NISC National Information Security Center

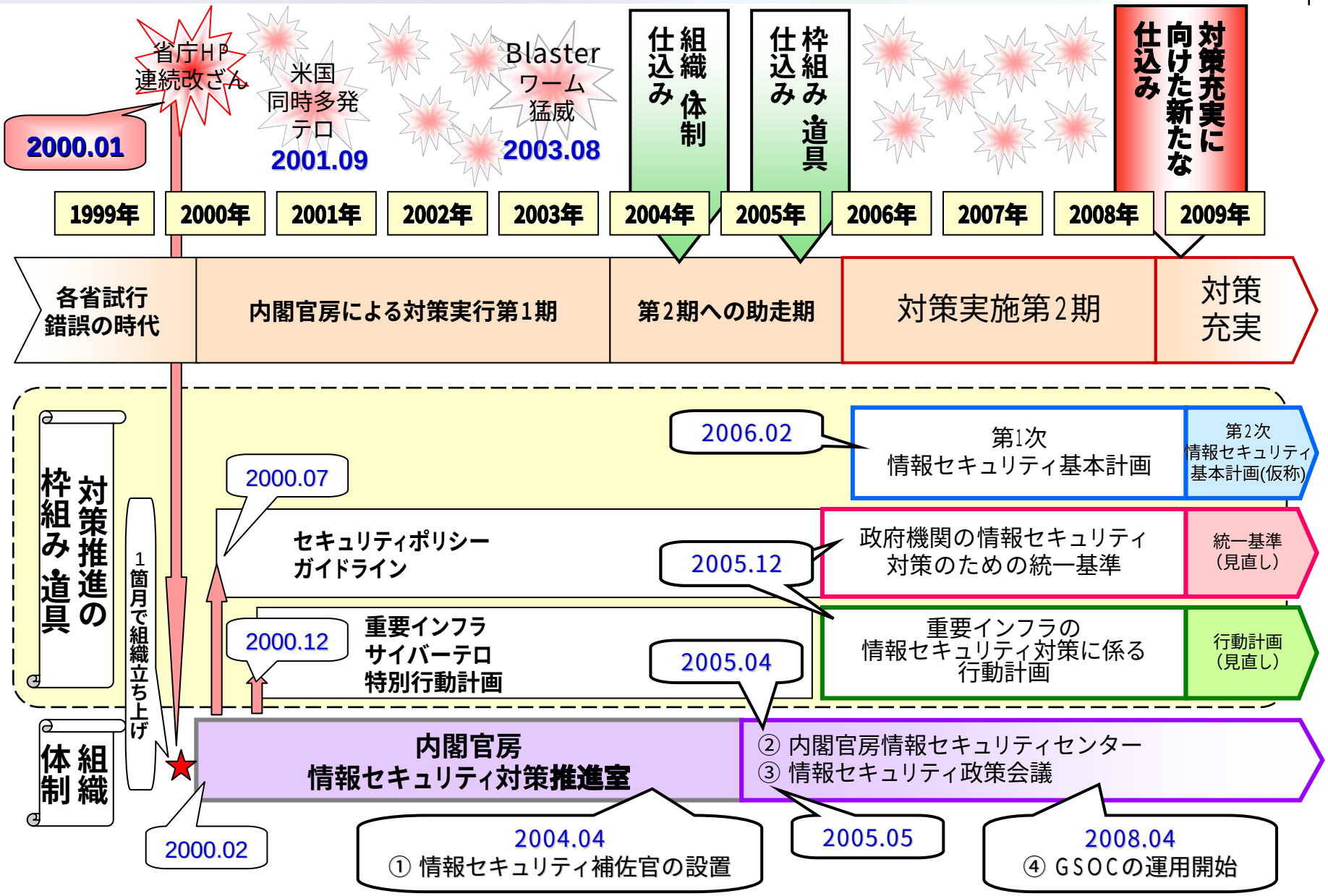
我が国の情報セキュリティ政策の概要とグランドチャレンジ検討WG設置の背景

2008年8月

内閣官房情報セキュリティセンター（NISC）
http://www.nisc.go.jp/

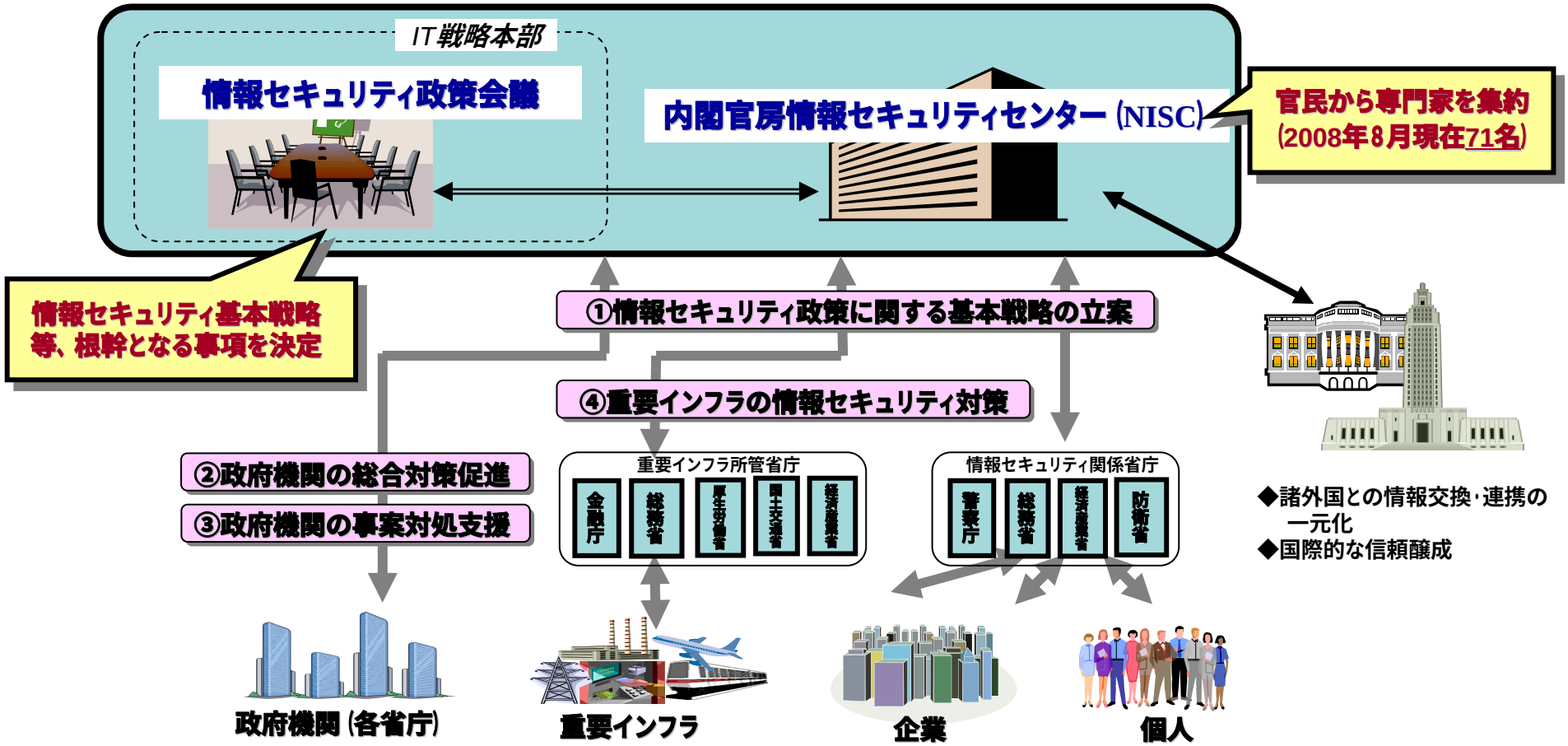
資料4

内閣官房における情報セキュリティ政策の流れ（２０００年以降の概要）



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）の設置

- 「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を強化
  - 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」を設置



