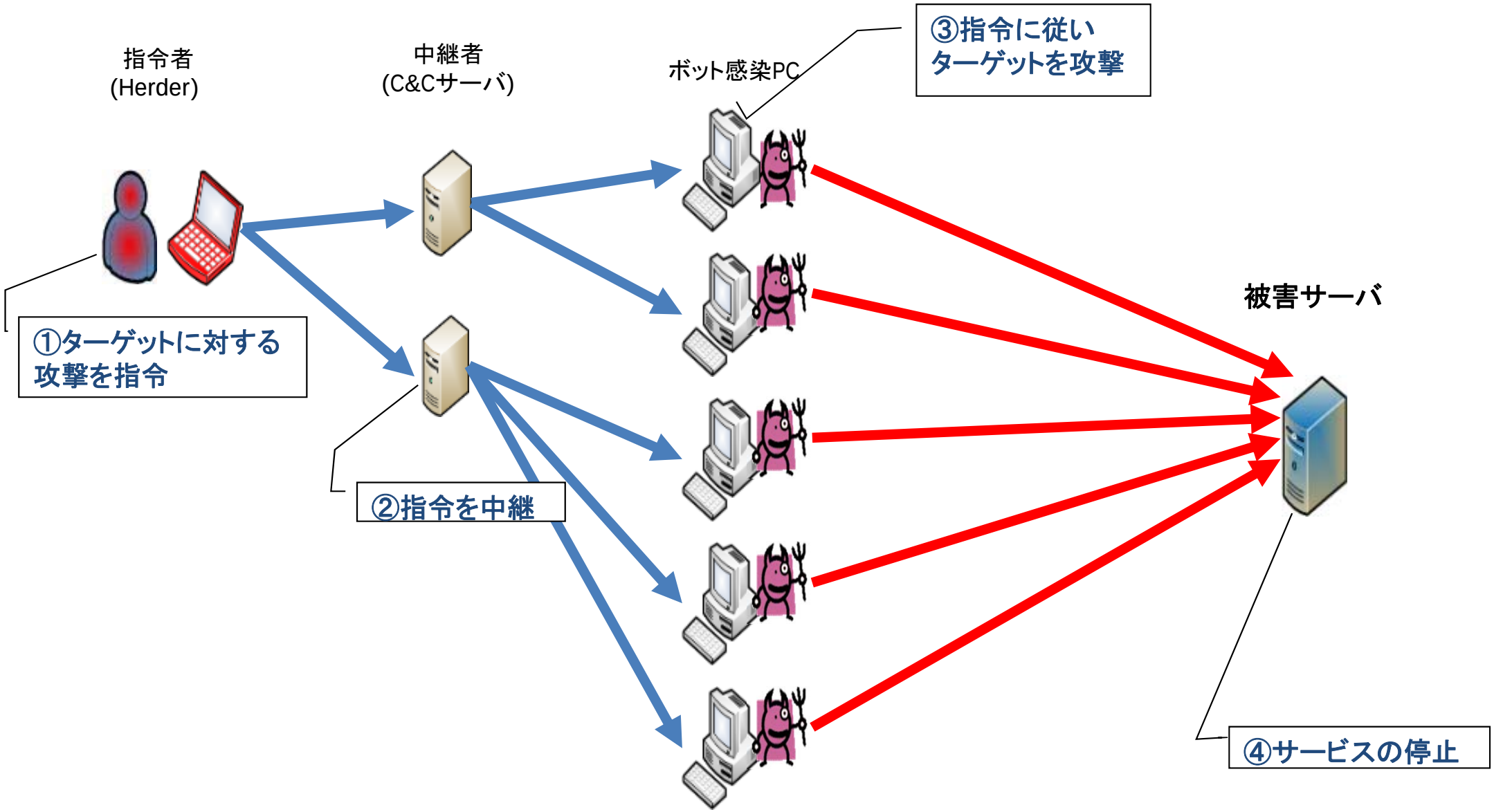
2013年1月・・・**農林水産省**のPCが遠隔操作型のウイルスに感染し、TPPに関する機密文書が窃取されたおそれがあることが報道。

2013年1月・・・**米紙ニューヨーク・タイムズ**及び**ウォール・ストリート・ジャーナル**より、同紙が中国のハッカーからサイバー攻撃を受け、記者らのパスワードが窃取されたとの報道。

2013年3月・・・**韓国**において、主要**放送局**や金融機関のコンピュータが一斉にダウンするというサイバー攻撃が発生。

DDoS攻撃

DDoS：Distributed Denial of Service（分散型サービス妨害攻撃）



出典：内閣官房情報セキュリティセンター

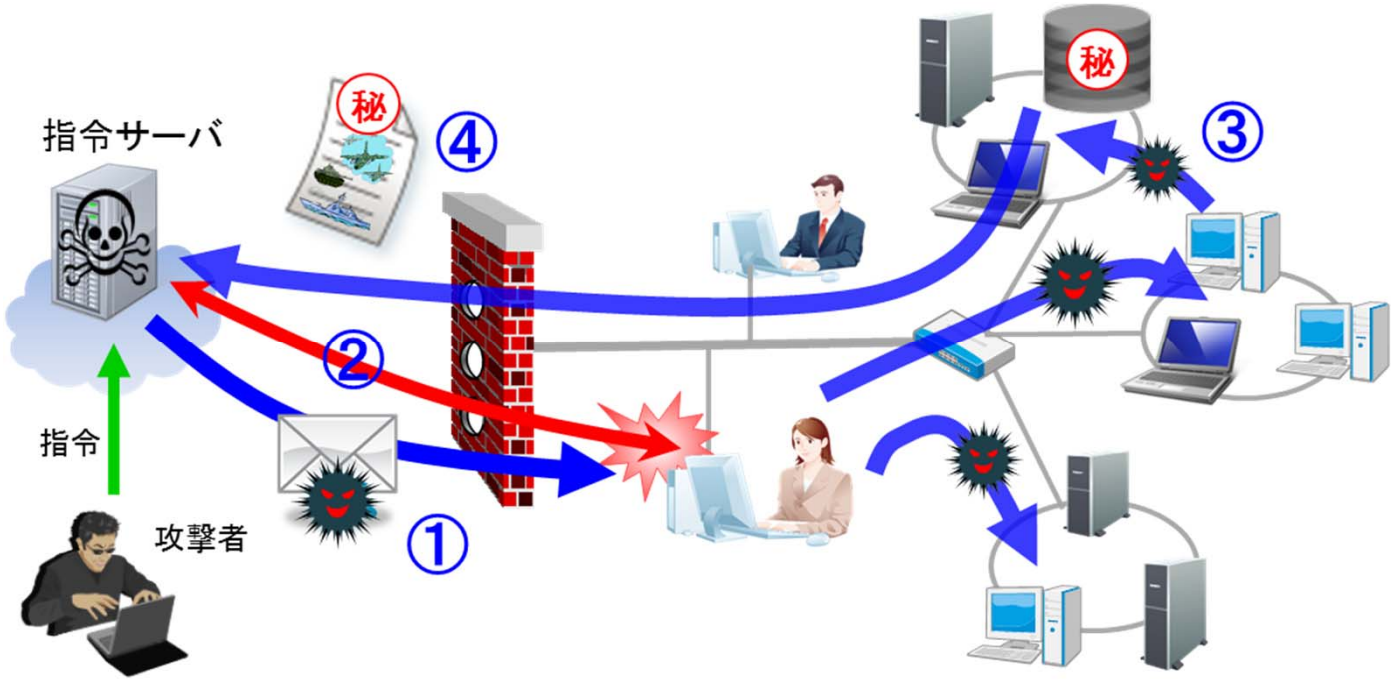
標的型攻撃

標的型攻撃とは、特定の組織や個人を標的に複数の攻撃手法を組み合わせ、執拗かつ継続的に行われる攻撃。攻撃が巧妙化・複合化しており、検出・防御が困難。

標的型攻撃の代表的な手順

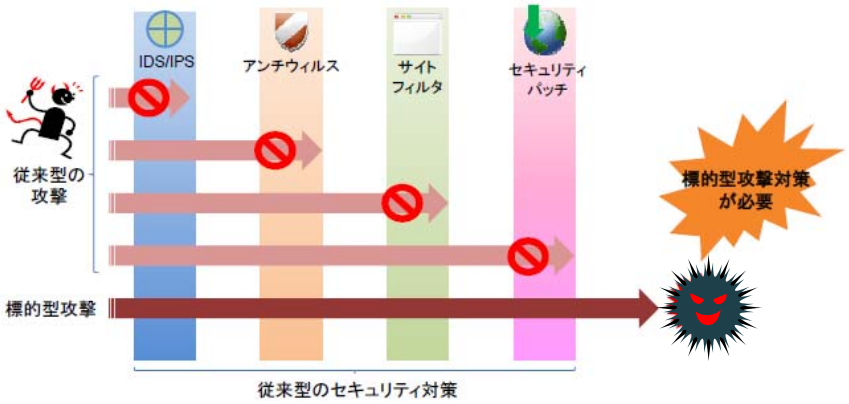
攻撃の標的となる組織について、事前にLAN環境に関する調査、SNSや社会的な手段により、攻撃の標的となる組織に関する調査を行った上で、次のような段階を踏んで攻撃を行う。

① 標的型メールにより、PCをマルウェアに感染させる。
② 当該PCと、指令サーバとを通信させる。
③ ネットワークを内偵しつつ、組織内でマルウェアの感染を拡大させる。
④ 最終目標への攻撃を遂行し、秘密情報等を手に入れる。



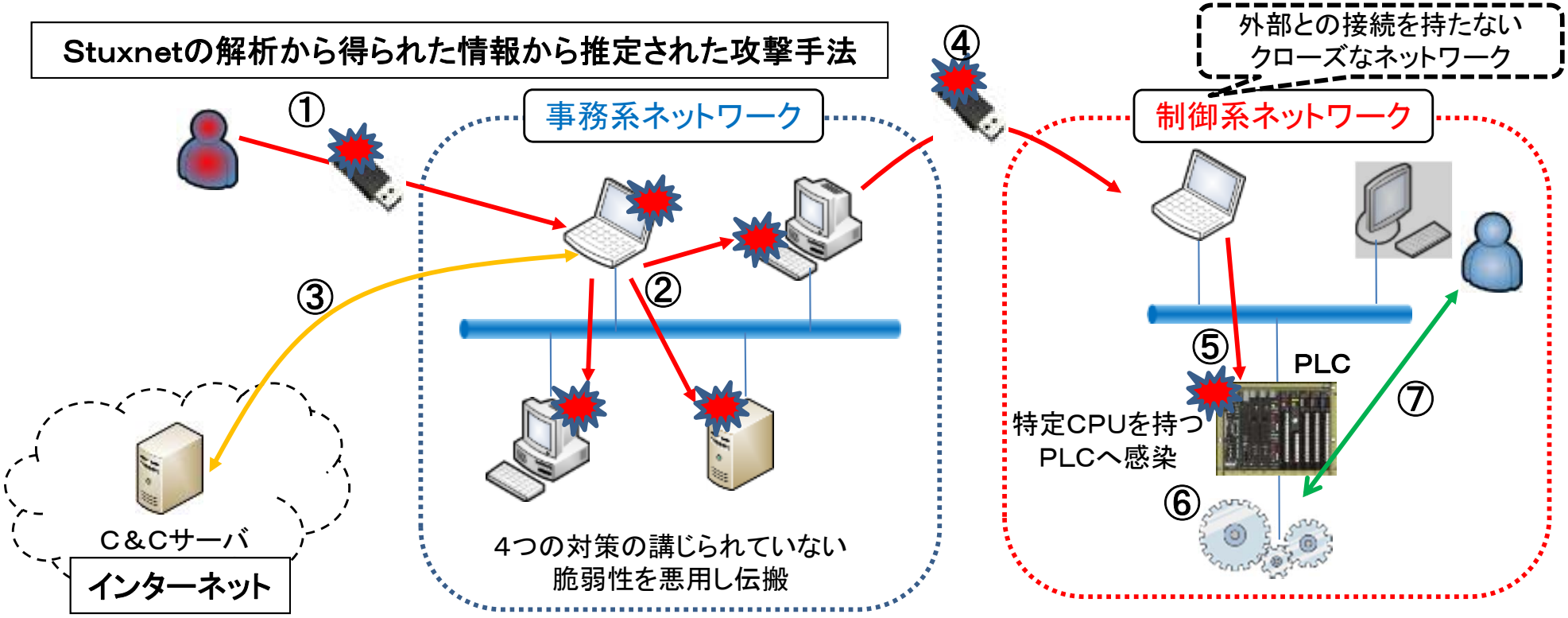
現状の課題

標的型攻撃は、未知のぜい弱性（ゼロデイ）を突くマルウェアを利用して攻撃が行われることもあるため、従来型の情報セキュリティ対策では検出・防御ができない。また、その被害や攻撃されていること自体に気づくのが事後、又は困難である場合もある。



制御系ネットワークへの攻撃

Stuxnet（スタックスネット）：2010年7月イランのブシェール原子力発電所及び同年11月ナタンツのウラン濃縮施設がサイバー攻撃によって被害を受けていたことが判明。



出典：内閣官房情報セキュリティセンター

- □ はじめに
- □ 情報セキュリティに関する脅威の変遷
- ☑ 政府全体における情報セキュリティ政策の動向
- □ 総務省における情報セキュリティ政策の概要
- □ パーソナルデータの利用・促進に向けて
- □ 終わりに

政府における情報セキュリティ政策の推進体制

内閣官房を中心に関係省庁も含めた横断的な体制を整備

高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）

本部長　内閣総理大臣
副本部長　情報通信技術（IT）政策担当大臣
内閣官房長官
総務大臣
経済産業大臣
本部員　本部長及び副本部長以外のすべての国務大臣
民間有識者（10人）

（事務局）

内閣官房IT総合戦略室

室長（政府CIO）

情報セキュリティ政策会議　（平成17年5月30日　IT戦略本部長決定により設置）

議長　内閣官房長官
議長代理　情報通信技術（ＩＴ）政策担当大臣
構成員　国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣

閣僚が参画

遠藤　信博	日本電気株式会社代表取役執行役員社長
小野寺　正	KDDI株式会社代表取締役会長
土屋　大洋	慶應義塾大学大学院教授
野原佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英	首都大学東京法科大学院教授
村井　純	慶應義塾大学教授

（事務局）

内閣官房情報セキュリティセンター　（NISC）

センター長（官房副長官補（安危））
副センター長（内閣審議官）2名
内閣参事官6名

情報セキュリティ緊急支援チーム（CYMAT）

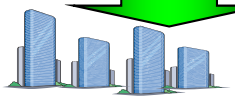
協力

その他の関係省庁

重要インフラ所管省庁
金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス）
国土交通省（鉄道、航空、物流）

その他
文部科学省（セキュリティ教育）　等

重要インフラ事業者　等



政府機関（各府省庁）

協力5省庁

- **警察庁**（サイバー犯罪の取締り）
- **総務省**（通信・ネットワーク政策）
- **外務省**（外交政策）
- **経済産業省**（情報政策）
- **防衛省**（国の安全保障）

企業

個人

サイバーセキュリティ戦略の策定について

○　情報通信技術の進展により、国民生活、社会経済、行政や安全保障・治安等のあらゆる活動がサイバー空間に依存。それに伴い、重要情報の窃取等のリスクや被害が増大するのみならず、サイバー攻撃等が国家基盤や社会基盤を揺るがすという脅威も大規模化・高度化・国際化。

○　こうした深刻化する国内外における環境変化等を踏まえ、「サイバーセキュリティ戦略」の早急な策定が必要。

「サイバーセキュリティ戦略」については、IT戦略本部におけるIT戦略の再構築に関する検討等と連携しつつ、　平成25年6月10日に、情報セキュリティ政策会議にて決定。

