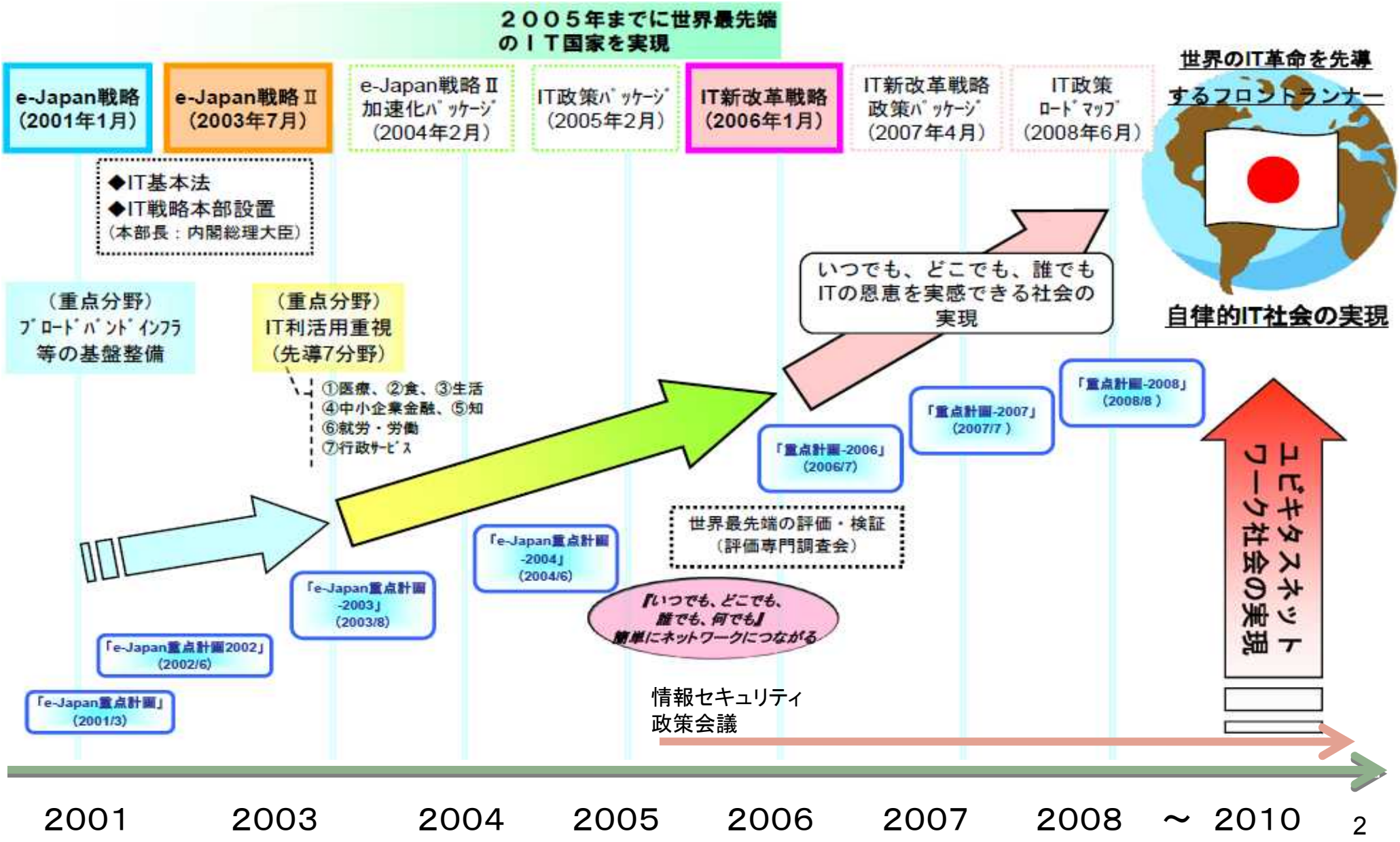
総務省の情報セキュリティ政策

中野　正康

総務省　情報流通行政局
情報セキュリティ対策室長

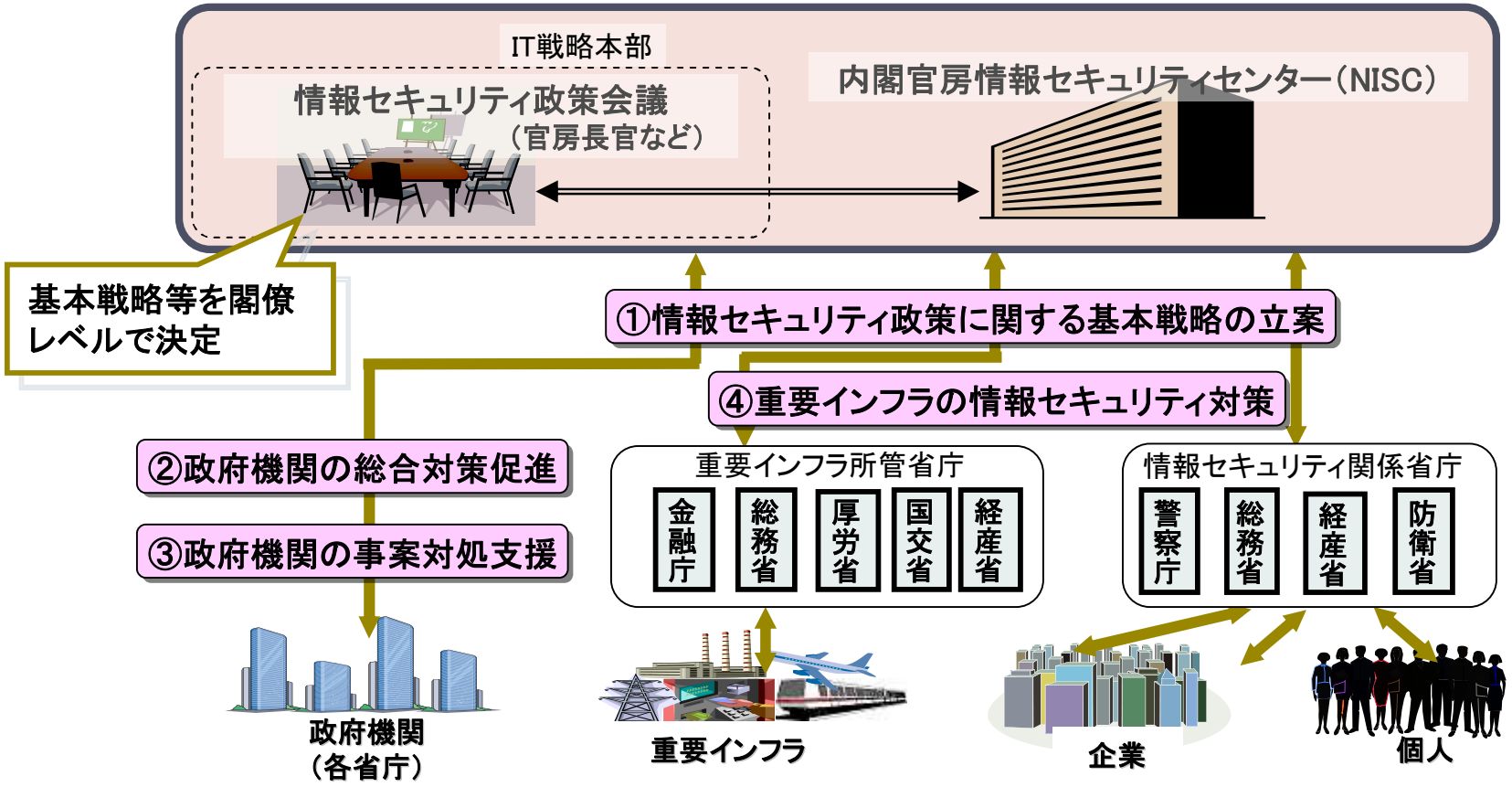
平成22年2月16日

政府のICT戦略の推移



情報セキュリティ政策会議及び内閣官房情報セキュリティセンター（NISC）

- 「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」（2004年12月7日IT戦略本部決定）を受け、情報セキュリティ問題に関する政府中核機能の強化に向けて機能・体制等を整備。
  - 2005年4月25日、内閣官房情報セキュリティセンター（NISC；National Information Security Center）を設置。
  - 2005年5月30日、IT戦略本部の下に「情報セキュリティ政策会議」（議長：内閣官房長官）を設置。
  - 2006年2月2日、第一次情報セキュリティ基本計画公表（情報セキュリティ政策会議決定）
  - 2009年2月3日、第二次情報セキュリティ基本計画公表（同上）