情報セキュリティ政策会議の構成

議長

内閣官房長官

議長代理

内閣府特命担当大臣（科学技術政策）

構成員

国家公安委員会委員長
総務大臣
経済産業大臣
防衛大臣

江畑 謙介	拓殖大学客員教授／軍事評論家
小野寺 正	ＫＤＤＩ株式会社代表取締役社長
黒川 博昭	富士通株式会社代表取締役社長
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	首都大学東京教授
村井 純	慶應義塾大学教授

このほかの国務大臣も必要に応じ会議に出席し意見を述べることができる

情報セキュリティ政策の構造及び概要

「第1次情報セキュリティ基本計画」（2006年2月2日 情報セキュリティ政策会議決定）

2006～2008年度の3ヵ年計画。全主体が適切な役割分担を果たす「新しい官民連携モデル」の構築を目指している。

	政府機関・地方公共団体	重要インフラ	企　業	個　人
3カ年の目標	すべての政府機関が「政府機関統一基準」が求める水準に	IT障害を限りなくゼロに	対策の実施状況を世界トップクラスの水準に	「IT利用に不安を感じる」個人を限りなくゼロに
各実施領域の重要政策	◆ 政府機関統一基準に基づく各省庁の評価 ◆ サイバー攻撃等への緊急対応能力の強化	◆ 重要インフラ行動計画 ・安全基準等の整備の推進 ・情報共有体制の強化 ・相互依存性解析 ・分野横断的演習実施	◆ 第三者評価制度の活用 ◆ ウィルス等への体制強化	◆ セキュリティ教育の推進 ◆ 広報啓発の強化 ◆ ユーザーフレンドリーなサービスの提供等

横断的な重要政策

- 情報セキュリティ技術戦略の推進
- 情報セキュリティ人材の育成確保
- 国際連携・協調の推進
- 犯罪の取締り、権利利益の保護救済

→ 第2次情報セキュリティ基本計画

2005年度 | 2006年度 | 2007年度 | 2008年度 | 2009年度

評価2006 → セキュア・ジャパン2006
評価2007 → セキュア・ジャパン2007
評価2008 → セキュア・ジャパン2008
セキュア・ジャパン2009

「セキュア・ジャパン」：基本計画の遂行を確実にするため、毎年の政府の重点施策をまとめた年度計画

内閣官房情報セキュリティセンター（NISC）の機能・体制

センター長（安全保障・危機管理担当副長官補）

副センター長（内閣審議官）

情報セキュリティ補佐官（２名）

山口　英（奈良先端大教授）
篠田陽一（北陸先端大教授）

副センター長（内閣審議官）

職員数約７０名

基本戦略立案

●全体戦略（「情報セキュリティ基本計画」）策定
●研究開発・技術開発戦略の立案
●情報共有・対策その他の官民連携の推進　等

政府機関総合対策促進

●政府統一的な「対策基準」の策定
●政府統一的な情報セキュリティ対策の「評価」　等

事案対処支援

●早期警戒情報の収集・分析機能の強化
●情報セキュリティ関係機関との連携強化　等

重要インフラ対策

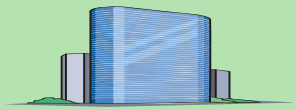
●相互依存性の分析
●横断的な対策基準の策定
●総合的演習の実施　等

国際戦略

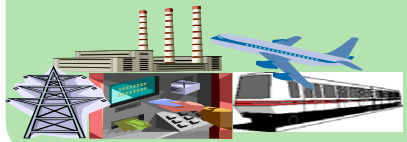
●情報セキュリティに関する我が国の国際戦略の立案
●諸外国の関係機関等との緊密な連携　等