年度：2000 ／ 2004 ／ 2005 ／ 2006 ／ 2009 ／ 2010 ／ 2011 ／ 2012 ／ 2013 ／ 2014

- 各省における試行錯誤
- サイバー攻撃への対応を中心とした対策実施時期
- IT障害への対応も含めた総合的な対策基盤づくりの推進
- サイバー攻撃事態発生を念頭、新たな環境変化対応、能動的情報セキュリティ対策
  「事故前提社会」への対応力強化など成熟した情報セキュリティ先進国へ向けた取組

IT戦略

- e-Japan戦略（2001.1）
- e-Japan戦略Ⅱ（2003.7）
- IT新改革戦略（2006.1）
- i-Japan戦略2015（2009.7）
- 新たな情報通信技術戦略（2010.5）
- 世界最先端IT国家創造宣言

情報セキュリティ戦略

- サイバーセキュリティ戦略（2013年6月10日に策定）

中長期計画

- 国民を守る情報セキュリティ戦略（2010.5　2013年度までが対象）
- 第１次情報セキュリティ基本計画 ～「セキュア・ジャパン」の実現に向けて～（2006.2）
- 第２次情報セキュリティ基本計画 ～IT時代の力強い「個」と「社会」の確立に向けて～（2009.2）

【現行目標】
2020年までに、情報通信技術を安心して利用できる環境（高品質、高信頼性、安全・安心を兼ね備えた環境）を整備し、世界最先端の「情報セキュリティ先進国」の実現

年度計画：2006 ／ 2007 ／ 2008 ／ 2009 ／ 2010 ／ 2011 ／ 2012 ／ 2013 ／ ・・・・・

我が国の経済発展及び国家安全保障、国民の安全・安心を確保するため、サイバー空間の持続性・発展性（「サイバーセキュリティ」）が確保された、「サイバーセキュリティ立国」の実現へ　＜情報セキュリティ政策会議資料より作成＞

サイバーセキュリティ戦略①

1. 環境の変化

サイバー空間と実空間の「融合・一体化」
► 情報通信技術の普及・高度化・利活用の進展

サイバー空間を取り巻く「リスクの深刻化」
► リスクの甚大化・拡散・グローバル化

2. 基本的な方針

(1) 目指すべき社会像：「サイバーセキュリティ立国」の実現

**国家の安全保障・危機管理、社会経済の発展、国民の安全・安心確保のため、
「世界を率先する」「強靭で」「活力ある」サイバー空間を構築し、
サイバー攻撃等に強く、イノベーションに満ちた、世界に誇れる社会を実現**

(2) 基本的な考え方

① 情報の自由な流通の確保
► 表現の自由やプライバシーの保護等が確保され、経済成長等を享受

② 深刻化するリスクへの新たな対応
► リスクの変化に迅速・的確に対応できる多層的な取組が必要

③ リスクベースによる対応の強化
► 動的対応力を通じ、リスクの性質を踏まえた対応の強化が必要

④ 社会的責務を踏まえた行動と共助
► 多種多様な主体が各々の役割を発揮し、相互連携・共助が必要

(3) 各主体の役割

① 国
► サイバー空間の外交・防衛・犯罪対策、政府機関等における対策強化・対処態勢整備 等

② 重要インフラ事業者等
► 現行10分野の取組強化、新たな分野における必要な対策の実施 等
（10分野：情報通信、金融、航空、鉄道、電力、ｶﾞｽ、政府・行政ｻｰﾋﾞｽ（地方公共団体を含む）、医療、水道、物流）

③ 企業や教育・研究機関
► 情報共有等の集団的対策、産学連携による高度技術・人材の供給 等

④ 一般利用者や中小企業
►「他者に迷惑かけない」認識醸成やリテラシー向上など自律的取組、情報共有 等

⑤ サイバー空間関連事業者
► 製品等の脆弱性への対応、インシデント認知・解析、国際競争力の強化 等

サイバーセキュリティ戦略②

3. 取組分野

2015年度までの3年間、以下に掲げる取組を実施。

(1)「強靭な」サイバー空間の構築

※GSOC: Government Security Operation Coordination team
CSIRT: Computer Security Incident Response Team
CYMAT: Cyber Incident Mobile Assistant Team

① 政府機関等における対策：情報システム等に関する対策及びサイバー攻撃への対処態勢を一層強化

- 政府共通プラットフォームによる情報システムのクラウド化、技術標準化等を通じ、攻撃等に強いシステム基盤構築。
- 国家機密等に関する情報及び情報システムの重要度等に応じてセキュリティ対策を重点化。

例
- 国の安全に関する重要な情報の国以外の事業者による取扱い、独立行政法人等におけるセキュリティ強化。
- GSOCを抜本的に強化し、監視対象を拡大するとともに、インシデント情報を効果的に収集・活用。
- CYMAT、CSIRT等の間の連携強化により、政府内におけるインシデント情報共有・即応体制を一層強化。
- 大規模サイバー攻撃事態等を想定した対処訓練を毎年度実施するなど対処態勢を強化。

② 重要インフラ事業者等における対策：政府機関等における対策に準じた取組

- 重要インフラ事業者等とサイバー空間関連事業者との間の、攻撃情報等の情報共有を促進。

例
- GSOCが保有するインシデント情報等を重要インフラ事業者等と共有するための仕組みを整備。
- 重要インフラの範囲及び対応の在り方等を検討し、対策をとりまとめた新たな「行動計画」を策定。

③ 企業・研究機関等における対策：インシデントの認知・情報共有の強化、CSIRT構築促進や演習等

- セキュリティ投資促進のためのインセンティブ検討等により、中小企業等におけるサイバー攻撃認知機能等を強化。

例
- 演習用テストベッドを利用した実践的な防御演習等により、企業等におけるサイバー攻撃への対応能力を向上。
- 企業・研究機関等のCSIRT構築促進・連携強化を図り、インシデント発生時の対応能力を向上。

④ サイバー空間の衛生：個々の主体による対策に加え、社会全体が参加した予防的対策実施

- 「サイバー・クリーン・デー」（仮称）の新設などサイバー空間の衛生確保を国民運動化。

例
- 悪性サイトにアクセスしようとする一般利用者に対するISP等による注意喚起等を行うための仕組みを構築。
- セキュリティ目的の通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方を検討。

⑤ サイバー空間の犯罪対策： 対処能力強化や民間事業者等の知見の活用等による対処態勢強化

- 日本版NCFTAの創設、アンチウイルスベンダーとの情報共有枠組みの構築等の取組を強化。

例
- サイバー犯罪に対する事後追跡可能性を確保するため、関係事業者における通信履歴等に関するログの保存の在り方やデジタルフォレンジックに関する取組を促進するための方策について検討。

※NCFTA: National Cyber-Forensics and Training Alliance

サイバーセキュリティ戦略③

(1)「強靱な」サイバー空間の構築 ［続き］

⑥ サイバー空間の防衛：国家レベルのサイバー攻撃から我が国に係るサイバー空間を守るための対応強化

例
- 重要インフラ等の情報システムに対する攻撃における自衛隊など非常時における関係機関の役割を整理し、必要な体制・機密情報等の共有システムや制度の整備等を行うとともに、個別具体的な国際法の適用も併せて整理。
- 武力攻撃の一環としてサイバー攻撃が行われた場合に対処する任務を負う自衛隊等の能力・態勢等を強化。

(2)「活力ある」サイバー空間の構築

① 産業活性化：海外製品等への依存度が高い我が国のサイバーセキュリティ産業の国際競争力強化

例
- 国際標準化や評価・認証の国際的な相互承認枠組み作りに積極的に関与するとともに、
- 産業制御システムの評価・認証機関を設立
- 新たな技術が採用された製品等の政府による積極的な調達。

② 研究開発：リスクの変化に適切に対応できる、創意と工夫に満ちたセキュリティ技術の創出

例
- サイバー攻撃の検知や高度解析等の向上に向けた技術の研究開発等を加速させ、最先端の研究開発を保持・向上。
- 潜在型マルウェア等多様・高度化するサイバー攻撃に対し、有効な革新的技術を確立するため、先端技術を開発。

③ 人材育成：高度かつ国際的なセキュリティ人材の育成

例
- ソフトウェア関連分野における優れた個人を発掘等するための合宿研修や実践的技能を競うコンテスト等を官民で連携実施。
- グローバルに活躍できる人材の育成等のため、国際会議への参加や海外の専門大学院等への留学を支援。

④ リテラシー向上：一般国民のリテラシーの向上

例
- 初等中等教育において、情報セキュリティを含む情報モラルやソフトウェアのプログラミングに関する教育、デジタル教科書の活用など実践的な取組を推進。高齢者に対するセキュリティ啓発のためのサポーター等を育成・活用。
- スマートフォンのアプリについて、一般利用者がリスクを認知し、利用等の判断を行う自ら行える仕組みを構築。

サイバーセキュリティ戦略④

(3)「世界を率先する」サイバー空間の構築

① 外交：基本的な価値観を共有する国等とのパートナーシップ関係の多角的構築・強化

例
- サイバー空間を利用した行為に対する国連憲章や国際人道法等の個別具体的な国際法の適用について引き続き検討。
- 米国等との間で、サイバー領域での具体的対処の在り方、国際的なルール作りといった分野における議論を深化。

② 国際展開：ASEAN等とともに成長できる関係を構築し、サイバー攻撃への対応能力構築の支援

例
- 諸外国と連携してサイバー攻撃に関する情報収集ネットワークを構築し、攻撃の発生予知、即応等に関する研究開発を実施。
- 官民連携によるボットウイルス対策など国内における成功事例の紹介や共同プロジェクト、机上演習等を実施。

③ 国際連携：国境を越えるサイバー攻撃に関するインシデントへの対応・連携の強化

例
- 外国捜査機関等とのサイバー犯罪に係る情報交換を継続的に行うとともに、連携強化等のため、職員を派遣。
- 相互不信による不測事態回避のため、我が国の基本的な立場等を共有するとともに、インシデント発生した場合の相互の連絡体制等を平時から構築し、国際共同研究や複数国間におけるサイバー攻撃対応演習等を実施。

4. 推進体制等

- NISCについて権限等の必要な組織体制を整備し、2015年度を目途として「サイバーセキュリティセンター」（仮称）に改組・機能強化
- 政府機関や重要インフラ事業者等におけるサイバー攻撃関連情報の共有促進のための枠組み整備
- 取組を進めるにあたっての具体的な中長期（2015年度・2020年）の目標の管理

例
- 2015年度までに、政府機関等におけるサイバー攻撃関連情報の共有体制のカバー率向上、マルウェア感染率や国民の不安感の改善、国際インシデント調整の対応連携が可能な国等の３割増
- 2020年までに、国内の情報セキュリティ市場規模の倍増、セキュリティ人材の不足割合の半減

- 2015年度までの3年間を戦略の対象とし、年次計画の策定・評価等を実施
- サイバーセキュリティに関する国際戦略を策定

日・ASEANサイバーセキュリティ協力に関する閣僚政策会議

○　2013年の日・ASEAN友好協力40周年記念事業として、サイバーセキュリティ分野での日・ASEAN間の協力の推進を閣僚級で合意するため、閣僚級の会合を開催。

1．日程・場所

2013年9月12～13日　東京（ホテルオークラ）

2．議題案

① 日・ASEAN情報セキュリティ政策会議（局長級）の成果の確認と今後のセキュリティ向上に向けた共通認識

② 安心・安全なネットワーク環境構築に向けた課題と協力

③ ビジネスのための安心・安全なサイバー空間構築に向けた課題と協力

④ 政府及び国民の情報セキュリティ水準の向上に向けた課題と協力

⇒閣僚宣言

政府の情報セキュリティ予算について

＜第34回情報セキュリティ政策会議資料より作成＞

平成25年度政府予算額

241．9億円（平成24年度当初予算：186．3億円）

（※）情報セキュリティに関する予算として切り分けられない場合には計上していない。

主な施策例及び平成25年度政府予算額（括弧内は平成24年度当初予算額）

- ○サイバーテロ対策用資機材の増強等（警察庁） 5．8億円（1.3億円）
- ○重要無線通信妨害対策の強化（総務省） 46．8億円（56.6億円）
- ○ICT環境の変化に応じた情報セキュリティ対応方策の推進事業（総務省） 10．3億円（新規）
- ○情報セキュリティ対策推進事業（経済産業省） 16．0億円（22.7億円）
- ○東北復興再生に資する重要インフラIT安全性検証・普及啓発拠点整備・促進事業（経済産業省） 5．4億円（新規）
- ○ネットワーク監視態勢の強化（防衛省） 69．3億円（新規）
- ○サイバー演習環境構築技術に関する研究（防衛省） 15．8億円（新規）

平成24年度政府補正予算額

183．2億円

（※）情報セキュリティに関する予算として切り分けられない場合には計上していない。

主な施策例及び平成24年度補正予算額（括弧内は平成24年度当初予算額）

- ○政府機関・情報セキュリティ横断監視・即応調整チーム（GSOC）の運用（内閣官房） 13．9億円（6.5億円）
- ○デジタルフォレンジック用資機材の増強等（警察庁） 6．4億円（0.3億円）
- ○情報セキュリティ技術の研究開発・実証実験施設の整備（総務省） 100．0億円（新規）
- ○サイバー攻撃解析・防御モデル実践演習（総務省） 15．2億円（新規）
- ○サイバー攻撃の被害拡大に対する緊急対策事業（経済産業省） 7．5億円（新規）

- □ はじめに
- □ 情報セキュリティに関する脅威の変遷
- □ 政府全体における情報セキュリティ政策の動向
- ☑ 総務省における情報セキュリティ政策の概要
- □ パーソナルデータの利用・促進に向けて
- □ 終わりに

総務省の情報セキュリティ政策の概要

1. 安心なネットワーク環境の整備

①事業者との情報共有

・テレコム・アイザック推進会議等の所管事業者や(独)情報通信研究機構と情報共有し、被害の拡大防止等に寄与。

②サイバー攻撃対処に向けた官民連携の強化

・経済産業省及び関連4団体と、各機関が保有する情報を高度解析し、サイバー攻撃の実態等を把握(サイバー攻撃解析協議会)。

③ＩＣＴ環境の変化に応じた情報セキュリティ対応方策の推進事業（平成25～29年度）

・国民のウイルス感染被害予防に資する研究開発・実証実験等を実施。

2. 技術開発の推進

①サイバー攻撃解析・防御モデル実践演習（平成24～29年度）

・サイバー攻撃への防御モデルの検討を行うとともに、官民参加型の実践的な防御演習を実施。

②国際連携によるサイバー攻撃予知・即応技術の研究開発（平成23～27年度）

・諸外国と連携してサイバー攻撃の発生を予知し即応を可能とする技術の研究開発を実施。

3. 利用者意識の向上

・「国民のための情報セキュリティサイト」による情報提供、セミナー開催による周知啓発活動。

・スマートフォン、無線LAN等の情報セキュリティに関する様々なメディアを活用した周知啓発活動。

4. 国際連携の推進

・米国、ASEAN等の海外諸国と情報セキュリティ対策に関する取組を共有し、国際的な連携を推進。

5. パーソナルデータの利用・流通の促進

・プライバシー保護等に配慮したパーソナルデータ(個人に関する情報)のネットワーク上での利用・流通の促進に向けた方策について検討するため、「パーソナルデータの利用・流通に関する研究会」を開催。

情報セキュリティ アドバイザリーボード

情報通信分野における官民において、時々刻々と変化する情報セキュリティ上の課題に対して効果的な対策や、日本の経済成長に繋がるような有効な施策が講じられるよう、**有識者から助言を得ることを目的として設置**する。

「情報セキュリティ アドバイザリーボード」の任務

（１）**情報セキュリティ対策の在り方への助言**

情報セキュリティの推進にあたり、日本の経済成長への貢献も視野に入れつつ、情報通信分野に携わる関係者において短期的及び中長期的に講ずべき対策や既存の取組の改善などの方向性について、幅広い観点から助言を行う。

（例）・ 官民連携や国際連携の在り方
・ 情報セキュリティに係る研究開発の方向性
・ DDoS攻撃や情報窃取など情報セキュリティに係るインシデント等への即応の在り方