※重要インフラ：情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流

「第２次情報セキュリティ基本計画」2009～2011

「事故前提社会への対応強化」「合理的アプローチ」等を柱に新たな基本計画を策定

	政府・地方公共団体	重要インフラ	企業	個人
対策実施４領域における取組	◆推進体制確立（年次報告書作成・公表等） ◆事業継続性確保の検討、サイバー攻撃等への緊急対応能力強化	◆安全基準の整備等 ◆情報共有体制の強化 ◆セプターカウンシル ◆共通脅威分析、分野横断的演習の実施	◆情報セキュリティ・ガバナンスの促進 ◆対策ツール提供 ◆中小企業の対策促進 ◆コンピュータウィルス等への対応体制の強化	◆ 学校や地域における情報モラル教育の推進 ◆ 個人の質問対応等を行う地域サポータ育成 ◆ サービス提供者のリスク情報等の提供促進
主体	政府機関統一基準	重要インフラ行動計画	各所管省庁の施策	各省庁の施策

情報提供

自身の有する情報を預ける主体 ：新たな課題として、関係機関等が協力しながら取組みを検討・推進

横断的事項

技術戦略の推進
◆セキュリティ対策の機器・技術開発の推進

情報セキュリティ人材の育成・確保
◆ 保有スキルの見える化、政府の人材育成

国際連携・協調
◆ 脅威把握の官民連携、アジアの知恵結集

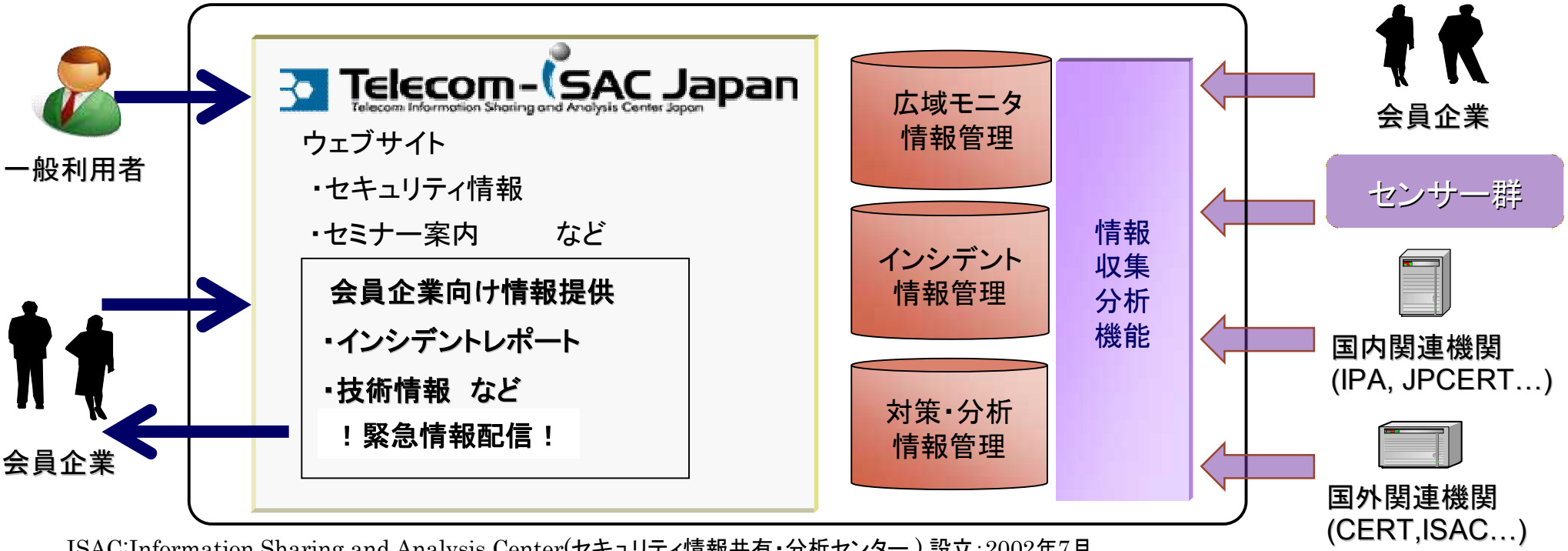
犯罪取締まり・保護救済
◆ 犯罪取締りのための基盤整備の推進

情報共有・分析　Telecom-ISAC Japan

◆国内の主要ISPが発起人となり、2002年からスタート

◆インシデント情報等を収集・分析し、業界内で共有することが目的

共有・分析する情報：　①システムの脆弱性、②対抗策・ベストプラクティス、③サイバー攻撃・犯罪、等



ISAC:Information Sharing and Analysis Center(セキュリティ情報共有・分析センター) 設立：2002年7月
〈正式名称〉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
〈会員企業〉NEC、NTTコミュニケーションズ、KDDI、IIJ、ニフティ、日立、沖電気、ソフトバンクBB、パナソニック電工、NTT東日本、NTT西日本、NTTビジュアル通信、NTT持株、KDDI研究所、NECビッグローブ、富士通、インターネットマルチフィード、NTTコムテクノロジー

5

ボット(BOT)