企業　個人

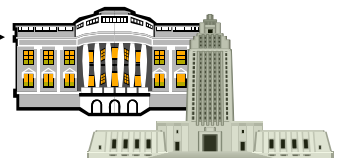
各政府組織



重要インフラ



諸外国関係機関



技術戦略専門委員会の位置づけと
これまでの技術戦略専門委員会報告書の内容

技術戦略専門委員会の位置づけ

- **情報セキュリティに係る研究開発・技術開発、その利用戦略について調査検討を行い、情報セキュリティ政策会議や総合科学技術会議情報通信PT等に対して、「技術戦略専門委員会報告書」としての提言を行う。**
- **情報セキュリティの確保において、継続的な技術開発と、その社会展開を円滑に行い、成果をすべての主体が享受できる環境作りが必要であり、喫緊の課題を解決するための技術開発と、中長期的な視点に立った研究投資開発の戦略設定が求められているとの認識に基づき、調査研究を行う。**

過去の技術戦略専門委員会報告書の概要

○ 報告書2005(2005年11月17日発表)

1. 報告書2005の位置づけ～第一次基本計画に向けた報告書
2. 報告書2005における技術戦略を考える上での基本的な考え方
   - ・我が国における情報セキュリティ上の問題点の全体の俯瞰
   - ・情報セキュリティ技術の役割と今後の方向性を検討
   - ・情報セキュリティ技術を支える環境整備の必要性
3. 情報セキュリティ技術の研究開発・技術開発を推進するための新しい構造のあり方について
4. 情報セキュリティ技術開発の重点化と環境整備のあり方
5. 「グランドチャレンジ型」研究開発・技術開発の推進

○ 報告書2006(2007年6月29日発表)

1. 情報セキュリティ技術の現状認識と今後の方向性
   - ・情報セキュリティ技術戦略の基本
   - ・情報セキュリティ技術の研究開発・技術開発を推進するための新しい構造のあり方
   - ・情報セキュリティ技術開発の重点化と環境整備のあり方
2. 2007年における実施のポイント
   - ・投資領域設定の継続的見直し構造の実現
   - ・調達を通して成果を活用するガイドライン策定の検討
   - ・「グランドチャレンジ型」テーマ検討の場

情報セキュリティ分野におけるグランドチャレンジ型研究開発･技術開発とは

第３期科学技術基本計画（２００６年）

理念１　人類の英知を生む
知の創造と活用により世界に貢献できる国の実現に向けて

理念２　国力の源泉を創る
国際競争力があり持続的発展ができる国の実現に向けて

理念３　健康と安全を守る
安心・安全で質の高い生活のできる国の実現に向けて

※優先的に資源配分がなされる「重点推進4分野」：
ライフサイエンス、情報通信、環境、ナノテク・材料

「ITを安心して利用可能な環境」の構築
第１次情報セキュリティ基本計画

情報セキュリティ技術に係る研究開発の必要性

IT基本法等を踏まえて策定された第1次情報セキュリティ基本計画において「ITを安心して利用可能な環境」の構築が求められている。また、科学技術基本計画には安心・安全で質の高い生活のできる国の実現が基本理念として謳われている。これらの計画・理念等の実現のためには情報セキュリティに係る研究開発の実施が不可欠。