（２）**その他**

情報セキュリティに係る諸問題への対応について、必要に応じて、提言をとりまとめる。

情報セキュリティ アドバイザリーボード

【構成員】（敬称略）

（座長）	山口　英	奈良先端科学技術大学院大学　教授
（座長代理）	林　紘一郎	情報セキュリティ大学院大学　前学長・教授
	飯塚　久夫	一般財団法人日本データ通信協会　テレコム・アイザック推進会議　会長
	岡村　久道	国立情報学研究所客員教授・弁護士
	藤沢　久美	シンクタンク・ソフィアバンク　副代表
（顧問）	小野寺　正	KDDI株式会社　代表取締役会長

※政府の「情報セキュリティ政策会議」のメンバー

ワーキンググループ　【構成員】技術系や法律系などの有識者、電気通信事業者等

スケジュール　平成25年３月から随時開催。

「総務省における情報セキュリティ政策の推進に関する提言」の概要

Ⅰ. 情報の自由な流通の確保

人間の尊厳、自由、民主主義等の核心的な価値を推進するサイバー空間の構築による経済成長の促進。

Ⅱ. 過度な規制によらない信頼できるサイバー空間の構築

イノベーションや経済成長を起こすサイバー空間の堅持。

Ⅲ. 動的防御プロセス連携の確立

高度化・複雑化するサイバー攻撃に対応するためには、PDCAという一連のサイクルが終わる前に、常に、動的に、適時適切な意思決定を行うプロセスの構築が必要。

動的防御プロセス連携

それぞれのプロセスにおいて得られた知見を常時他のプロセスに反映

①モニタリング（検知・解析）（Observe）
◇継続的なモニタリングによるサイバー攻撃の検知
◇サイバー攻撃の目的・意図を判別するための情報収集

②情勢判断（Orient）
◇攻撃の目的・意図を識別した上で、自組織に対する影響を把握

③意思決定（Decide）
◇サイバー攻撃に対する措置に関する迅速かつ的確な意思決定

④行動（Act）
◇問題解決やリスク要因の排除の実施

総務省の取組

官民連携	悪性サイトの検知機能の強化	サイバー攻撃解析協議会による観測データ等の蓄積
国際連携	PRACTICE※1による諸外国とのサイバー攻撃情報の共有	
技術開発・人材育成	NICT「サイバー攻撃対策総合研究センター（CYREC※2）」による解析能力の向上	サイバー攻撃の防御モデルの確立・実践演習の実施※3

政府自身の防御体制の構築

- 政府情報システムの情報セキュリティ対策の強化。
- 職員訓練の充実。

※1 諸外国と連携してサイバー攻撃に関する情報を収集するネットワークを国際的に構築し、サイバー攻撃の発生を予知し即応を可能とする技術の研究開発及び実証実験プロジェクト。

※2 Cybersecurity Research Center

※3 演習用テストベッドを利用した官民のLAN管理者等を対象に実践的な防御演習を実施。対象やその手法の提供等は、官庁・大企業にとどまらず、地方公共団体や中小企業に拡大。

Ⅳ. リスク認識に基づく対応の強化（事故前提社会）

自律的な対応を促す仕組みづくりの構築。

個人

- 通信事業者によるマルウェアの感染や悪性サイトへのアクセスに対する注意喚起等の実施。
- スマホのアプリについて、個人がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みの構築。

中小企業

- 情報セキュリティ投資促進税制等のインセンティブの検討。
- システムの共同利用など全体として低コストの情報セキュリティ対策の実現に向けた対策の推進。

Ⅴ. 国際連携によるサイバー空間政策の推進

我が国の経済成長を見据えた戦略的な国際連携の推進。

グローバルなインターネット環境の安全の確保

- 共同プロジェクト推進等のASEAN諸国等との連携による情報セキュリティ環境の向上。

日本企業のグローバル展開への貢献

- 情報セキュリティの名の下で行われる過度な規制の撤廃に向けて省庁の枠を超えて連携。

国際的なサイバー空間の規範形成への主導的な取組

- 顔が見える外交を展開し、先導的に国際的なサイバー空間の規範形成をリード。

総務省の主な情報セキュリティ関連予算

課題

標的型攻撃

昨今、標的型攻撃等の巧妙化するサイバー攻撃により、我が国政府機関、民間企業等において機密情報漏えい等の被害が発生する事態が頻発。

個人のマルウェア感染

個人利用者においても、ウイルス感染の拡大や、オンラインバンキングにおけるID・パスワードの漏えいなどの実被害が発生。

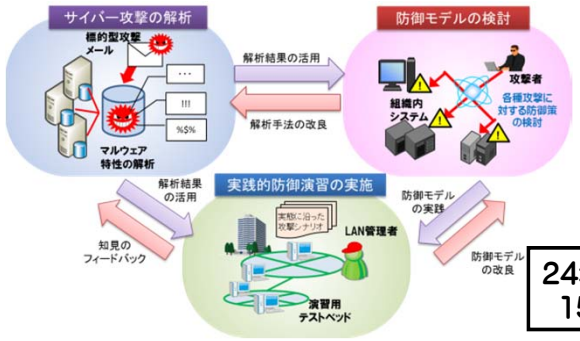
分散型サービス妨害攻撃（DDoS攻撃）

海外を主な発信源とするDDoS攻撃等により、政府機関等のウェブサイトのアクセス障害や改ざん等が頻発。

実証実験

サイバー攻撃解析・防御モデル実践演習

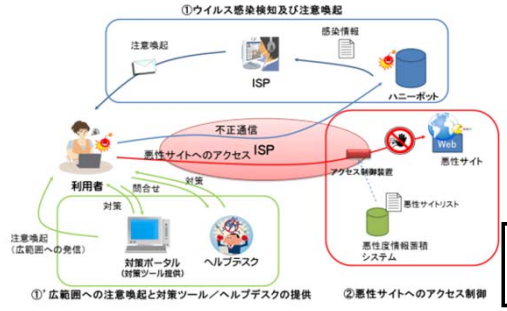
標的型攻撃の解析による実態把握、防御モデルの検討、官民参加型の実践的な防御演習による人材育成を実施。



24年度補正
15.2億円

国民のウイルス感染被害予防に関する実証実験

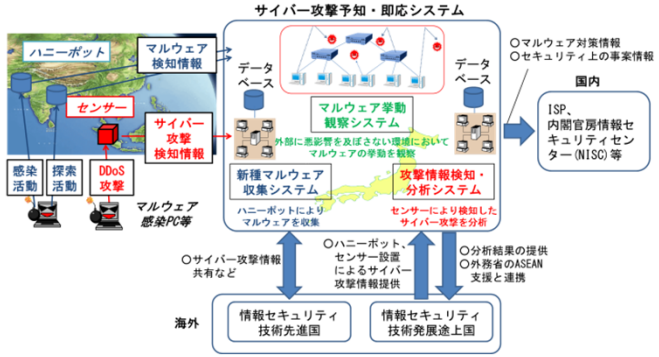
①PCがウイルス感染した個人利用者にISP等を通じて注意喚起。
②個人利用者がウイルス感染元等の悪性ウェブサイトにアクセスしようとした際に注意喚起。



25年度
4.8億円

国際連携によるサイバー攻撃予知・即応技術の研究開発

諸外国と連携してサイバー攻撃に関する情報を収集するネットワークを構築し、サイバー攻撃の発生を予知し即応を可能とする技術の研究開発及び実証実験を実施。



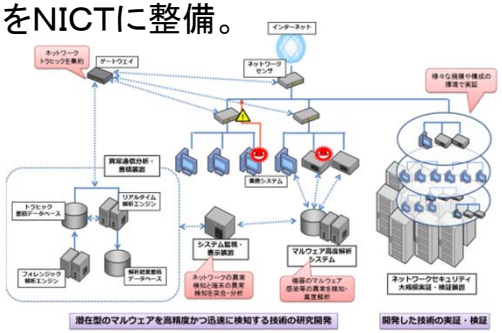
◇ 平成24年３月に、サイバー攻撃の予知のための研究開発の協力について、**米国と合意**。
◇ そのほか、平成24年３月**インドネシア**、平成24年４月に**モルディブ**、平成25年２月に**タイ**、３月に**マレーシア**との間で連携について合意。
◇ 現在、欧州諸国、シンガポール等と連携に向けて協議中。

23年度　6.3 億円
23年度補正　5.6 億円
25年度　5.8 億円

研究開発

NICT施設整備補助金

潜在型マルウェアの検知技術等、革新的な情報セキュリティ技術の研究開発・実証実験施設をNICTに整備。



24年度補正
100億円

サイバー攻撃の解析・検知に関する研究開発

①サイバー攻撃の存在に気づいた後、攻撃の侵入経路や進行状況を過去に遡って解析する技術の研究開発。
②サイバー攻撃が仕掛けられていることを早期に検出する不正検知技術の研究開発。
③これらの解析・検知を行うために有効なログの取得・縮退方法の研究開発。

25年度
5.5億円

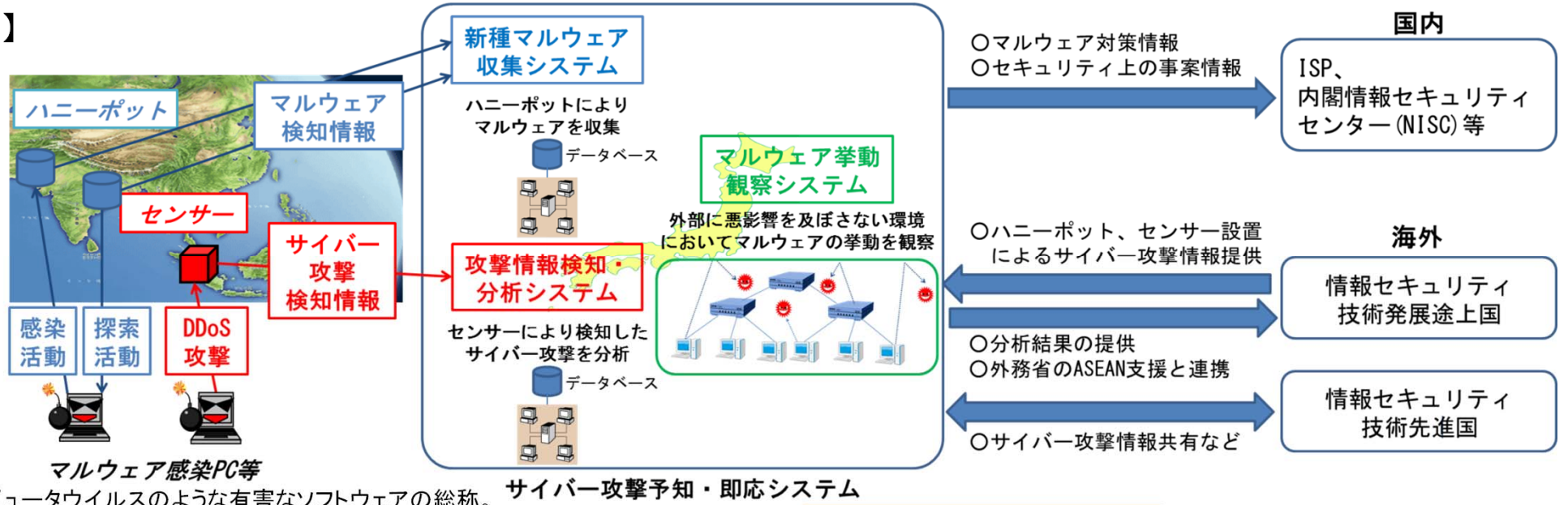
国際連携によるサイバー攻撃予知・即応技術の研究開発

プロジェクト略称：PRACTICE： **P**roactive **R**esponse **A**gainst **C**yber-attacks **T**hrough **I**nternational **C**ollaborative **E**xchange

○目的：
近年、被害が拡大しているサイバー攻撃（分散型サービス妨害攻撃、マルウェアの感染活動等）に対処し、我が国におけるサイバー攻撃のリスクを軽減。

○概要：
国内外のインターネットサービスプロバイダ（ISP）、大学等との協力によりサイバー攻撃、マルウェア等に関する情報を収集するネットワークを国際的に構築し、諸外国と連携してサイバー攻撃の発生を予知し即応を可能とする技術について、その研究開発及び実証実験を実施。

【イメージ図】



○マルウェア：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。
○DDoS（Distributed Denial of Service）攻撃：分散型サービス妨害攻撃。多数のPCから一斉に大量のデータを特定宛先に送りつけることにより、当該宛先のネットワークやサーバを動作不能にする攻撃。
○ハニーポット：故意に外部からの進入を容易にした囮のネットワーク機器。マルウェアの感染活動等の検知を目的にネットワーク上に設置。

○ 実施期間：平成23～27年度
○ 予 算 額：平成23年度当初予算 6.3 億円
平成23年度補正予算（第４号） 5.6 億円
平成25年度当初予算 5.8 億円

国際連携の状況

○ 平成23年11月、「第4回日・ASEAN情報セキュリティ政策会議」において、ASEAN各国に連携を呼びかけ。
○ 平成24年3月には、サイバー攻撃の予知のための研究開発の協力について、**米国と合意**。6月に研究者中心の日米会合を実施。
○ そのほか、平成24年3月に**インドネシア**、4月に**モルディブ**、平成25年2月に**タイ**、3月に**マレーシア**との間で合意。
○ 現在、シンガポール等と連携に向けて協議中。

ICT環境の変化に応じた情報セキュリティ対応方策の推進事業①

（国民のウイルス感染被害予防方策）

施策概要

○ 昨今、国会、政府機関、民間企業等がネットワークを通じたサイバー攻撃を受け、情報漏えい等の被害が発生する事態が頻発している。ICT環境が変化する中、サイバー攻撃が標的型攻撃※をはじめ巧妙化・複合化するなど、我が国における情報セキュリティ対策基盤の強化が喫緊の課題となっている。

※ 標的型攻撃：特定の組織や個人を標的に複数の攻撃手法を組み合わせ、執拗かつ継続的に行われる攻撃

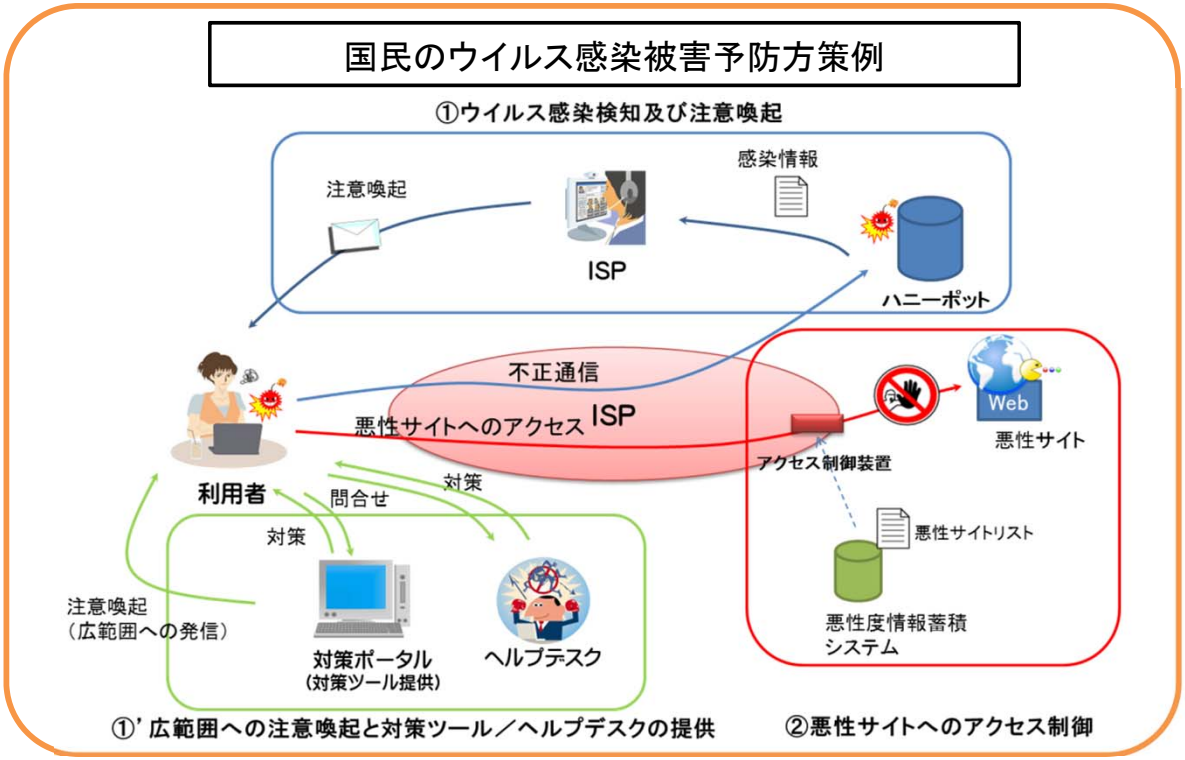
○ 個人利用者においても、ウイルス感染やID・パスワードの漏えいなどの実被害が発生していることから、インターネット利用に関する安全の確保を図るため、攻撃の解析・検知の高度化、ウイルス感染被害予防に資する研究開発・実証実験等を民間企業等への委託により実施する。