◆PCの遠隔操作・悪用を目的に作られたコンピュータウイルスの一種

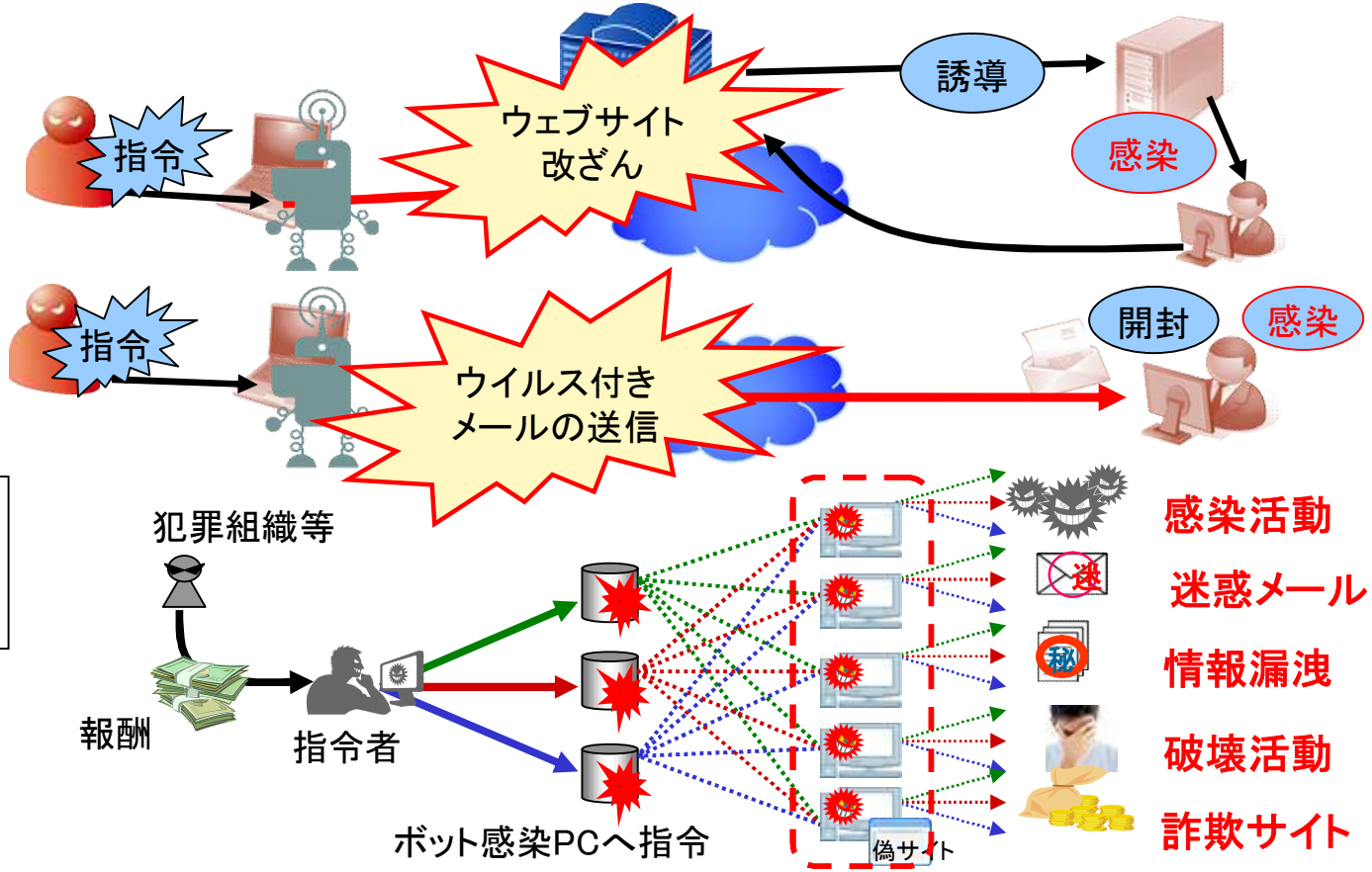
（感染したパソコンに目立った症状がでないためユーザは感染に気付きにくい）

◆感染したPCは、迷惑メールの発信元となる等、各種サイバー脅威の源

◆国内感染率 はブロードバンド利用者のうち約1%(約30万)と推計

〈感染〉
・メールの添付ファイル
・改ざんされたウェブサイト

〈ボットの運用〉
・感染PCを遠隔操作
・各種サイバー脅威の源

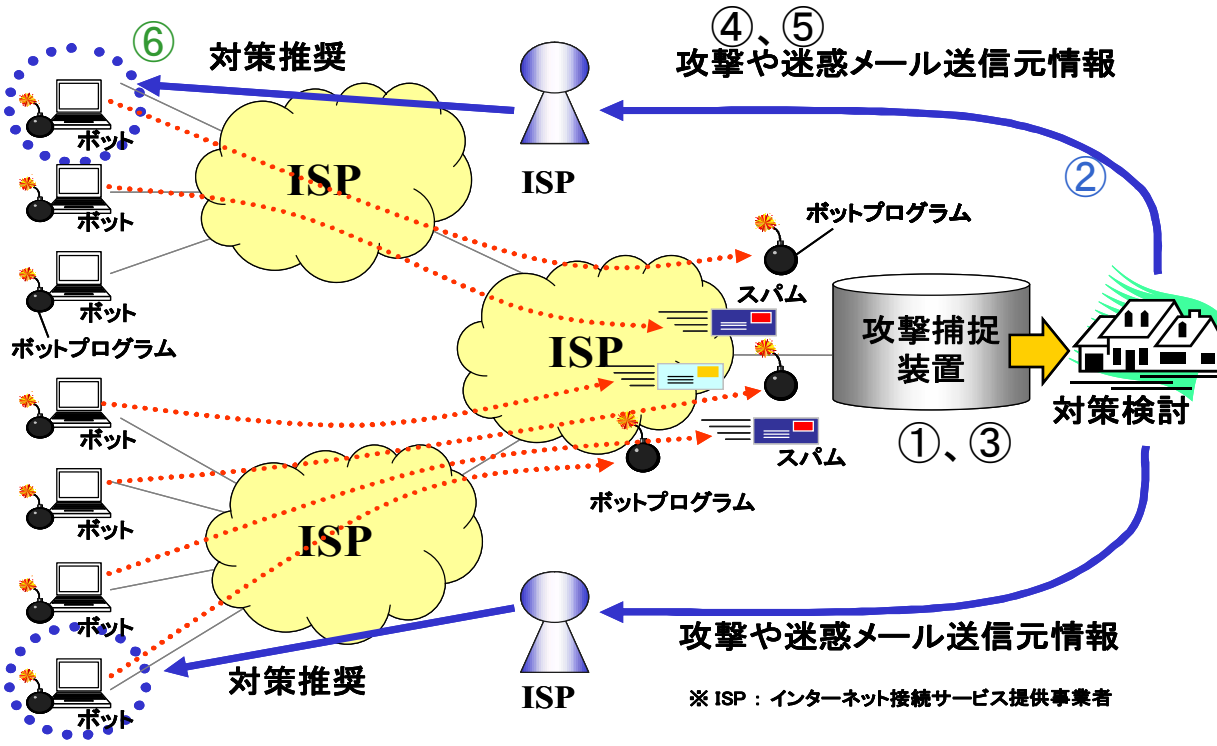


ボット対策プロジェクト（1）

2006-2010年度・総務省・経済産業省プロジェクト 〈サイバー・クリーン・センター〉

◆ハニーポット（おとりPC）を設置して、国内の感染ユーザーを探索

◆プロジェクト協力ISPが感染ユーザーを特定して、駆除を依頼



① 多数のIPアドレスを持つ「Honey Pot（おとりPC）」で感染拡大中ボットプログラムを捕捉

② 捕捉したボットプログラムを解析。併せてボットプログラム駆除ソフトを作成

③ 解析結果を踏まえ、動的保存。新たに感染拡大中のボットプログラムを捕捉

④ ②の解析結果を踏まえ、ボット化したPCによる通信特性をISPに伝達

⑤ ④をもとに、ボット化したPCを検出

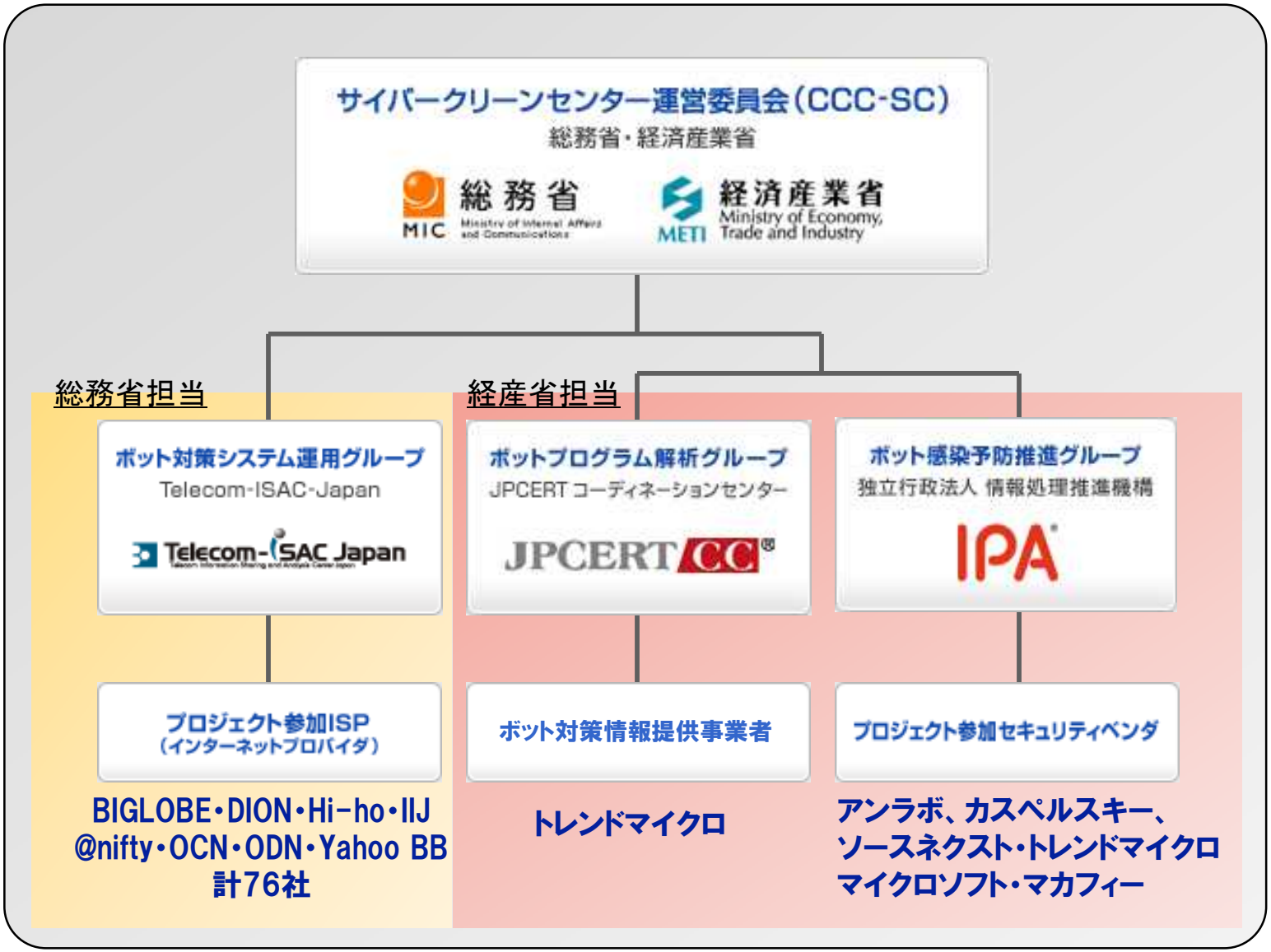
⑥ ボット化したPCの所有者（接続契約者）に対し、駆除ソフトの利用を推奨

⑦ ポータルサイトにて駆除ソフトを配布

※ なお、青字部分②は経済産業省にて、緑字部分⑥はISPにて実施