課題

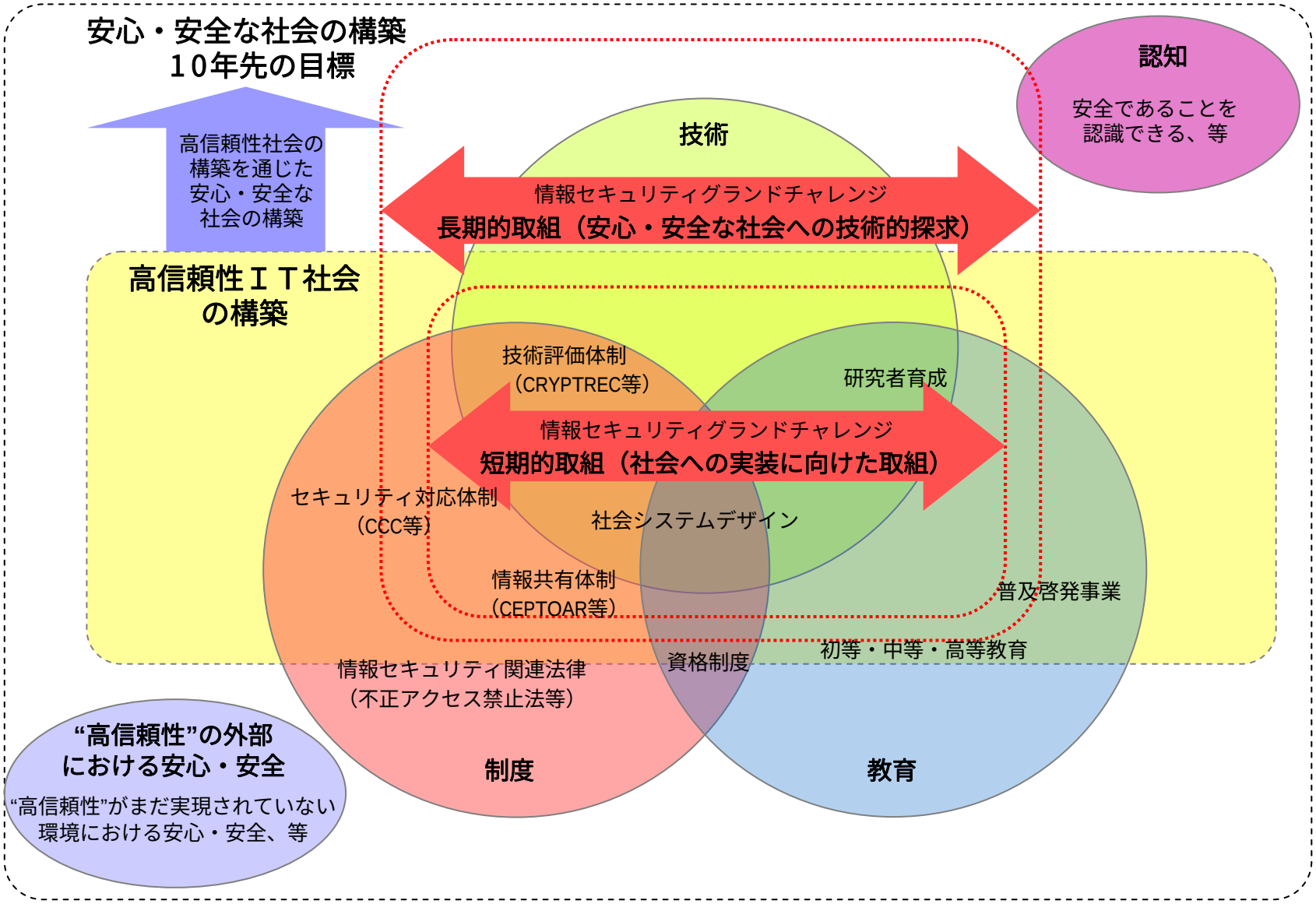
急速に拡大するＩＴ利用・活用に、情報セキュリティ技術の開発が対応できていない

既存の情報セキュリティ技術の限界を補完する組織・人間系の管理手法とのバランスを欠いている

「グランドチャレンジ型」研究開発・技術開発の必要性

情報セキュリティ対策においては、対症療法的な対応だけでなく、中長期的な視野に立った研究開発等が重要である。したがって、情報セキュリティ技術の研究開発・技術開発においても、短期的な問題解決はもとより、長期的な視野で抜本的な技術革新等の実現を目指す「グランドチャレンジ型」の研究開発・技術開発が必要