【国民のウイルス感染被害予防方策例】

①ウイルス感染した個人利用者のPCによる不正通信を自動的に検知。利用者にインターネットサービスプロバイダ（ISP）等を通じて注意喚起情報を送付し、駆除等の対策を促す。

②ウイルス感染元等、ウェブサイトの悪性度の情報を蓄積したシステムを構築し、個人利用者がアクセスしようとした場合に、当該システムにより検知し、注意喚起等を行う。

○ 実施期間：平成25～29年度
○ 所 要 額：平成25年度当初予算 10億円



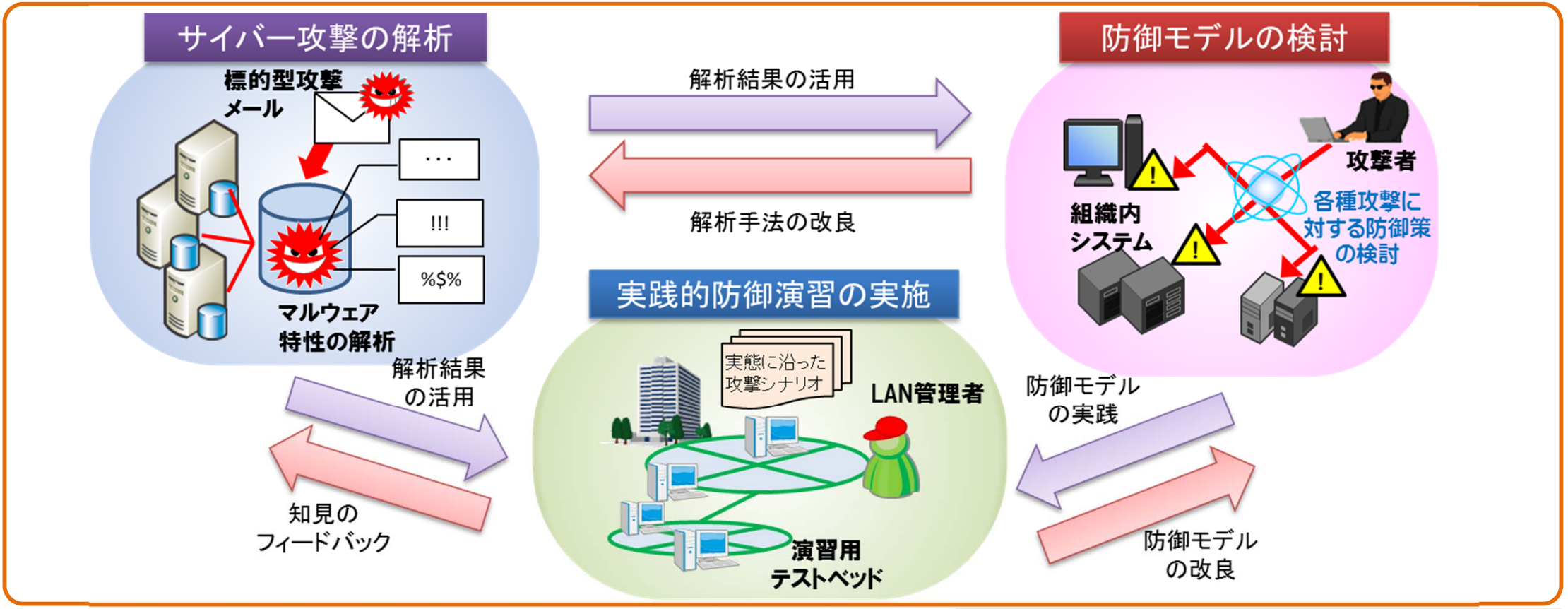
ICT環境の変化に応じた情報セキュリティ対応方策の推進事業②

（サイバー攻撃解析・防御モデル実践演習）

昨今、国会、政府機関、民間企業等がネットワークを通じたサイバー攻撃を受け、情報漏えい等の被害が発生する事態が頻発している。サイバー攻撃が標的型攻撃※をはじめ巧妙化・複合化するなど、ICT環境が変化する中、我が国における情報セキュリティ対策基盤の強化が喫緊の課題となっている。

新たなサイバー攻撃に対応可能な環境を実現するため、攻撃の解析及び防御モデルの検討を行い、官民参加型のサイバー攻撃に対する実践的な防御演習を実施する。

標的型攻撃：特定の組織や個人を標的に複数の攻撃手法を組み合わせ、執拗かつ継続的に行われる攻撃。



○ 実施期間：平成24～29年度
○ 所 要 額：平成24年度補正予算 15億円

情報セキュリティ技術の研究開発・実証実験施設の整備

施策概要

○ 政府機関、民間企業等を狙った近時のサイバー攻撃では、技術的に高度な潜在型のマルウェア※等が使用されており、既存の技術では対処が極めて困難。

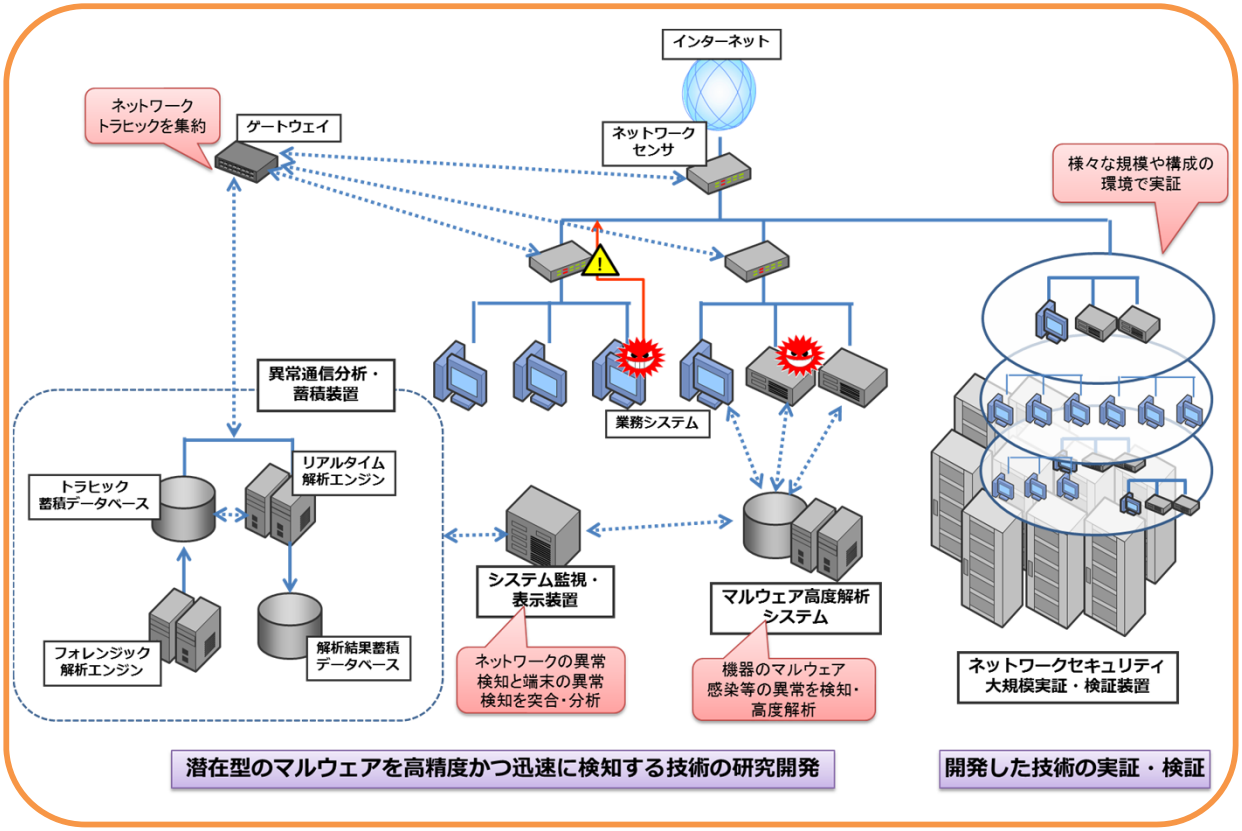
※ マルウェアとは、コンピュータウイルスのような有害なソフトウェアの総称。
潜在型のマルウェアとは、自らの挙動を正常の通信に紛れ込ませ、検知を極めて困難にしているマルウェア。

○ 潜在型のマルウェアへの感染を高精度かつ迅速に検知する技術等、革新的な情報セキュリティ技術の研究開発・実証実験を実施するための施設を、(独)情報通信研究機構(NICT)に整備する。

＜整備対象＞

①潜在型のマルウェアを高精度かつ迅速に検知する技術の研究開発環境

②様々な規模や構成のネットワークを模擬し、開発した技術の実証・検証を行うための環境



○ 所 要 額：平成24年度補正予算 100億円

- ☐ はじめに
- ☐ 情報セキュリティに関する脅威の変遷
- ☐ 政府全体における情報セキュリティ政策の動向
- ☐ 総務省における情報セキュリティ政策の概要
- ☑ パーソナルデータの利用・促進に向けて
- ☐ 終わりに

- 議論の背景等
- 欧米における議論の動向
- 我が国におけるこれまでの取組等
- パーソナルデータの利用・流通に関する研究会の報告について

パーソナルデータの利活用に関する課題と研究会の開催について

◆多種多様なパーソナルデータを含む大量の情報の流通

➢新事業の創出、利便性の向上、より安心・安全な社会の実現

➢プライバシー等の面における不安

◆データの越境流通の加速化

➢グローバルなビジネス展開

➢国際的な自由な情報の流通とプライバシー保護等の双方を確保する必要性

パーソナルデータの利活用とプライバシー保護等の調和を図る必要

国際的に調和の取れた制度の構築が必要

情報の自由な流通とプライバシー保護等の調和に配慮したパーソナルデータの利活用のルールの明確化が必要

総務省の対応

平成24年11月1日より「パーソナルデータの利用・流通に関する研究会」（座長：堀部政男 一橋大学名誉教授）を開催し、検討。

本年（平成25年）4月8日に論点整理、5月20日に報告書案を公表。6月12日に取りまとめ。

構成員

敬称略（順不同）

◎	堀部政男	一橋大学名誉教授（座長）
○	辻井重男	中央大学教授　（座長代理）
	菅谷実	慶應義塾大学教授
	新保史生	慶應義塾大学教授
	曽我部真裕	京都大学教授
	桑子博行	一般財団法人 日本データ通信協会
	岡村久道	弁護士
	長田三紀	全国地域婦人団体連絡協議会
	吉川尚宏	A.T.カーニー株式会社 パートナー
	安岡寛道	野村総合研究所 上級コンサルタント
	岩下直行	株式会社 日立製作所
	菊池公男	富士通株式会社
	奥屋滋	日本電気株式会社
	糸井雅晴	日本アイ･ビー･エム株式会社
	冨沢高明	日本マイクロソフト株式会社

新居眞吾	ＫＤＤＩ株式会社
別所直哉	ヤフー株式会社
関聡司	楽天株式会社
吉田一雄	一般社団法人 日本経済団体連合会
土合成幸	三鷹市
中尾康二	独立行政法人 情報通信研究機構
高橋克巳	日本電信電話株式会社 セキュアプラットフォーム研究所

（オブザーバー）

消費者庁

経済産業省

「パーソナルデータの利用・流通に関する研究会」検討事項（例）

1．適切な流通に向けた、パーソナルデータの取扱いについての基本的な考え方

（1）情報の自由な流通とプライバシー保護等の関係

・情報の自由な流通とプライバシー保護等のバランスを図ることが重要ではないか。

・情報の自由な流通を確保するためにも適切なプライバシー保護等がなされることが必要ではないか。

（2）パーソナルデータの性質に応じた適切な取扱い

・パーソナルデータはその内容（プライバシー情報、センシティブ情報等）に応じて適切に取り扱うことが必要ではないか。

・パーソナルデータはその個人識別性・特定性の強弱に応じて適切に取り扱うことが必要ではないか。

等

2．適切な流通に向けた、パーソナルデータの具体的な取扱いの在り方

（1）パーソナルデータの性質に応じた、プライバシー保護等の観点から適切な取扱い（利用目的の通知、本人の同意、安全管理措置等）を整理する必要があるのではないか。

（2）プライバシーバイデザインの考え方をどのように適用すべきか。

（3）匿名化、暗号化などの技術の利用により、プライバシー保護等を確保しつつ、より情報の自由な流通を確保する方策があるのではないか。

等

3．適切な流通に向けた、安心安全なパーソナルデータの取扱いの確保に向けた方策

（1）プライバシーの保護等について国民の信頼や安心を確保するための方策

・パーソナルデータの適切な取扱いについて、パーソナルデータの本人やパーソナルデータを取り扱う事業者等からの相談等を受け付け、迅速な判断を行うことができる公的な窓口・体制の整備が必要ではないか。

・パーソナルデータを取り扱う事業者等のプライバシー保護等の在り方について適切に評価・監査する体制の整備が必要ではないか。

（2）国際的な情報の円滑な流通の確保のため、プライバシー保護等について国際的なハーモナイゼーションを図ることが重要ではないか。

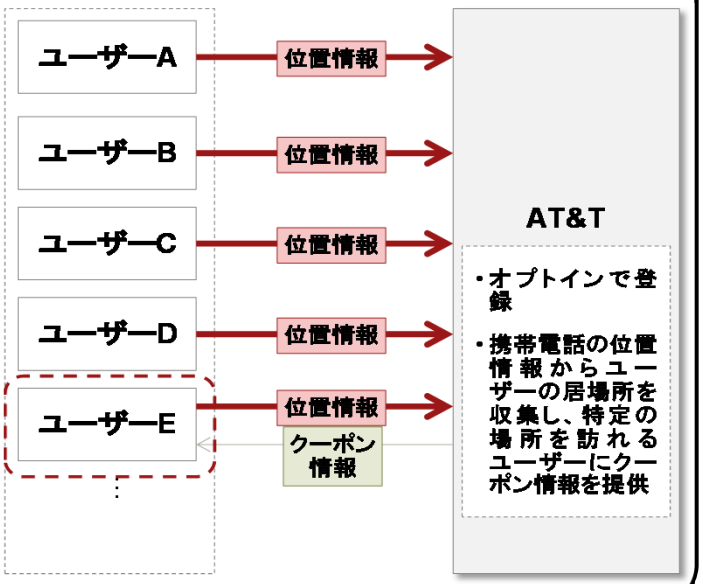
（3）パーソナルデータが我が国から外国へ移転する場合に、適切なプライバシー保護等が行われることを確保する必要があるのではないか。