【予算額：2010年度・5.5億円】（総務省計上分）

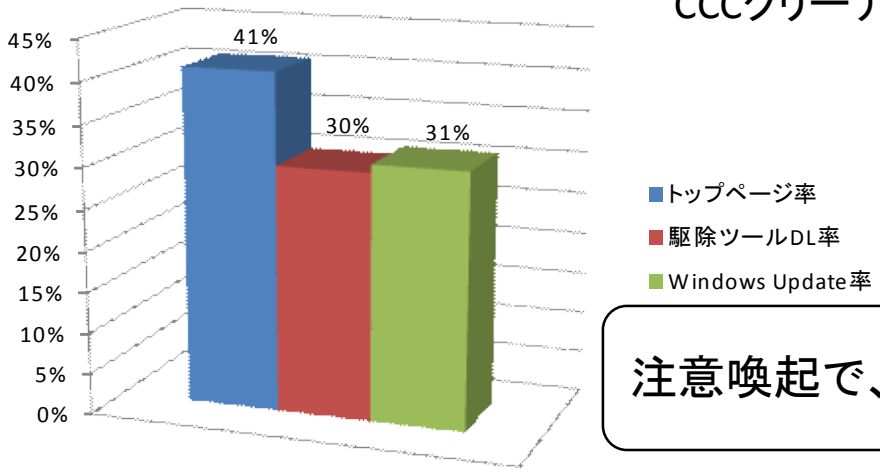
ボット対策プロジェクト（スパムメールやフィッシング等サイバー攻撃の停止に向けた試行）



ボット対策プロジェクト（2）

	2007年5月	2009年12月
注意喚起メール（当月）	22,674通	8,753通
注意喚起メール（累積）	54,209通	464,175通
CCCクリーナーDL率	29%（累積）	30%（累積）

CCCクリーナーをダウンロードする人は活動当初から30%前後で推移



注意喚起対応期間
（2007年2月～2009年12月）
注意喚起ユーザ数95,399

注意喚起で、トップページ訪問率は4割、駆除ツールDL率は3割

リテラシーを磨かずに
インターネットを利用して
いるユーザーが悪いのか？

・相談しても、たらいまわしにされる
・身近に正しい情報を与えてくれる人がいない

ユーザー
サポート面

・ネットワークが未完成であり、ある程度のレベルの品質を供給者側で維持する必要がある

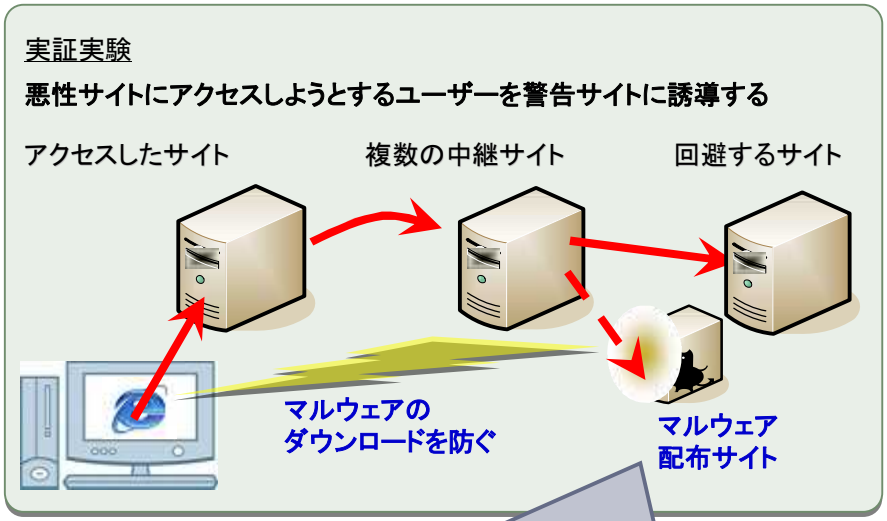
技術面

技術面からのアプローチ：悪性サイト回避システム

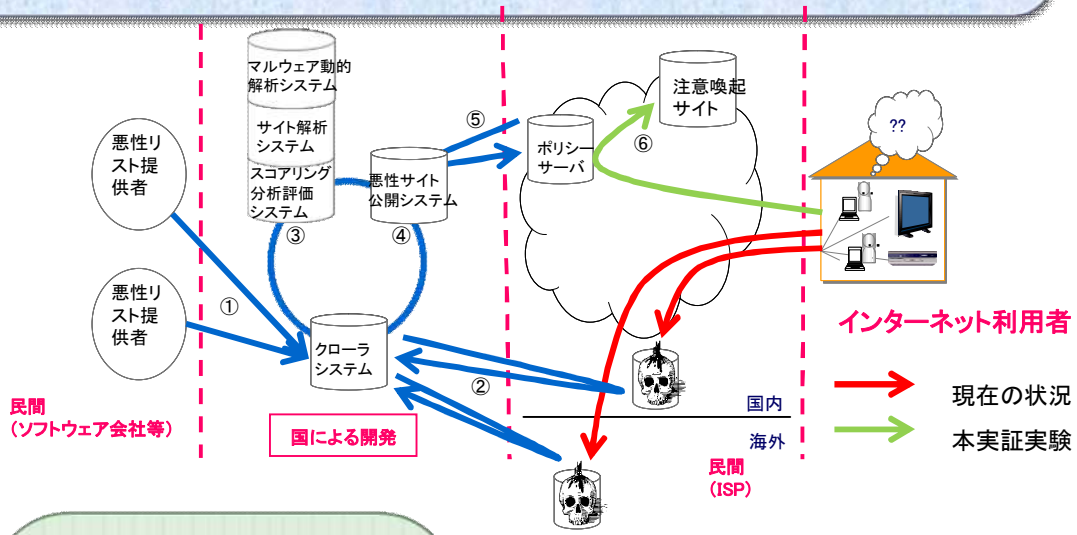
2009-2011年度・総務省プロジェクト〈悪性サイト回避システム実験〉

◆マルウェアを配布等する悪性サイトにアクセスしようとする利用者に警告

◆最新の悪性サイト情報等をISPが共有して、脅威に協働で対応



マルウェア配布サイトへの接続を遮断することで脅威に対処



・悪性サイトの調査技術の開発(最新状況の反映など)