グランドチャレンジ型研究開発・技術開発の位置づけ



グランドチャレンジ検討WG設置に至る経緯の概要

平成17年（2005年）

技術戦略専門委員会 報告書2005

- 「グランドチャレンジ型」研究開発・技術開発が初出
- 第1次情報セキュリティ基本計画へのインプット

第1次情報セキュリティ基本計画

- 情報セキュリティ技術戦略の項で「グランドチャレンジ型」研究開発・技術開発の推進が謳われる

平成18年（2006）年

技術戦略専門委員会 報告書2006

- 「グランドチャレンジ型」研究開発・技術開発が報告書の項目として引き継がれる

平成19年（2007年）

関係者によるグランドチャレンジ検討（計3回）

- 関係者による検討を計三回実施
- 技術戦略専門委員会報告書（第1次案）（別添）として取りまとめ

平成20年（2008年）

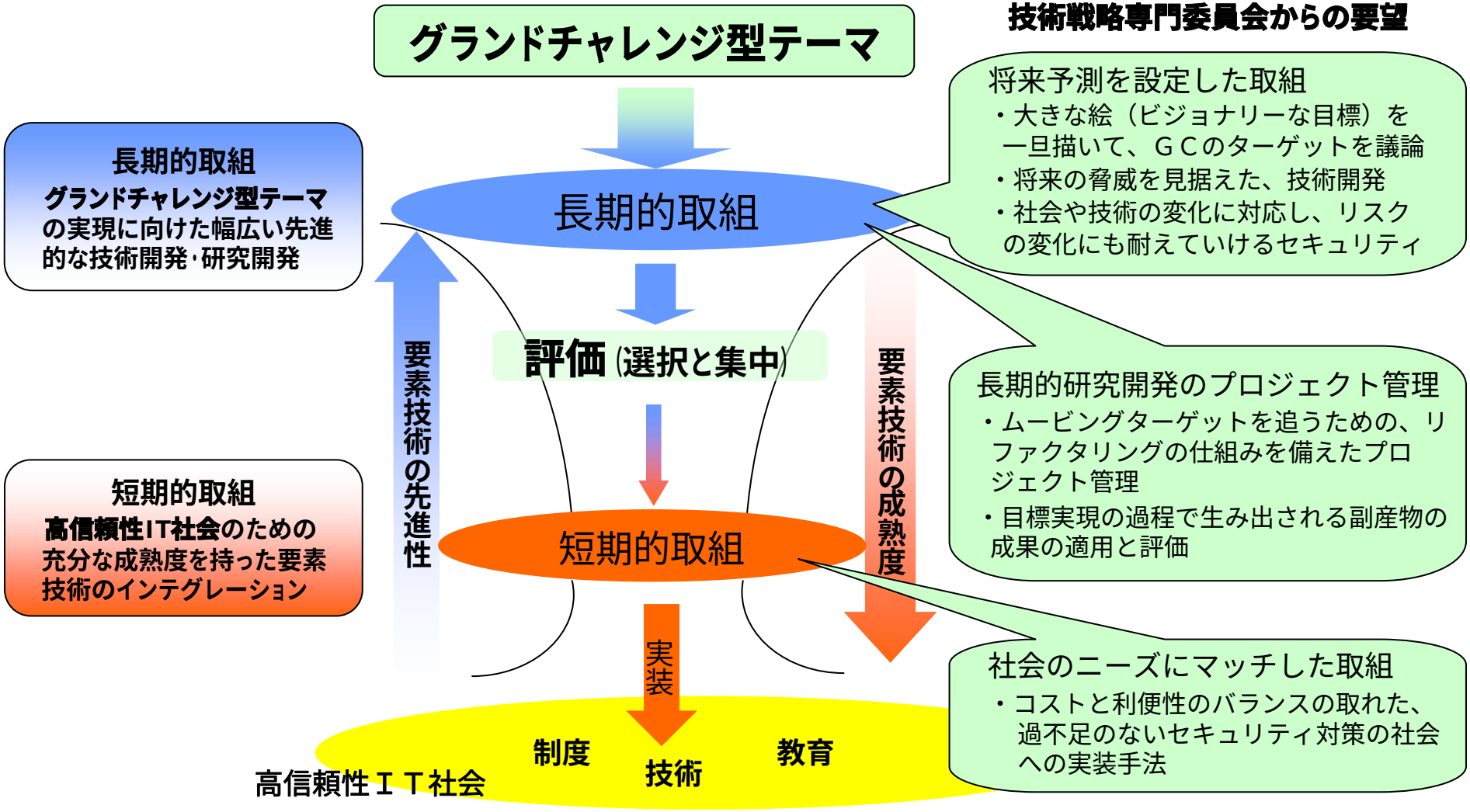
第10回 技術戦略専門委員会

- グランドチャレンジ検討WGの設置を決定

【参考：今後の予定】
- WGの報告書をもとに、技術戦略専門委員会が技術戦略専門委員会報告書2008を作成
- 技術戦略専門委員会報告書2008に記載される内容をもとに、総合科学技術会議情報通信PTや第2次情報セキュリティ基本計画へインプットを行う予定