等

パーソナルデータの利活用の事例①（情報通信業）

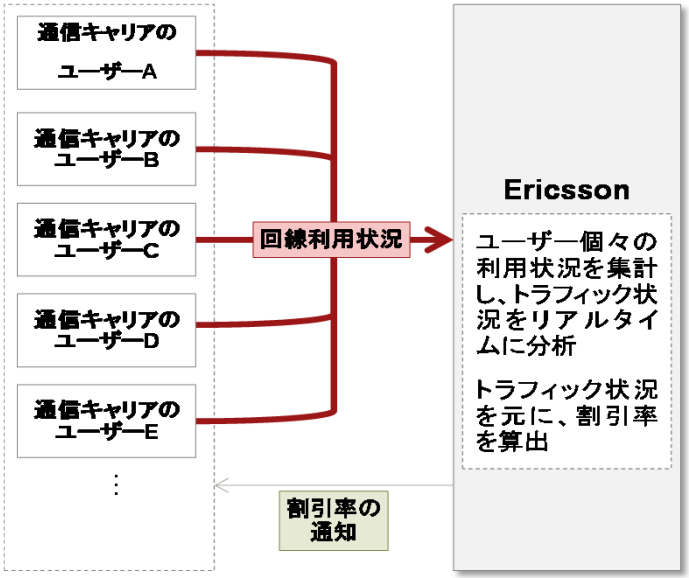
AT&T Shop Alerts（米国）

- AT&Tが、Placecastの位置情報プラットフォームを活用し、同社の顧客に対してクーポンを配信
- 飲食店やイベント開催場所など、一定区域内に入ったユーザーに対し、適切なクーポンや割引情報を配信
- 携帯電話のGPS機能を活用することで、ユーザーに対して適切なタイミングで割引情報を提供することができ、広告効果を高めることが可能に
- ※AT&Tのプライバシーポリシーに、取得する情報の種類、利用目的、第三者提供や情報収集時の同意取得、オプトアウトに関する記載がある



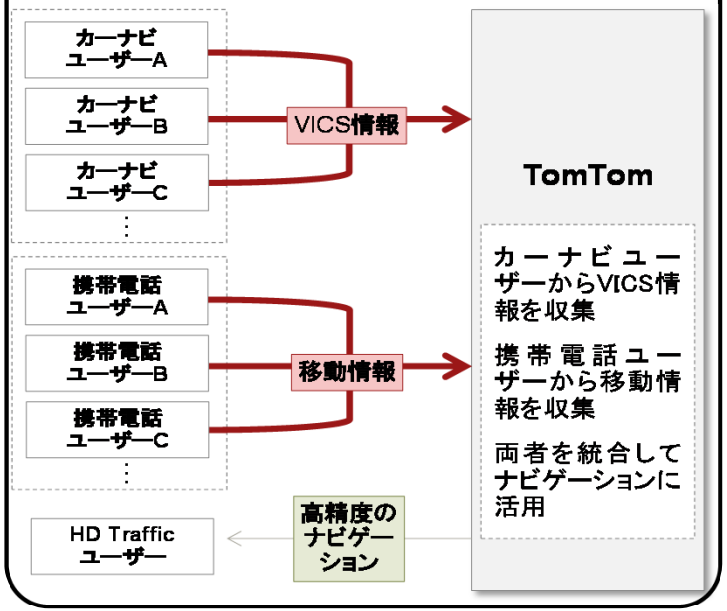
Ericsson DDS（南アフリカ）

- Ericssonが南アフリカの通信キャリアMTNグループと開発したリアルタイム割引サービス（DDS : Dynamic Discount Service)を提供
- 全ユーザーの回線利用状況を集計し、基地局毎のトラフィック状態をリアルタイムに分析
- エリア・時間帯別に、トラフィックに余裕のある場合には高い（最大80%）割引率を動的に設定
- 発展途上国の貧弱な回線であっても、大規模な設備投資を行うことなくトラフィックを最適化可能に
- ※MTNのプライバシーポリシーに、取得する情報の種類、利用目的、情報収集時の同意、情報収集時の同意に基づく第三者提供に関する記載がある



TomTom HD Traffic（オランダ）

- TomTomのカーナビは通信機能を備えており、FM放送を利用して端末の情報を収集（VICSに相当）
- 一方で最大1670万台の携帯電話の基地局情報／GPSデータを匿名化して収集し、利用者の移動速度・進行方向を判別
- 両データを統合することでリアルタイムに精度の高いナビゲーションを提供
- 通常よりも目的地までの時間を平均で15%削減
- ※TomTomのプライバシーポリシーにユーザライセンス取得時の同意取得、取得する情報の種類、利用目的に関する記載がある

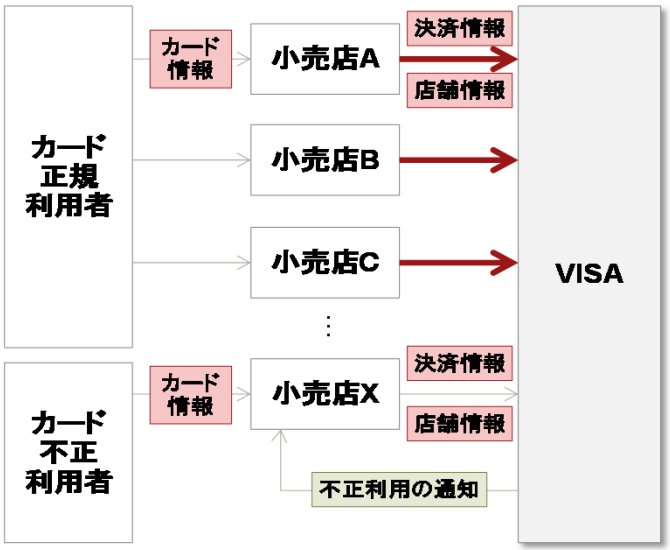


出典：本研究会第4回会合吉川構成員資料、（株）日立コンサルティング作成資料より作成

パーソナルデータの利活用の事例②（金融業・保険業）

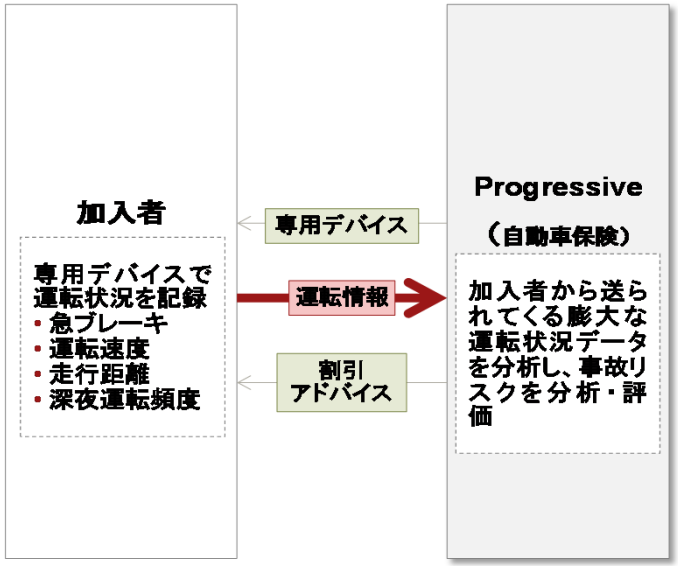
Visa Advanced Authorization（北米）

- 各店舗から送られてくる決済情報を、リアルタイムで照合・分析
- 「短時間に大きく離れた店舗で決済が発生したケース」など、不正利用の可能性が高い取引を監視し、取引が発生したその場で店舗に対して通知を実施
- カードの不正利用をリアルタイムに発見し、不正利用を早期に発見、対応することが可能になり、店舗、正規利用者の双方に対し、より高いセキュリティを提供することが可能に
- ※同サービスに関するプライバシーポリシーは公開されていないが、各店舗での決済情報をVISAが分析し、不正利用と思われる場合に店舗に通知するため、決済情報を第三者提供することはない



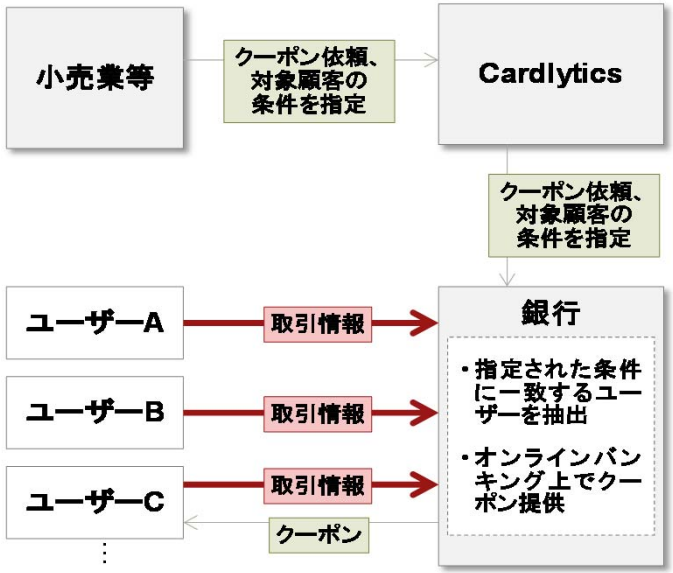
Progressive Snapshot（米国）

- 加入者に専用のデバイス（一種のドライブレコーダー）を配布し、詳細な運転状況を記録
- 加入者の事故リスクを分析・評価、個々人の運転状況に合わせた割引率を算定
- インターネットを通して、運転状況のフィードバックや安全運転のアドバイスを実施
- 蓄積された詳細な行動データを解析することで、リスクを適正に判断可能に
- ※Snapshotサービスの利用規約に、取得する情報の種類とサービス利用時の同意取得、Progressiveのプライバシーポリシーに、取得する情報の種類、利用目的に関する記載がある



Cardlytics（米国）

- クーポンを配布したい小売業者等が、Cardlyticsにクーポンの配布条件を依頼
- Cardlyticsは、銀行に対して該当する顧客の抽出を依頼
- 銀行は取引データを分析して該当顧客を抽出し、対象顧客にインターネットバンキング上でクーポンを提供
- ※対象顧客抽出やクーポン配布は銀行で行われ、Cardlytics等に第三者提供することはない

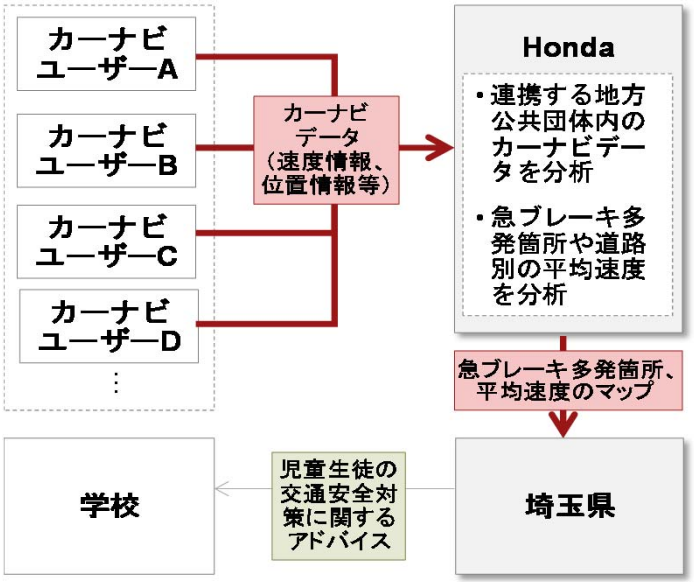


出典：本研究会第4回会合吉川構成員資料、（株）日立コンサルティング作成資料より作成

パーソナルデータの利活用の事例③（行政分野、公益事業）

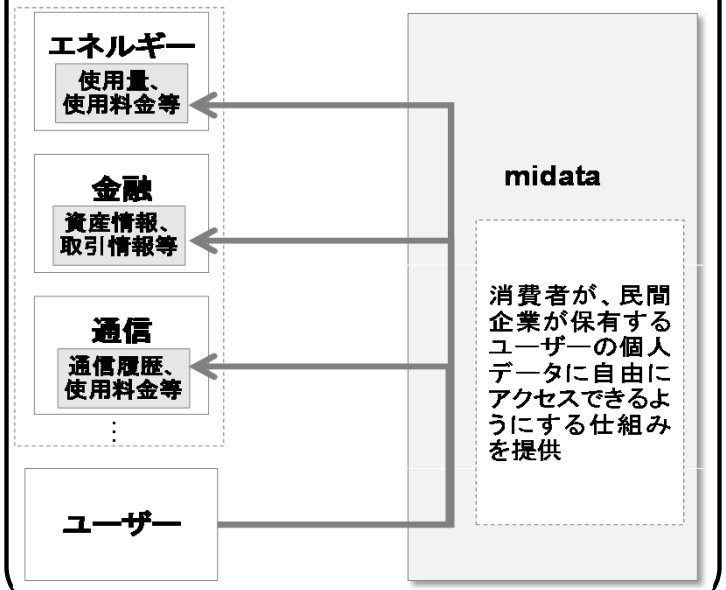
埼玉県 カーナビデータ活用（日本）

- 埼玉県では、Hondaと連携してカーナビデータの分析結果を道路行政に活用
- 車の位置情報や速度情報から急ブレーキの多発箇所を分析・抽出し、区画線の設置や街路樹の伐採によって事故件数が減少
- また、児童生徒等の交通安全対策のため、登下校時の急ブレーキ多発箇所や通学路における車の平均走行速度を分析、登下校時の人員配置や注意喚起に活用
- ※同サービスの利用規約に、取得する情報の種類、利用目的、情報収集時・第三者提供の際の同意取得に関する記載がある



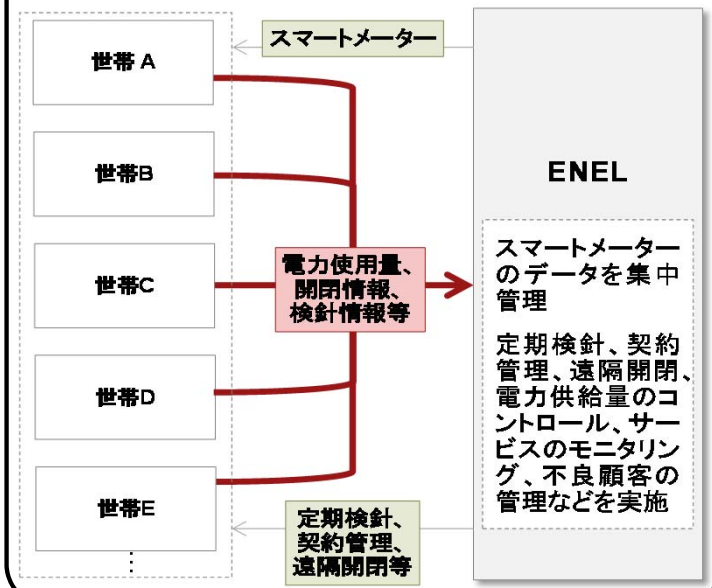
midata（英国）

- 消費者が民間企業の持つ自分の個人データに自由にアクセスできるようにすることを目指し,英政府主導で2011年に開始されたプロジェクト
- midataにはエネルギー、金融、通信などの業界から20を超える企業がパートナーとして個人データを提供
- 民間保有の個人データ活用を狙ったMidataHackathonなども開催された



ENEL Smart Meter（イタリア）

- ENELはイタリアの電力会社であり、スマートメーターの大規模設置を実施、顧客3300万戸のほとんどに導入を完了
- スマートメーターのデータは、PLC（電力線通信）およびGSM（携帯通信）を経由して集中管理
- 定期検針（15分間隔）、契約管理、遠隔開閉、電力供給量のコントロール、サービスのモニタリング、不良顧客の管理などを遠隔で実施可能
- ※パーソナルデータの取扱いは契約時の説明書に記載されているためその内容を確認できないが、世帯からのデータの管理や定期検診等のサービスはENELが行うものであり、データを第三者提供することはない