・取得マルウェアの悪性レベルのスコアリング技術の開発

・悪性サイトの公開システムの構築と運用

・ISP等との連携による注意喚起の実施・悪性サイトを回避

本実証実験

① 悪性サイトのリストを収集

② ①の悪性サイトからマルウェアを収集

③ ②で収集したマルウェアの解析、サイト解析、悪性サイトのスコアリング分析評価

④ 悪性サイト情報をISPに公開する。

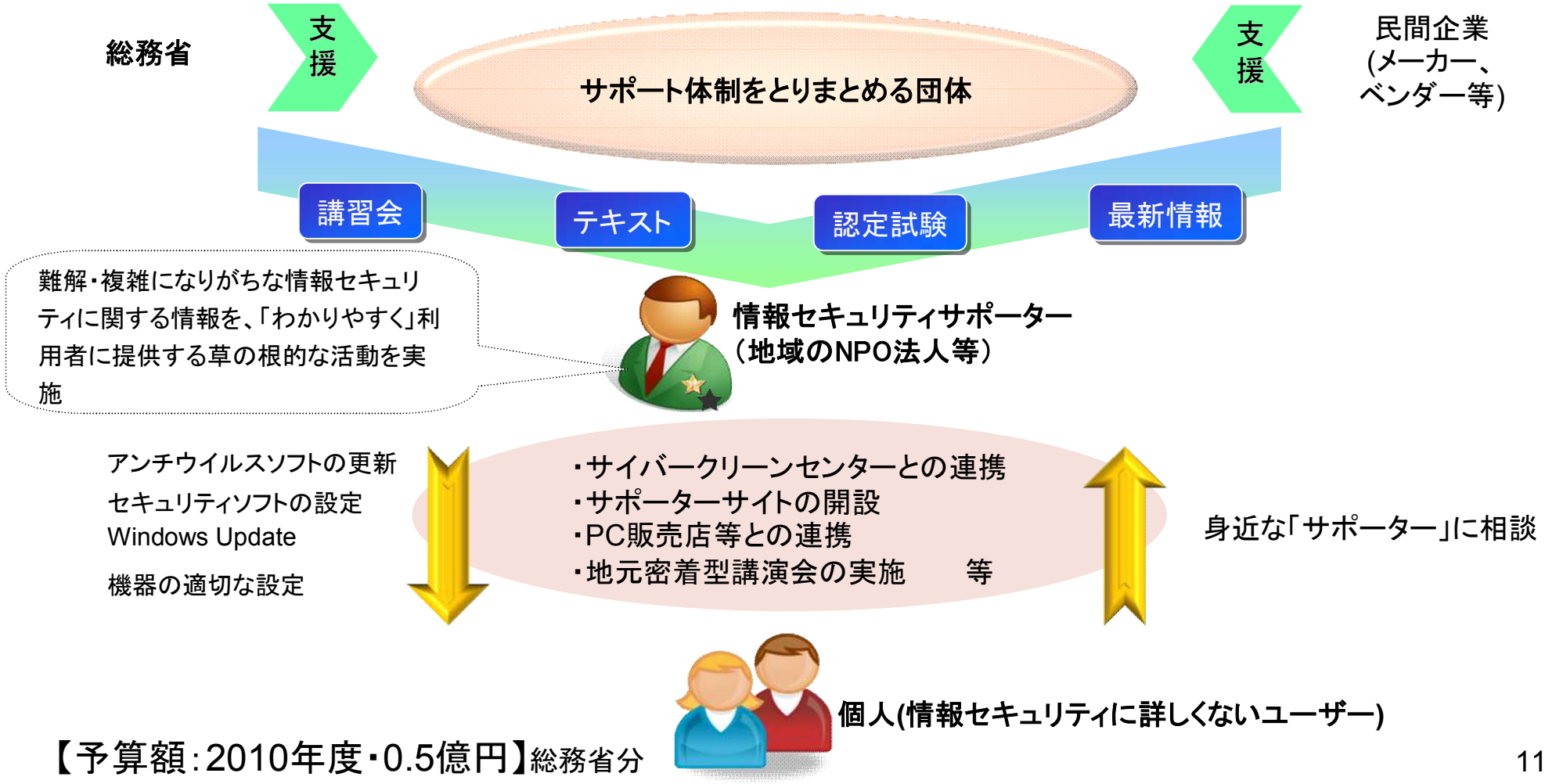
⑤ ④を元にポリシーサーバを作成。

⑥ ユーザが接続しようとしているサイトがマルウェア配布サイトであれば、注意喚起

【予算額：2010年度・2.2億円】

ユーザーサポート面からのアプローチ：地域活動を通じた個人のセキュリティ水準向上

2010-2012年度・総務省プロジェクト
◆地域NPO法人等と連携して、セキュリティ対策をサポートする人材の育成や体制整備を支援



【予算額：2010年度・0.5億円】総務省分

大規模仮想化サーバ環境における情報セキュリティ対策技術

○必要性

2010-2012年度・総務省プロジェクト〈情報セキュリティ対策技術〉

- 仮想化技術の活用により、サーバ環境の大規模化・集約化が進展
- 現状の仮想化技術導入はIT資産の効率的活用など「コスト重視」で「セキュリティ」は二の次

→ 大規模仮想化サーバ環境での漏洩事故等は、被害が深刻化・広大化

○各要素技術

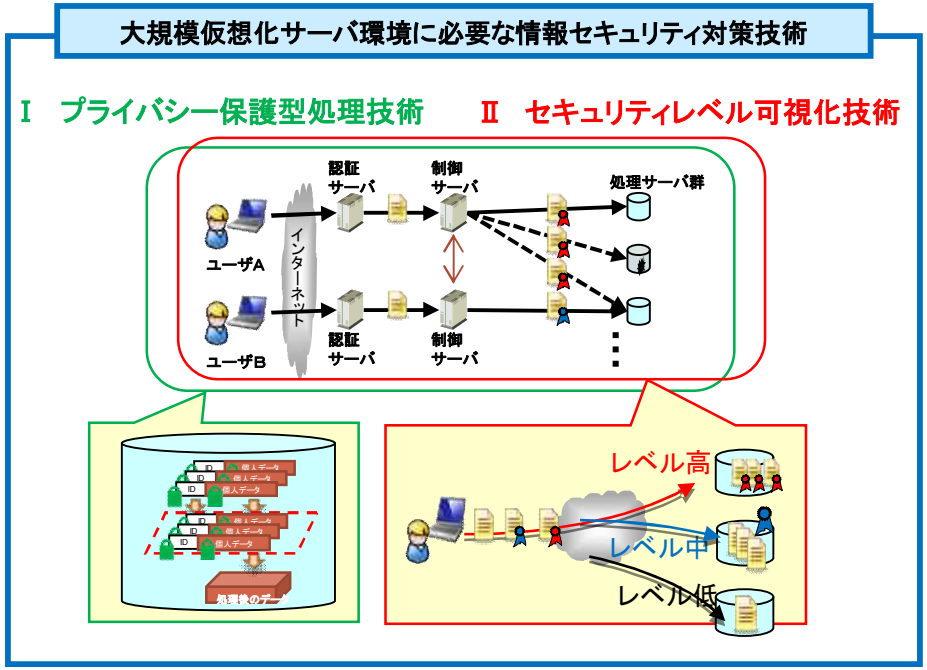
Ⅰ プライバシー保護型処理技術

仮想化サーバに保存された暗号化情報を開示することなく統計値等の計算処理を行う技術

Ⅱ セキュリティレベル可視化技術

サーバ利用者が仮想化サーバの情報セキュリティ対策状況を把握可能とする技術

【予算額：2010年度・5.2億円】総務省分



〈参考〉

経済産業省プロジェクト2010年度

次世代高信頼・省エネ型IT基盤技術開発・予算額8.6億円

→高い信頼・互換性を有するビジネス向け次世代IT基盤を構築するソフトウェア技術の開発・検証

税制（現行）・情報基盤強化税制

2008-2009年度（：2010年3月まで）
◆セキュリティが確保された情報システムを企業等が取得した場合に、その取得額の一部に対して税額控除又は特別償却を認める特別措置