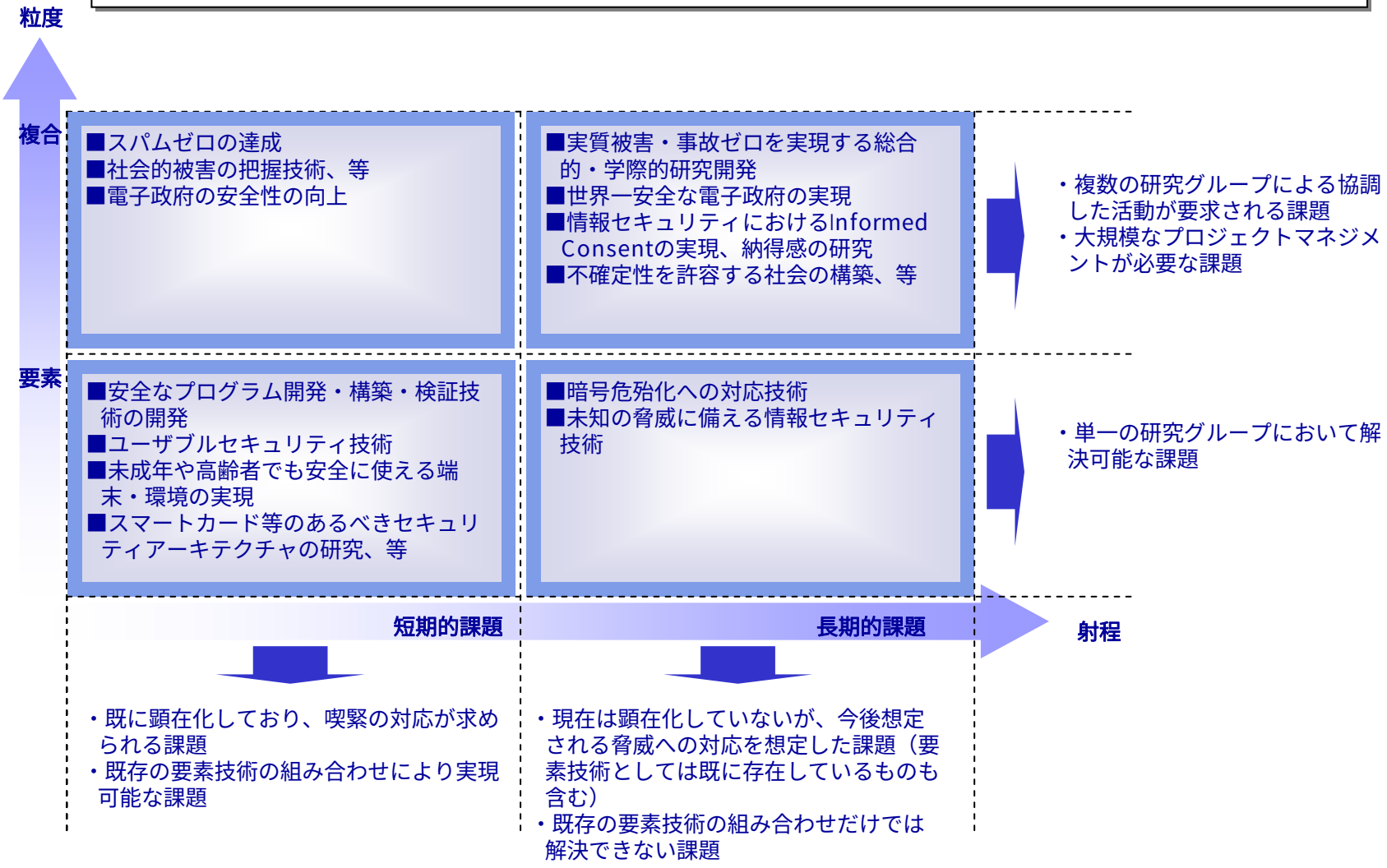
グランドチャレンジ検討WGの設置について

各分野の専門家からなるWGを設置し、グランドチャレンジを実現するための ロードマップの検討を行う



技術戦略専門委員会報告書（第1次案）概要（1）
長期的取組（安心・安全な社会への技術的探求）

■グランドチャレンジ型研究開発テーマについて、研究開発の射程（短期・長期）、粒度（複合・要素）の２軸、計４象限で整理
■検討されたテーマについて、それぞれの特性を踏まえ４象限に分類



技術戦略専門委員会報告書（第1次案）概要（2）
短期的取組（社会への実装に向けた取組）

情報セキュリティリスクの評価・分析技術

（1） 背景と目的：
- 情報セキュリティ対策の基本はリスク分析であるにもかかわらず、リスク分析が正しく行われていることは少ない。
- 複合的なコンポーネントから構成される情報システムのリスク分析技術は確立されていない。
- また、定量的リスク分析に必要なデータの蓄積がない。

（2）期待される効果：
- 人間系も含めた情報システムの信頼性向上。

（3）概要：
- 小規模なシステム（組込システム等）から大規模システム情報システム（重要インフラの業務システム等）に対応できる、リスク分析技術。
- 情報システムを運用する人間系を含めたリスク分析技術。
- システム間、あるいは外部環境とシステムの相互依存性を加味したリスク分析技術。
- リスク分析に必要な基礎的データの収集と蓄積。