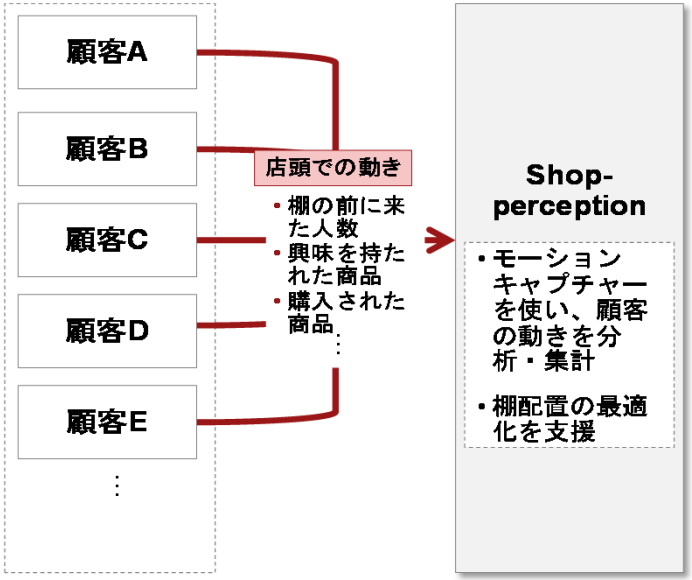


出典：本研究会第5回会合奥屋構成員資料、（株）日立コンサルティング作成資料より作成

パーソナルデータの利活用の事例④（小売業）

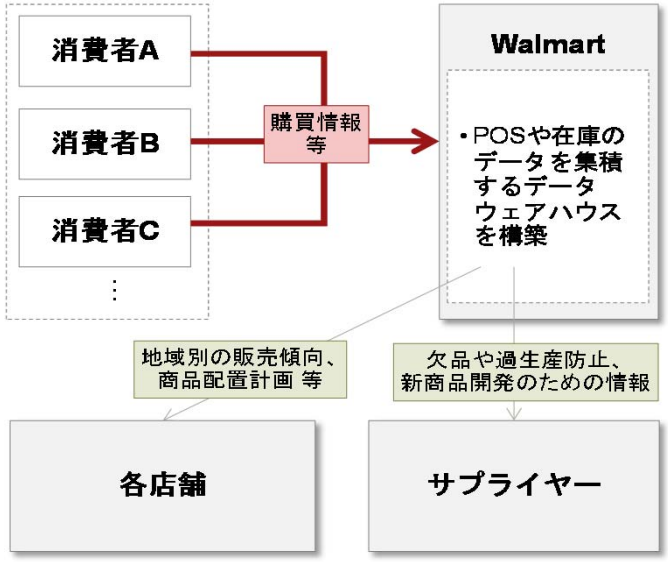
Shopperception（米国）

- 小売店の陳列棚に設置されたKinectモーションキャプチャーシステムにより、手に取られた商品や顧客の動線等を機械的に分析・記録することが可能
- 販売時点のPOS（Point of Sales）データに加え、POB（Point of Buying）データを取得
- 「興味は持たれたが購買に至らなかった商品」と「全く興味が持たれなかった商品」の区別が可能になり、販売促進費の投資を最適化
- ※Shopperceptionのサービスを導入する小売店がパーソナルデータについて適正な取扱いをすれば問題は生じない



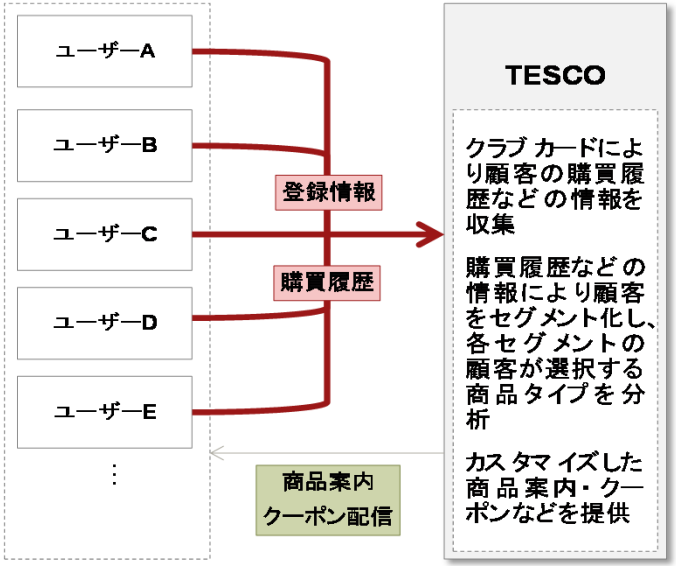
Walmart Data-warehouse（米国）

- Walmartでは、POSや在庫のデータを集積するデータウェアハウスを構築
- POSデータ分析から、同時購入されやすい商品を同じ売り場に配置するなどのクロスマーチャンダイジングを展開
- また、データはサプライヤーとも共有され、店舗とサプライヤーが協力して欠品や過生産の防止、新商品開発等に活用
- ※プライバシーポリシーにて、消費者の購入情報を収集している旨や、データをマーケティング等に活用する旨、サプライヤーと共有する旨について述べている



TESCO Club-card（英国）

- TESCOでは、ポイントプログラムであるクラブカードにより顧客の購買履歴などの情報を収集
- 購買履歴などの情報を用いて顧客を類型化し、各類型の顧客が選択する商品タイプを分析
- 顧客に対し、カスタマイズした商品案内やクーポンなどを提供
- ※クラブカードのプライバシー・クッキーポリシーには、取得する情報の種類、利用目的、Webサイトを通じたサービスを受ける場合にはそれらの情報の取得に同意する旨が記載されている



出典：本研究会第4回会合吉川構成員資料、（株）日立コンサルティング作成資料より作成

- 議論の背景等
- 欧米における議論の動向
- 我が国におけるこれまでの取組等
- パーソナルデータの利用・流通に関する研究会の報告について

EUのパーソナルデータ保護に関する制度（現行制度）①

データ保護指令（1995年）
「個人データ処理及びデータの自由な移動に関する個人の保護に関する指令（95/46/EC）」

分野横断的な個人データ保護に関する規制

（主な内容）
（1）データ内容に関する原則（特定された明示的かつ適法な目的のための取扱い等）
（2）データ取扱いの正当性の基準（データ主体の明確な同意等）
（3）センシティブデータ※の取扱い ※人種又は民族、政治的見解、宗教的又は思想的信条、労働組合への加入、健康又は性生活に関するデータ
（4）データ主体のデータへのアクセス権
（5）取扱いの機密性及び安全性
（6）第三国への個人データの移転に関する規律（第三国が十分なレベルの保護措置を確保していることを条件とする等）
（次頁参照）
（7）独立した監督機関

eプライバシー指令（2002年、2009年改正）
「電子通信部門における個人データの処理とプライバシーの保護に関する指令（2002/58/EC）」

電子通信部門に関するデータ保護指令の特則

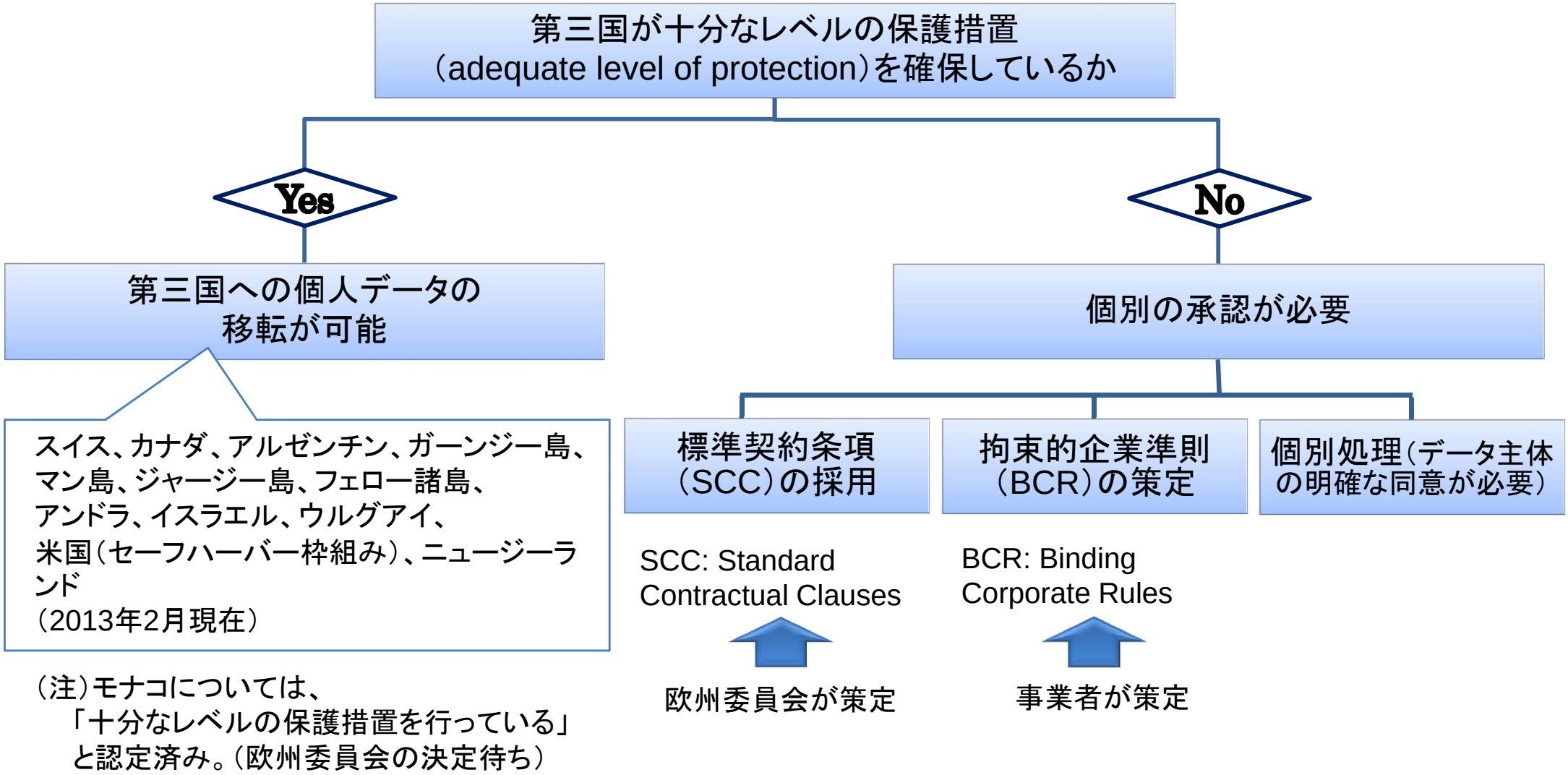
（主な内容）
（1）通信の秘密保持
（2）Cookieの利用に当たって内容を明示しオプトインによる利用者同意を求める
（3）ロケーションデータを利用する際にオプトインによる利用者同意を求める

英国	フランス	ドイツ	イタリア
データ保護法	情報処理、情報ファイル及び自由に関する法律	連邦データ保護法	個人データの処理に関する個人その他の主体の保護に関する法律

等

EUのパーソナルデータ保護に関する制度（現行制度）②

【 データ保護指令における第三者への個人データ移転の仕組み 】



（注）モナコについては、
「十分なレベルの保護措置を行っている」
と認定済み。（欧州委員会の決定待ち）

EUのパーソナルデータ保護に関する制度（データ保護規則提案）①

データ保護指令（1995年）

↓

eプライバシー指令（2002年、2009年改正）

- 急速な技術進展
- 情報の共有・収集の規模の劇的な増加

↓

データ保護規則提案（2012年1月）

立法手続きを開始

① EU域内における規制の単一化・簡素化

- 国内法制化の不要な「規則」に変更
- 一国からの承認を得れば、他国の当局からの承認は不要
- データ保護当局間の調査協力のメカニズム

② より強固な個人データ保護ルールの整備

③ 個人データ保護に関するグローバルな課題への対応

EUのパーソナルデータ保護に関する制度（データ保護規則提案）②
－より強固なパーソナルデータ保護ルール－

事業者

個人データ

個人

「プライバシー・バイ・デザイン」原則

- 新サービスの導入時、データ保護への考慮の義務付けの導入
- 個人の権利や自由に対するリスクを伴う個人データの取扱いを行うに当たって、当該取扱いが個人データの保護に対して与える影響度の評価（PIA: Privacy Impact Assessment プライシー影響評価）を実施する必要がある旨の規定
- 「データ保護職員」の任命義務（250人以上の従業員の雇用などの要件を満たす事業者が対象）

個人データ漏えい時の通知義務

- データ保護当局に対しては可能な場合24時間以内に、個人に対しては当該個人プライバシー等に悪影響を及ぼす可能性がある際には遅滞なく通知

忘れられる権利

- データ削除に関する現行法令における個人の権利をより明確化するとともに、データ管理者は、ネット上での個人データへのリンクやコピー・複製された個人データについて、当該個人から削除要求があった場合、当該要求を（それらデータを扱う）第三者に対して通知するなど、あらゆる合理的手段を講ずる義務がある旨規定

データ持ち運びの権利

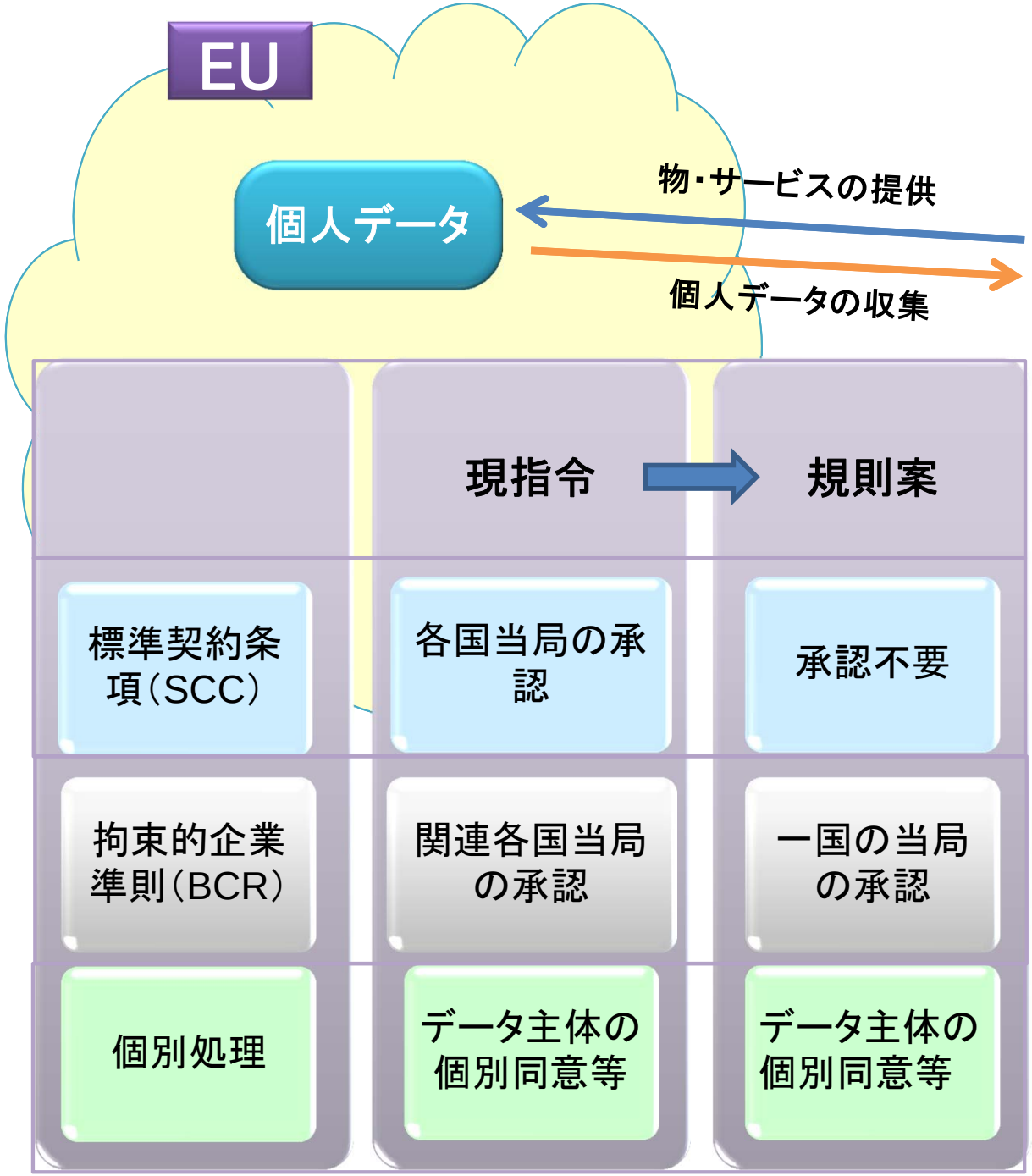
- 共通化されたフォーマットで電子的に自らのデータのコピーをデータ管理者から取得できるとともに、自らのデータをあるアプリケーションから別のアプリケーションに移転させることができる権利について規定