対象者

青色申告を行う法人又は個人

対象設備

（1）サーバ用OS※1及びそれがインストールされたサーバ
（2）データベース管理ソフトウェア　※1及びこれと同時に設置されるアプリケーションソフトウェア
（3）ファイアウォール　※1（（1）、（2）、（4）のいずれかと同時に取得されるものに限る）
（4）連携ソフトウェア　※2

※1　ISO/IEC 15408に基づいて評価・認証されたもの。
※2　情報処理の促進に関する法律第3条第1項に規定する電子計算機利用高度化計画（平成20年経済産業省告示第61号）において定められたプログラムとして独立行政法人情報処理推進機構（IPA）により技術上の評価を受けたもの。

課税特例

取得価額の70%相当額の10%の税額控除又は50%の特別償却

取得価額要件

資本金	投資額（年間）
資本金１０億円超の法人	１億円以上、２００億円以内
資本金１億円超１０億円以下の法人	３，０００万円以上
資本金１億円以下の法人・個人	７０万円以上

減収額試算

減税額：約653億円（2009年度見込み）

税制(新規)・中小企業等基盤強化税制

2010年-2011年度
◆特別措置の**対象者を中小企業に限定**し、中小企業等基盤強化税制に位置付け
◆対象となる設備として「仮想化ソフトウェア」「ＩＤＳ/ＩＰＳ、ＷＡＦ」を追加

対象者

資本金1億円以下の中小企業者(大規模法人(資本金1億円超)子会社等を除く。)

対象設備

下線部が拡充項目

（１）①サーバ用ＯＳ※、②ＯＳがインストールされたサーバ、③仮想化ソフトウェア※
（２）①データベース管理ソフトウェア(DBMS) ※、② ①＋当該DBMS機能を利用するアプリケーションソフトウェア
（３）連携ソフトウェア※
（４）ファイアウォール※【（１）～（３）と同時設置】
（５）①ＩＤＳ／ＩＰＳ※、②ＷＡＦ※【（１）～（３）と同時設置】

※ISO/IEC 15408に基づいて評価・認証されたもの。

・IDS・・・Intrusion Detection System（侵入検知システム）
・IPS・・・Intrusion Prevention System（侵入防止システム）
・WAF・・・Web Application Firewall（webアプリケーションファイアウォール）

課税特例

取得価額の７％の税額控除又は３０％の特別償却

取得価額要件

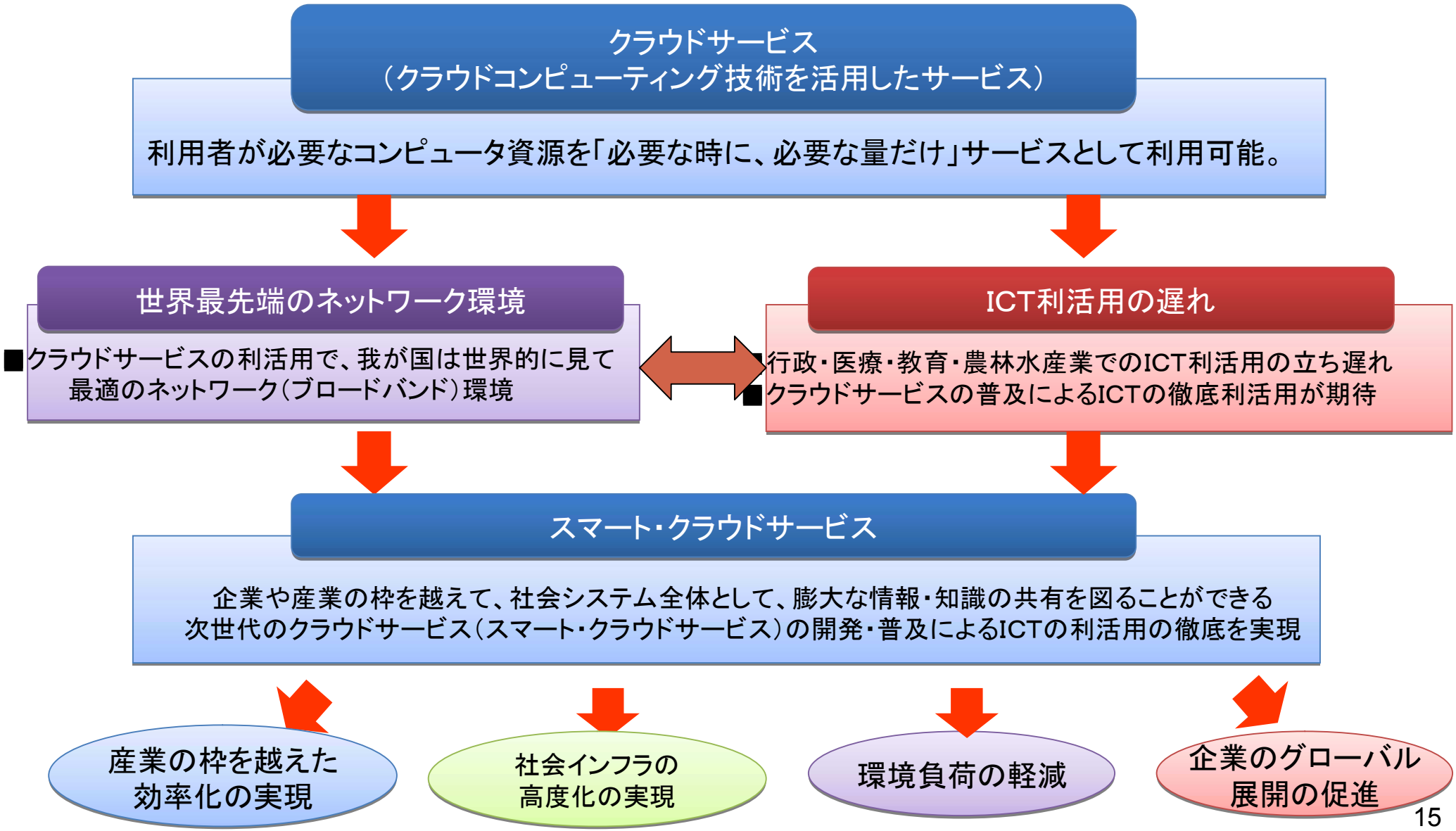
資本金	投資額
資本金１億円以下の中小企業者	７０万円以上（取得した対象設備の合算）

減収額試算

2010年度：約２４０億円　　セキュリティ関連（上記（4）(5)）は約２億円

クラウドサービスの普及・発展に向けて

2009年7月～「スマート・クラウド研究会」内藤総務副大臣主宰



「ASP・SaaSにおける情報セキュリティ対策ガイドライン」

ASP・SaaSの情報セキュリティ対策に関する問題意識

- ○ 多数を占める中小のASP・SaaS事業者においても、適切な情報セキュリティ対策が施されているのか
- ○ 多様な業界に多様なサービスを提供する中で、講じるべき情報セキュリティ対策の基準が不明瞭ではないか
- ○ 利用者に対して、必ずしも十分な説明や情報開示がなされていないのではないか　など