- 脆弱性の存在がシステムに与えるリスク量の算出技術。

情報セキュリティ実装工学

（1） 背景と目的：
- 情報セキュリティ関係の個々の要素については、これまで様々な研究が行われてきているところ。
- しかしながら、それら技術をシステムとして実装したり、社会に普及していく際に検討すべきことについては、十分に研究がなされていない。

（2）期待される効果：
- ソフトウエア脆弱性や暗号危殆化時における社会的コストの最小化。

（3）概要：
- 情報システムのライフサイクルを通じたセキュリティ確保・技術の体系的研究。
- 暗号危殆化時において、社会的影響を最小化するようなシステム構成技術。また、ユーザーへのデプロイ手法の研究。
- 稼動を停止できないシステム（原子力発電所の制御システム）等における脆弱性発生時の対処技術。

新たな情報システムアーキテクチャに対応した新しいセキュリティモデルの提示

（1） 背景と目的：
- 従来の情報システム構築技術は、信頼できるドメイン内に閉じたシステムを対象に研究されてきた。
- 今後普及が見込まれる、P2P、SaaS、グリッドなどの新しいシステムアーキテクチャに対応したセキュアなシステム構築技術について十分な研究がなされていない。

（2）期待される効果：
- 安全なインターネットサービスの提供。

（3）概要：
- 新しいシステムアーキテクチャに対応した脆弱性のモデル化、体系化の研究。
- 分散化、匿名化された情報の保護技術。
- 問題が発生したときの責任分界のあり方に関する研究。
- 事業継続性・可用性の確保技術。