同意の明示

オプトイン原則

- 個人データの取得に当たって必要な同意は明示的な（explicit）ものであることを要する旨の規定

EUのパーソナルデータ保護に関する制度（データ保護規則提案）③
－グローバルな課題への対応－



- データ保護規則の域外適用
- EU域内に代理人を置く必要（一定の要件を満たす場合）

域外事業者

規則に違反した場合（域内事業者を含む）

制裁（課徴金）

最大で、100万ユーロ、又は事業者の全世界での売上高の2%相当額の課徴金

米国（連邦政府）のパーソナルデータ保護に関する制度

分野横断的な個人情報保護法は存在しない

（民間部門）

政府部門	健康情報等	信用情報	通信分野	金融部門	児童のプライバシー
プライバシー法（Privacy Act of 1974）	医療保険の相互運用性及び説明責任に関する法律（HIPPA）	公正信用報告法(FCRA)	電子通信プライバシー法（ECPA）	金融サービス近代化法（Gramm-Leach-Bliley Act）	児童オンラインプライバシー保護法（COPPA）

自主規制

（参考）EU・米国間のセーフハーバーの枠組み（2000年7月）

商務省

セーフハーバー原則

① 告知：利用目的等の告知
② 選択：オプトイン、オプトアウトの機会の提供
③ 第三者への提供：告知と選択の原則の適用等
④ セキュリティ
⑤ データの完全性
⑥ アクセス；開示、訂正、変更、削除請求
⑦ 執行

企業

- セーフハーバー原則遵守の宣言
- プライバシーポリシーを公表
- セーフハーバー原則の遵守の確約書を商務省に提出
- 商務省は当該企業名等をウェブサイトに掲載

FTC

【違反行為が発覚した場合】

- 「不公正又は欺瞞的な行為又は慣行(unfair or deceptive acts or practices)」（FTC法第5条）として、排除措置・課徴金等の対象
- 民事責任も問われる。

消費者プライバシー権利章典

米国政府発表：“ Consumer Data Privacy in a Networked World ” (2012年2月23日)

個人プロファイリングを念頭

「消費者プライバシー権利章典」(The Consumer Privacy Bill of Rights)

1	個人による管理	：消費者は、自分の個人データを企業が収集し、それを使用する方法について管理する権利を有する。
2	透明性	：消費者は、プライバシー及びセキュリティの企業実務に関する情報に容易に理解しアクセスできる権利を有する。
3	**経緯の尊重**	**：消費者は、企業が、自分の個人データを、自分が情報を提供した経緯に沿う方法で、収集、使用、開示することを期待する権利を有する。**
4	セキュリティ	：消費者は、個人データを保護し、責任持って処理する権利を有する。
5	アクセス及び正確性	：消費者は、使用可能な形式で、また、データの機微性及びデータが不正確であった場合に消費者に悪影響を与える危険度に応じた方法で、個人データにアクセスし訂正する権利を有する。
6	**対象を絞った収集**	**：消費者は、企業が収集及び保持する個人データに合理的な制限を設ける権利を有する。**
7	説明責任	：消費者は、この権利章典の遵守を保証するための適切な措置を講じる企業によって個人データが処理される権利を有する。

NTIAにおけるcode of conduct (行動規範)の検討

Do Not Track（オプトアウト原則）

関係者間プロセスの強化

- 行動規範を採用するかどうかは企業が最終判断
- 遵守を公言した企業が違反した場合、FTCは行動規範に基づき、執行可能。

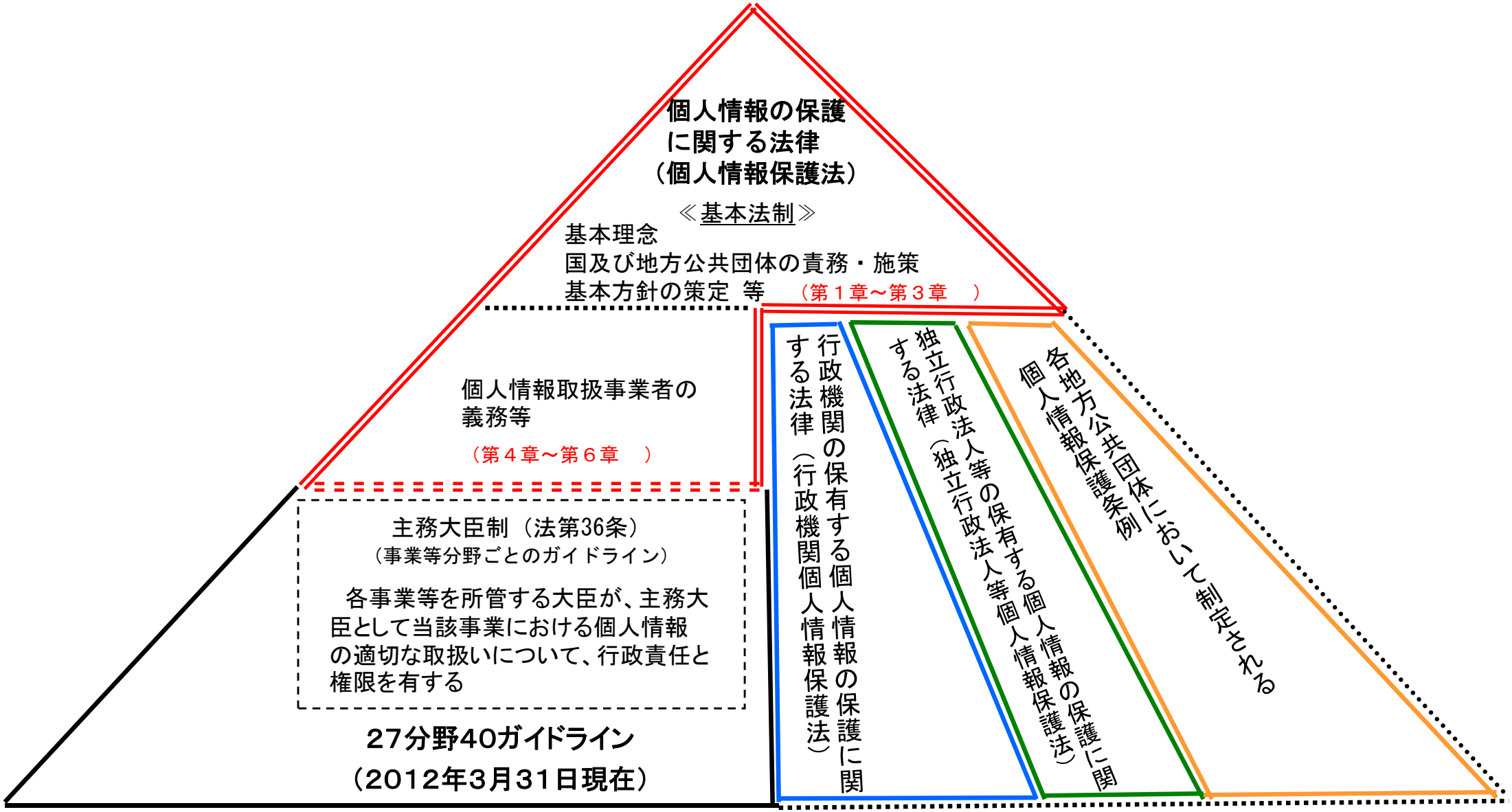
連邦取引委員会（FTC）の執行能力の向上

国際的な相互運用性の促進

- 相互認証・執行協力が必要

- 議論の背景等
- 欧米における議論の動向
- 我が国におけるこれまでの取組等
- パーソナルデータの利用・流通に関する研究会の報告について

我が国の個人情報保護法の体系



○配慮原則

◆対象情報

配慮原則の対象となる情報は、特定の端末、機器及びブラウザ等を識別することができるものとする。対象情報は、個人情報保護法上の個人情報であるか否かを問わない。

◆対象事業者

対象となる事業者は、対象情報を事業（ただし、対象情報を蓄積せずに行う事業は除く。）の用に供している者とする。

◆配慮原則

①広報、普及、啓発活動の推進

対象事業者その他の関係者は、利用者のリテラシーの向上や不安感や不快感の払拭に資するべく、対象情報を活用したサービスの仕組みや、本配慮原則に基づく取組について、広報その他の啓発活動に努めるものとする。

②透明性の確保

対象事業者その他の関係者は、対象情報の取得・保存・利活用及び利用者関与の手段の詳細について、利用者に通知し、又は容易に知り得る状態に置く（以下「通知等」という。）よう努めるものとする。通知等に当たっては、利用者が容易に認識かつ理解できるものとするよう努めるものとする。

③利用者関与の機会の確保

対象事業者は、その事業の特性に応じ、対象情報の取得停止や利用停止等の利用者関与の手段を提供するよう努めるものとする。

④適切な手段による取得の確保

対象事業者は、対象情報を適正な手段により取得するよう努めるものとする。

⑤適切な安全管理の確保

対象事業者は、その取り扱う対象情報の漏えい、滅失又はき損の防止その他の対象情報の安全管理のために必要かつ適切な措置を講じるよう努めるものとする。

⑥苦情・質問への対応体制の確保

対象事業者は、対象情報の取扱いに関する苦情・質問への適切かつ迅速な対応に努めるものとする。

スマートフォン プライバシー イニシアティブ（2012年8月）
（利用者視点を踏まえたICTサービスに係る諸問題に関する研究会）

スマートフォンの利用者情報の取扱いに関する包括的な対策を提案。アプリケーション提供者や情報収集モジュール提供者等を中心に、アプリケーション提供サイト運営事業者・OS提供事業者、移動体通信事業者等のスマートフォンの関係事業者に広く適用可能な**「スマートフォン利用者情報取扱指針」**等を示す（以下は同指針の概要）。

【総論】
- **1 基本原則**
  - ① 透明性の確保
  - ② 利用者関与の機会の確保
  - ③ 適正な手段による取得の確保
  - ④ 適切な安全管理の確保
  - ⑤ 苦情・相談への対応体制の確保
  - ⑥ プライバシー・バイ・デザイン
- 2 適用対象
- 3 用語の定義

【各論】

1 利用者情報取得者における取組（アプリ提供者、情報収集モジュール提供者、広告配信事業者）

（1）プライバシー・ポリシーの作成

☞ 以下の項目を記載したプライバシーポリシーを、アプリケーションや情報収集モジュールごとに分かりやすく作成する（簡略版も作成する。）。

（記載項目）
- ① 情報を取得するアプリ提供者等の氏名又は名称
- ② 取得される情報の項目
- ③ 取得方法
- ④ 利用目的の特定・明示
- ⑤ 通知・公表又は同意取得の方法、利用者関与の方法*1,2
- ⑥ 外部送信・第三者提供・情報収集モジュールの有無
- ⑦ 問合せ窓口
- ⑧ プライバシーポリシーの変更を行う場合の手続

*1 同意取得： 一部のプライバシー性の高い情報については、原則同意を取得する（電話帳、位置情報、通信履歴等）。
*2 利用者関与： 利用者がアプリによる利用者情報の利用や取得の中止を希望する場合に、その方法を記載する。

（2）適切な安全管理措置

- 利用者情報の漏洩、滅失、毀損の危険回避の措置を講ずる。

（3）情報収集モジュール提供者に関する特記事項

- アプリケーション提供者へ①取得する情報の項目、②利用目的、③第三者提供の有無等について通知する。

2 その他の関係事業者における取組

（1）移動体通信事業者・端末提供事業者： アプリ提供者の適切な取扱い支援・啓発活動、連絡通報窓口の整備等を行う。
（2）アプリ提供サイト運営事業者、OS提供事業者： 同上、OSによる利用許諾がある場合に分かりやすい説明を行う。
（3）その他関係しうる事業者： アプリケーション紹介サイトは有益な情報源となり得る。

- 議論の背景等
- 欧米における議論の動向
- 我が国におけるこれまでの取組等
- パーソナルデータの利用・流通に関する研究会の報告について

パーソナルデータ利活用の基本理念と原則

パーソナルデータの利活用の基本理念

① 個人情報保護を含むパーソナルデータの保護は、主としてプライバシー保護のために行うものである。

② プライバシーの保護は、絶対的な価値ではなく、表現の自由、営業の自由などの他の価値との関係で相対的に判断されるべきものである。

パーソナルデータの利活用の原則 （基本理念の具体化）

- 透明性の確保
- 本人の関与の機会の確保
- 取得の際の経緯（コンテキスト）の尊重
- 必要最小限の取得
- 適正な手段による取得
- 適切な安全管理措置
- プライバシー・バイ・デザイン

パーソナルデータの範囲

パーソナルデータ（個人に関する情報）

【保護されるパーソナルデータ 】
「実質的個人識別性」*を有するパーソナルデータ

＊プライバシーの保護という基本理念を踏まえて実質的に判断される個人識別性
（現行の個人情報保護法の「個人情報」の範囲との関係等は、さらに検討が必要）

（保護されるパーソナルデータに含まれるべきと考えられるもの）

・個人のPC・スマートフォン等の識別情報（端末ID等）など
一義的には特定の機械を識別するものであるが、実質的に特定の個人と継続的に結びついているもの

・継続的に収集される購買・貸出履歴、視聴履歴、位置情報等
個人識別性の要件を満たす情報と連結しない形で取得・利用される場合でも、特定の個人を識別することができるようになる可能性が高いもの

【保護されるパーソナルデータ以外のパーソナルデータ】
パーソナルデータの利活用の枠組みからは制約を受けず、自由に利活用が可能
（統計情報、匿名化情報等）

パーソナルデータの性質に応じた取扱い

保護されるパーソナルデータ

①一般パーソナルデータ

（保護されるパーソナルデータのうち
プライバシー性が高くないもの）

- コンテキストに沿う場合 → 明示的な同意は不要
- コンテキストに沿わない場合 → 明示的かつ個別的な同意が必要

②慎重な取扱いが求められるパーソナルデータ

（センシティブデータ以外のプライバシー性が高いパーソナルデータ）

- コンテキストに沿う場合
  - 【プライバシー性】
  - 比較的低い → 明示的かつ包括的な同意
  - 比較的高い → 明示的かつ個別的な同意が必要
- コンテキストに沿わない場合 → 明示的かつ個別的な同意が必要