2007年6月：総務省「ASP・SaaSの情報セキュリティ対策に関する研究会」開催（～2008年1月）

2008年1月：ASP・SaaS事業者の実態に即した、情報セキュリティ対策ガイドラインを新たに策定

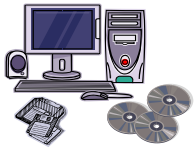
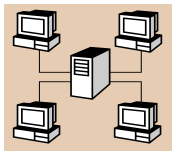
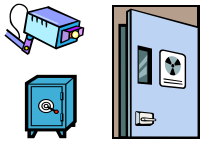
組織・運用面の対策

- ○ ASP・SaaS事業者内の運用管理体制の整備
  （情報資産管理、従業員管理等）
- ○ 外部関係組織との取り決め事項
- ○ ユーザーサポート責任　等



物理的・技術的対策

- ○ ASP・SaaSを構成するハードウェア及びソフトウェアの
  稼動監視・障害監視、ウィルス対策
- ○ 不正アクセス防止、データのバックアップ
- ○ 管理者権限割当ての制限、入退室管理　等

ASP・SaaS事業者向け医療分野ガイドライン

【関連する厚生労働省ガイドライン等】
「診療録等の保存を行う場所について」（平成14年3月29日、厚生労働省医政局長・厚生労働省保険局長通知、平成17年3月31日改正）
「医療情報システムの安全管理に関するガイドライン 第4版」（平成21年3月、厚生労働省） など

→ これまで医療情報の外部保存は例外的に可能（行政機関、危機管理目的など）

※ ASPIC： 特定非営利活動法人 ASP・SaaSインダストリ・コンソーシアム

2008年12月：総務省とASPIC(※)の「ASP・SaaS普及促進協議会」に「医療・福祉情報サービス展開委員会」設立

（厚生労働省も同委員会にオブザーバー参加）

2009年 7月：総務省「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」

医療情報の安全管理に関するガイドライン概要

第1章 本ガイドラインの前提条件及び読み方
目的、対象範囲、前提事項、用語の定義など

第2章 ASP・SaaS事業者が医療情報の処理を行なう際の責任等
医療機関等の責任、ASP・SaaS事業者の責任と役割の分担、第三者認証の取得、など

第3章 ASP・SaaS事業者に対する安全管理上の要求事項
組織的対策、技術的対策、人的対策、情報の破棄に係る対策、情報システムの改造、など

第4章 安全管理の実施における医療機関等との合意形成の考え方
契約、SLA等の合意文書の位置付け、組織体制・運用管理に関する合意項目、など

総務省予算プロジェクト
「ユビキタス特区」における取組み

〈2009年度補正予算〉
ASPICが、ASP・SaaSによる地域医療連携のための実証実験を、「長崎地域医療連携ネットワークシステム協議会」の協力で実施中

実証場所： 長崎県長崎市及び大村市
実証項目： ・左記ガイドラインに従い、安全管理上、確保すべきサービスレベルを整理
・外部保存に必要な保存性確保に関するサービスレベルも実証

2009年11月・厚生労働省「医療情報ネットワーク基盤検討会」で「診療録の保存を行う場所に関する提言」

2010年 2月・★外部保存拡大★：厚生労働省通知「診療録等の保存を行なう場所について」改正

（「民間事業者等との契約に基づいて確保した安全な場所」を追加）

「スマート・クラウド研究会」中間とりまとめ 2010年2月

クラウドサービスの普及に向けた基本3原則

① まずは多様なクラウドサービスの利活用を促進する
② 技術開発は、利用者ニーズを踏まえて、イノベーションを生み出す戦略的な取組を推進
③ 政府は、「環境整備」、「公的支援」、「調達主体」の3つの観点から公的役割を果たす

●電子行政クラウドの実現

✔“行政サービスの「見える化」”、“国民に開かれた「オープンガバメント」の推進”、“無駄を排除した「行政刷新」”の実現
✔「霞が関クラウド」「自治体クラウド」の推進と各府省BPRの徹底
✔政府・自治体がクラウドサービスを調達する際の「クラウドサービス調達指針（仮称）」の策定検討

（参考）米国オバマ政権は、行政の透明性向上を目的とする“Open Government Initiative”を推進中。

●医療、教育、農林水産業等におけるICT利活用の徹底

✔医療クラウド：集約された医療情報を基にした新薬・新治療法の開発、緊急医療体制や医療トリアージへの活用
✔教育クラウド：協働教育を実現するための効果的な教育手法の開発、デジタル教材等の全国提供、校務負担の軽減
✔農業クラウド：高齢化する農業従事者のノウハウの蓄積・活用、田畑等のデータの蓄積・活用、市場開拓への活用
✔コミュニティクラウド：地域「つながり力」による活性化、自治体の広域連携「ふるさとクラウドセンタ（仮称）」の構築支援

●スマート・クラウド基盤による社会インフラの構築

✔情報流、物流、金融流、エネルギー流を最適制御するスマート・クラウド基盤の構築支援
☞スマートグリッド、次世代ITS、広域センサネットワーク、橋梁管理など、クラウドサービスを活用したインフラ運用の高度化を社会プロジェクトとして推進

「スマート・クラウド研究会」中間とりまとめ 2010年2月

今後の主な課題として。。。

◆次世代クラウド技術の在り方

✔安全性・信頼性の向上を実現する技術

☞過負荷に対応するリソース融通の仕組み作り、暗号化技術や仮想化技術のセキュリティ向上、など

✔環境負荷の軽減に貢献する技術

☞ITU（国際電気通信連合）で進められているICTによるCO_2排出量削減効果の計測手法の確立に貢献、など

→ これらを実現するための技術開発ロードマップの明確化、ベンチャー企業等を対象とする競争的資金制度など

◆クラウド技術の標準化・共通化等

✔利用者の視点に立って、最低限の標準化・共通化が望ましい点

☞SLA（サービス品質保証契約）の在り方、セキュリティ基準の標準化、クラウド間の相互運用性の確保等を検討

→ これらについて、様々なクラウドサービス関連の標準化団体が存在することから、活動への貢献を図る

◆クラウドサービスに関する国際的コンセンサス作り

✔クラウドサービスを利用する際、利用者の居住する国とデータセンタが所在する国との間の裁判管轄権、個人情報保護法、知的財産権や著作権の保護等について、APEC、OECD等の国際的な場において検討が必要

✔クラウドサービスの普及がネット中立性（オープンインターネット）に与える影響について、国際的なコンセンサス作りを進めることが必要

国際連携・協調

【ITU（国際電気通信連合）】

国際連合の専門機関として191ヶ国が加盟

◆政府首脳が集うWSIS（世界情報社会サミット：2005年）の行動計画 に、世界戦略の策定、国際標準化、途上国への技術支援等の観点から、サイバーセキュリティに関する取組を推進

◆ 2006年「法制度」「技術」「組織構築」「能力向上」「国際協力」の5つを取組の柱とする世界的な戦略フレームワーク ”GCA（グローバル サイバーセキュリティ アジェンダ）”レポートを作成

【APEC（アジア・太平洋経済協力）】

アジア太平洋地域21ヶ国が加盟

◆ TEL（電気通信作業部会）に、SPSG（セキュリティ分科会）が設けられており、国際的なセキュリティ問題に関する情報交換や国際連携・協力に向けた議論を実施

◆これまで、スパム、ボット及びマルウェアなど主要なセキュリティ脅威への対処方策に関するプロジェクトを実施し、その成果は基本原則やガイドラインとして、まとめられている

【OECD（経済協力開発機構）】

欧米等の先進国30ヶ国が加盟

◆通信政策委員会に、ISP（セキュリティ・プライバシー作業部会）が設けられており、NGNセキュリティ、暗号、デジタルID管理、プライバシーの越境執行協力などに関し、政策提言や分析レポートが作成されており、加盟国の情報セキュリティ分野の政策形成に影響を与えている

クラウドに関する国際的な議論

米国（連邦取引委員会FTC）がOECD等と国際会議を共催　2009年3月16-17日　ワシントンDC

「国際データ・セキュリティ会議～グローバル経済における個人情報保護～」

→　データ・セキュリティと法制度、ビジネスの実態、漏洩等対処のベストプラクティス、など

OECD通信政策委員会（ICCP）での議論　2009年10月14日　OECDパリ本部

「クラウド・コンピューティングに関するフォーラム」

◆国境を越えるデータの流れに伴う諸課題

→　個人情報保護、企業コンプライアンスとの兼ね合い、など

◆寡占事業者による囲い込みの懸念

→　標準化、共通化、相互接続性の保証などの検討、など

◆「クラウド」が与える影響の評価

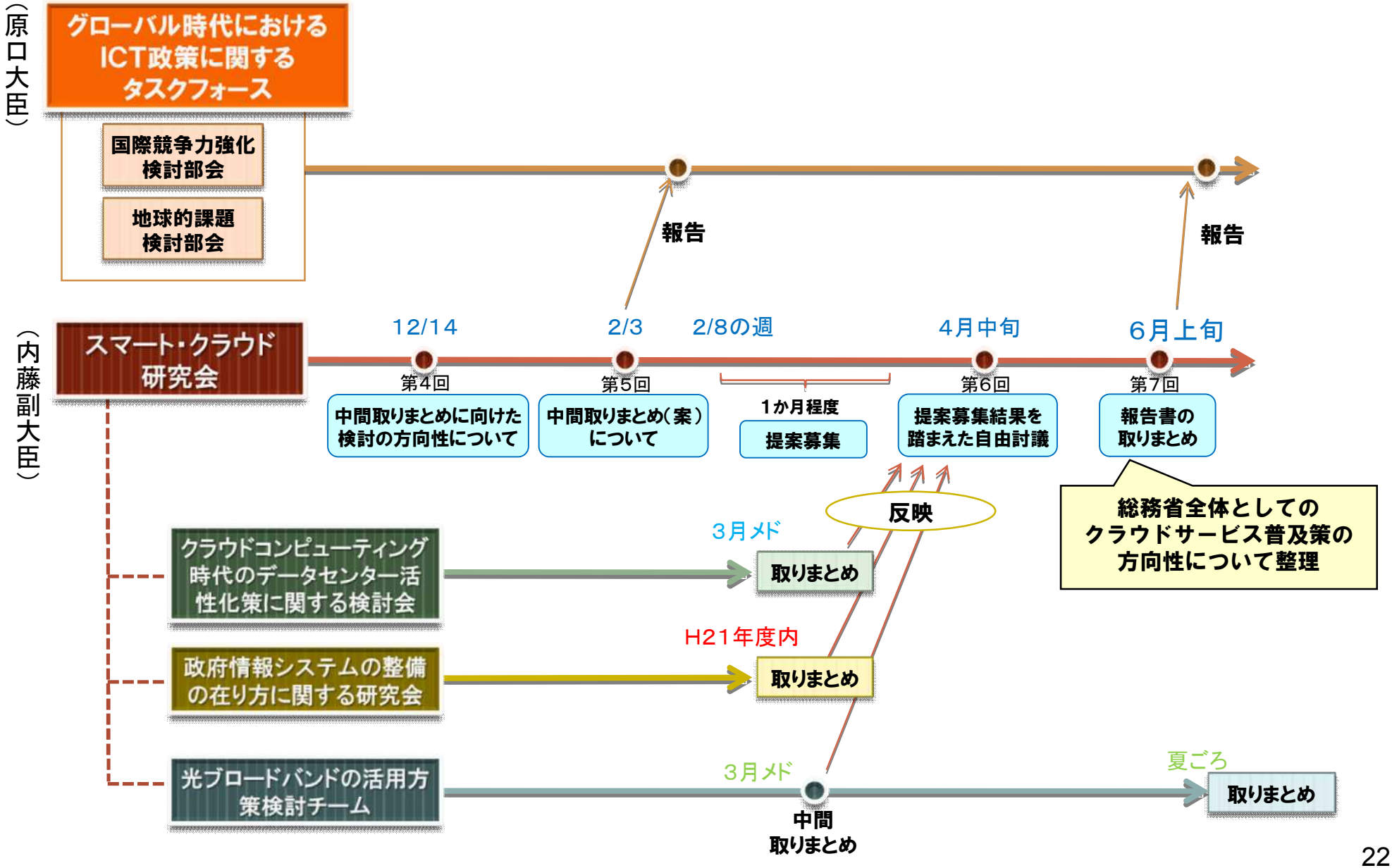
→　インフラへの負荷、経済的メリットの評価手法、環境への影響、など

EU（欧州連合）が研究会報告書を取りまとめ　2010年1月27日　ブリュッセル

「クラウド・コンピューティングの将来～欧州にとっての好機～」

→　研究開発の支援、法制度上の課題の検討、環境への影響等の見極め、など

総務省ICT分野の研究会等スケジュール（見込み）



諸外国における情報通信戦略の動き

アメリカ

■**オバマ新政権**は、**“技術・イノベーション戦略”**を主要施策の一つと位置付け。

（施策例） ○ 全ての学校、図書館、病院、家庭を世界で最も進んだ通信インフラに接続
○ 電子政府実現に向け、連邦政府全体を統括するCTO（Chief Technology Officer）を指名
○ 情報技術を活用した医療制度のコスト削減

【出典】オバマ候補政策 Technology and Innovation (2007年11月)

Barack Obama 米国大統領

“我々は新しい雇用創出だけでなく、成長のため新しい基盤を作らなければならない。我々は道路や橋、電線やデジタル通信網（digital lines）を作り、ビジネスを支え、我々の結びつきを強めなければならない。我々は科学を立て直し、技術を活用し医療の質の向上と共にコストを下げる。（中略）我々の学校や大学を新たな時代の要請にあわせるようにする。”（09年1月20日就任演説）

イギリス

■英国は、09年6月、**ICT分野の新行動計画”デジタル・ブリテン“**の最終報告書を公表。

■デジタル産業の成長を加速し、イノベーション・投資・品質における世界のリーダーとしての地位を高めるための計画。主に、情報通信インフラの整備、国民のデジタル参加の推進、デジタル・コンテンツについて記載。

Peter Mandelson ビジネス・企業・規制改革大臣のステートメント

“英国が通信・デジタル技術分野で世界のリーダーとしての地歩を固めることを政府として決定した。現在の金融・銀行危機に対し、 英国が最悪期を切りぬけ、上方転換に備えるため、デジタル・エコノミーはその中心に位置するものだ。”

フランス

■フランスは、08年10月、**包括的なデジタル国家戦略“デジタルフランス2012”**を発表。

■“2012年までにGDPに占めるICTのシェアを6%から12%へ倍増させる”（ベッソン・デジタル経済相（当時））ことを目標。

（注）全国民をブロードバンドネットワークに接続可能とする、デジタルコンテンツ制作へのテコ入れなど、計154項目の施策を盛り込む。

韓　国

■韓国は、08年7月、イ・ミョンバク政権の**情報通信産業政策となる“ニューIT戦略”**を発表。

■08年12月に、08～12年（5年間）の**「国家情報化基本計画」**を策定し、「創意と信頼の先進知識情報社会」を目指して、ICT産業生産額を267.6兆₩（2007年）から2012年に386兆₩に拡大するなど、5大目標（2大エンジン、3大分野）を設定。これを受け、09年4月に、20の議題に205の課題と期待効果を盛り込んだ**「国家情報化実行計画」**を発表。