③センシティブデータ

（プライバシー性が極めて高いもの）

→ 明示的かつ個別的な同意が必要

【検討事項】

- 災害時等の例外的取扱い
- プライバシー性の高低の具体的なあり方
- 同意の撤回やオプトアウトを可能とする仕組み
- 適切な表示の在り方

等

パーソナルデータの利活用に関するルール策定・遵守確保

国、企業、消費者、有識者等、多種多様な関係者が参画するオープンなプロセス

マルチステークホルダープロセスの活用

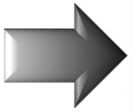
国（各省庁等）の役割

マルチステークホルダープロセスを活用したルール策定

- 場の提供
- ルールの対象・範囲の設定
- 求められるルールの内容の提示
- 議論の方向性・結論の検証

マルチステークホルダープロセスを活用したルール遵守確保

- ルールの普及啓発
- ルールを遵守している企業を国民・消費者に周知



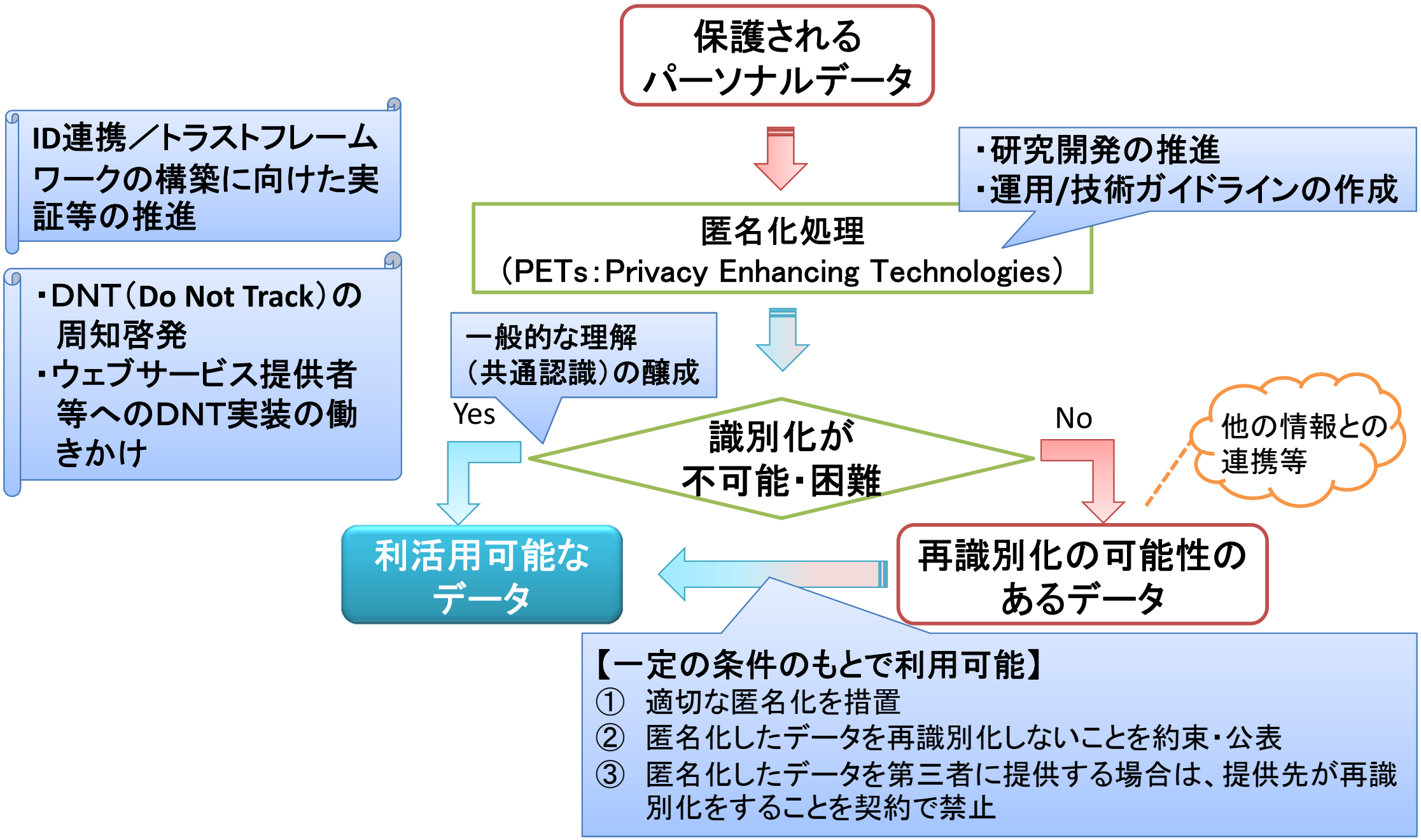
事前相談・ADR機能を持つ機関の設置

- ルールに関する判断の提示
- 消費者と企業間の紛争解決

契約約款への位置付け

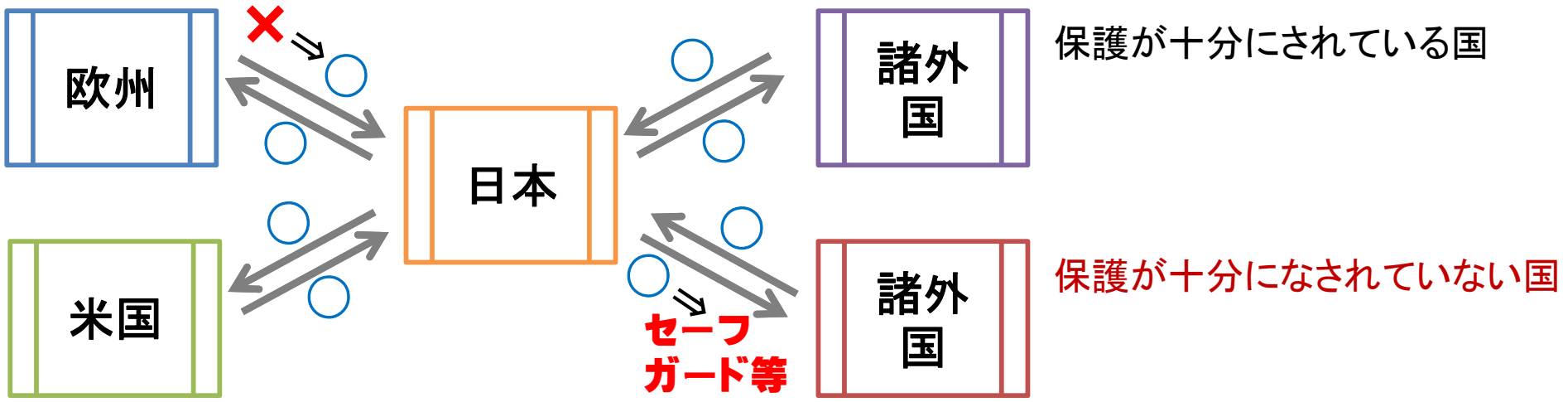
各企業

技術的解決策の有効性


保護される
パーソナルデータ
匿名化処理
（PETs：Privacy Enhancing Technologies）
・研究開発の推進
・運用/技術ガイドラインの作成
ID連携／トラストフレームワークの構築に向けた実証等の推進
・DNT（Do Not Track）の周知啓発
・ウェブサービス提供者等へのDNT実装の働きかけ
一般的な理解
（共通認識）の醸成
Yes
識別化が
不可能・困難
No
他の情報との
連携等
利活用可能な
データ
再識別化の可能性の
あるデータ
【一定の条件のもとで利用可能】
① 適切な匿名化を措置
② 匿名化したデータを再識別化しないことを約束・公表
③ 匿名化したデータを第三者に提供する場合は、提供先が再識別化をすることを契約で禁止

国際的なパーソナルデータの利用・流通の確保

国際的に調和のとれたパーソナルデータの利活用の枠組みを実現する必要



【検討課題】

- 国際的なパーソナルデータ保護の執行協力の可能性
- 我が国のパーソナルデータ保護のルールの国際的な適用の可能性
- 保護が十分になされていない国等への日本からパーソナルデータを移転する場合に、十分なセーフガードを求めること
- 海外から日本国内への情報流通についても、円滑に行われる環境の確保

パーソナルデータの利活用の枠組みの本格的な実施

・事業者の自主的な取組みや現行制度の運用改善等では、法的拘束力が十分でなく、永続性・安定性の確保のためには、個人情報保護法の在り方の見直しなど制度的な取組が必要不可欠。

・これにより、企業の国際展開や国境を越えたビッグデータの活用などが容易になり、世界最高水準のICT社会の実現、我が国の経済成長に寄与。

以下の事項について、政府全体として速やかに検討を進めていくことが必要

○我が国におけるプライバシー・コミッショナー制度

- パーソナルデータに関し、国民の信頼を確保し、実質的な判断を行う、**専門的な知見を有する人材が、分野横断的に迅速かつ適切に処理していく体制の整備**が不可欠
- パーソナルデータの保護については、**独立した第三者機関であるプライバシー・コミッショナーを設置している国**が、**欧米など先進国を始め国際的には多数**

  これを前提に、**各国のプライバシーコミッショナーが意見表明・調整を行う体制が国際的に形成**されている。
- ＥＵは日本がパーソナルデータの十分な保護を行っているとは認定しておらず、ＥＵと我が国の間のパーソナルデータの自由な流通に支障

○マルチステークホルダープロセス等の実効性の確保

- 企業等が**自主的に宣言したポリシー・ルール等への遵守を確保するための制度**整備
- **マルチステークホルダープロセスに参加する企業**への**インセンティブ**
- **マルチステークホルダープロセスに参加しない企業**にも**プライバシー保護を確保**するための仕組み

○現行の個人情報保護法に関する制度整備

- 小規模事業者の扱い、共同利用の在り方、プライバシー保護を実質的に確保するための認証制度の在り方等

諸外国のパーソナルデータ保護の監督機関

	監督機関名称	所管法令	管轄	組織形態
米国	連邦取引委員会 (Federal Trade Commission(FTC)) ※Department of Health and Human Services、Federal Communication Commissionなども個別分野を監督	連邦取引委員会法、金融サービス現代化法、公正信用報告法、児童オンラインプライバシー保護法　等	民間部門 （一部事業を除く）	委員会 （5名）
ＥＵ	欧州データ保護監察官 (European Data Protection Supervisor(EDPS))	Regulation (EC) No 45/2001 of 18 December 2000	EU機関	独任制
英国	情報コミッショナー （Information Commissioner）	データ保護法、情報自由法、プライバシー及び電子通信規則、環境情報規則	民間部門・公的機関	独任制
フランス	情報処理及び自由に関する国家委員会 (Commission nationale de l'informatique et des libertés(CNIL))	情報処理、情報ファイル及び自由に関する1978 年1月6日の法律第78-17号	民間部門・公的機関	委員会 （17名）
ドイツ	連邦データ保護・情報自由監察官	ドイツ連邦データ保護法 （民間部門・公的機関を包括的に規制）	鉄道・郵便・通信部門及び連邦の公的機関	独任制
	各州の監督機関		鉄道・郵便・通信部門以外の民間部門及び各州の公的機関	州により異なる
カナダ	カナダプライバシーコミッショナー (Privacy Commissioner of Canada)	プライバシー法（連邦の公的機関）、個人情報保護及び電子文書法（連邦及び州の民間部門（４州は州法が適用））	民間部門・連邦の公的機関	独任制
	各州プライバシーコミッショナー	各州の法律	各州公的機関 （民間部門も対象とする場合あり）	独任制
ニュージーランド	プライバシーコミッショナー事務局 (Privacy Commissioner)	プライバシー法	民間部門・公的機関	独任制
オーストラリア	オーストラリア情報コミッショナー（Australian Information Commissioner ） プライバシーコミッショナー（Privacy Commissioner） （前者が後者の上位にあたる。）	オーストラリア情報コミッショナー法（Australian Information Commissioner Act） プライバシー法（Privacy Act）	民間部門・公的機関	独任制
シンガポール	シンガポール個人情報保護委員会(Personal Data Protection Commission Singapore(PDPC))	個人情報保護法(PDPA)	民間部門	委員会 （3～17名）
韓国	個人情報保護委員会	個人情報保護法	民間部門・公的機関	委員会 （15名）

「行政手続における特定の個人を識別するための番号の利用等に関する法律案」（番号法案）（2013年3月に提出されたもの）の概要

基本理念 （第3条）

○　個人番号及び法人番号の利用に関する施策の推進は、個人情報の保護に十分に配慮しつつ、社会保障、税、災害対策に関する利用の促進を図るとともに、他の行政分野及び行政分野以外の国民の利便性の向上に資する分野における利用の可能性を考慮して行う。

個人番号 （第7条～第16条）

○　市町村長は、法定受託事務として、住民票コードを変換して得られる個人番号を指定し、通知カードにより本人に通知。盗用、漏洩等の被害を受けた場合等に限り変更可。中長期在留者、特別永住者等の外国人住民も対象。
○　個人番号の利用範囲を法律に規定。①国･地方の機関での社会保障分野、国税･地方税の賦課徴収及び災害対策等に係る事務での利用、②当該事務に係る申請･届出等を行う者（代理人･受託者を含む。）が事務処理上必要な範囲での利用、③災害時の金融機関での利用に限定。
○　番号法に規定する場合を除き、他人に個人番号の提供を求めることは禁止。本人から個人番号の提供を受ける場合、個人番号カードの提示を受ける等の本人確認を行う必要。

個人番号カード （第17条･第18条）

○　市町村長は、顔写真付きの個人番号カードを交付。
○　政令で定める者が安全基準に従って、ＩＣチップの空き領域を本人確認のために利用。（民間事業者については、当分の間、政令で定めないものとする。）

個人情報保護 （第19条～第57条等）

○　番号法の規定によるものを除き、特定個人情報（個人番号をその内容に含む個人情報）の収集･保管、特定個人情報ファイルの作成を禁止。
○　特定個人情報の提供は原則禁止。ただし、行政機関等は情報提供ネットワークシステムでの提供など番号法に規定するものに限り可能。
○　民間事業者は情報提供ネットワークシステムを使用できない。
○　情報提供ネットワークシステムでの情報提供を行う際の連携キーとして個人番号を用いないなど、個人情報の一元管理ができない仕組みを構築。
○　国民が自宅のパソコンから情報提供等の記録を確認できる仕組み（マイ･ポータル）の提供、特定個人情報保護評価の実施、特定個人情報保護委員会の設置、罰則の強化など、十分な個人情報保護策を講じる。

法人番号 （第58条～第61条）

○　国税庁長官は、法人等に法人番号を通知。法人番号は原則公表。民間での自由な利用も可。

検討等 （附則第6条）

○　法施行（公布後３年以内）後３年を目途として、個人番号の利用範囲の拡大について検討を加え、必要と認めるときは、国民の理解を得つつ、所要の修正を講ずる。
○　法施行後１年を目途として、特定個人情報保護委員会の権限に特定個人情報以外の個人情報の取扱いに関する監視・監督を追加すること等について検討を加え、その結果に基づいて所要の措置を講ずる。

政府における検討状況（IT総合戦略本部）

世界最先端IT国家創造宣言（平成25年6月14日閣議決定）　【抜粋】

Ⅲ.目指すべき社会・姿を実現するための取り組み

1．革新的な新産業・新サービスの創出と全産業の成長を促進する社会の実現

（1）オープンデータ・ビッグデータの活用の推進

② ビッグデータ利活用による新事業・新サービス創出の促進

個人や機器・インフラの行動・状態等が日々刻々とITにより流通・蓄積されており、この「ビッグデータ」の利活用による、付加価値を生み出す新事業・新サービス創出を強力に推進する。

このため、「ビッグデータ」のうち、特に利用価値が高いと期待されている、個人の行動・状態等に関するデータである「パーソナルデータ」の取扱いについては、その利活用を円滑に進めるため、個人情報及びプライバシーの保護との両立を可能とする事業環境整備を進める。また、**環境整備に当たっては、**プライバシーや情報セキュリティ等に関するルールの標準化や国際的な仕組み作りを通じた利便性向上及び国境を越えた円滑な情報移転が重要であり、OECD 等国際交渉の場を活用し、**国際的な連携を推進する。**

（中略）

また、速やかに、ＩＴ総合戦略本部の下に新たな検討組織を設置し、個人情報やプライバシー保護に配慮したパーソナルデータの利活用のルールを明確化した上で、個人情報保護ガイドラインの見直し、同意取得手続きの標準化等の取り組みを年内できるだけ早期に着手するほか、新たな検討組織が、第三者機関の設置を含む、新たな法的措置も視野に入れた、制度見直し方針（ロードマップを含む）を年内に策定する。

さらに、2014 年以降に、制度見直し方針に示されたロードマップに従って、国際的な連携にも配慮しつつ、順次パーソナルデータ利活用環境を整備し、利活用を促進する。

（後略）

- ☐ はじめに
- ☐ 情報セキュリティに関する脅威の変遷
- ☐ 政府全体における情報セキュリティ政策の動向
- ☐ 総務省における情報セキュリティ政策の概要
- ☐ パーソナルデータの利用・促進に向けて
- ☑ 終わりに

終わりに

我が国の経済発展を支える世界最高水準のICT 社会の実現

・政府、重要インフラの情報セキュリティ対策の強化

→ 電気通信事業者、各関係機関との協力、連携による対策を推進

ICT を利用した安全・便利な生活環境実現

・利用者の情報セキュリティ対策への意識の向上

→電気通信事業者、ベンダー、研究機関等との連携による
インターネット利用者向けの対策の実施、普及啓発活動を推進

ご清聴ありがとうございました

国民のための情報セキュリティサイト

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/