報道発表

平成19年8月3日
内閣官房情報セキュリティセンター

第13回情報セキュリティ政策会議の開催について

－政府機関の情報セキュリティ対策の実施状況等－

1．第13回情報セキュリティ政策会議の報告及び討議事項

本日、「情報セキュリティ政策会議」（議長：内閣官房長官）の第13回会合が開催され、

(1) 内閣官房情報セキュリティセンター（NISC）のこれまでの取組み
(2) 「技術戦略専門委員会報告書2006」
(3) 政府機関の情報セキュリティマネジメントに関する評価結果
(4) 政府機関の情報セキュリティ対策の実施状況に関する重点検査及び評価結果
(5) 情報セキュリティ政策における「具体的目標」

について、報告がなされるとともに、

(6) 「我が国の情報セキュリティ分野における国際協調・貢献（国際戦略）（仮称）」

について、検討状況の報告がなされ、議論がなされました。

※本日の会議資料は、内閣官房情報セキュリティセンター（NISC）のホームページ（http://www.nisc.go.jp/conference/seisaku/index.html#seisaku13）において公表しています。

2．政府機関の情報セキュリティマネジメントに関する評価結果について

各府省庁における情報セキュリティマネジメントが確実かつ効果的に行われているかを調査したマネジメント評価では、政府機関の模範となる優れた取組みを44件選定し、そのうち5件を2006年度のベストプラクティスとして選定しました。

また、

○　各府省庁で情報セキュリティ対策を担当する職員（常任）の平均経験年数は1年～3年が中心であること

○　一般職員の情報セキュリティ教育受講率については、約6割の府省庁は受講率9割以上となっている一方、約4分の1の府省庁では受講率が4割に満たない

など、より組織的な教育の実施に向けた課題があること

○　半数近くの府省庁が障害等に備えた訓練等を行っていないこと

などが分かりました。詳細な内容については、別紙1をご参照ください。

3．政府機関の情報セキュリティ対策の実施状況に関する重点検査及び評価結果について

重点検査では、昨年に引き続き、各府省庁の端末及びウェブサーバに関する対策実施状況について定量的な評価を行いました。その結果、昨年と比較して大幅な改善がみられ、各府省庁における情報セキュリティ対策が着実に向上していると認められました。詳細な内容については、別紙2をご参照ください。

4．情報セキュリティ政策における「具体的目標」について

本日報告された、「情報セキュリティ政策における「具体的目標」」については、情報セキュリティ政策におけるＰＤＣＡサイクルのＣ（チェック）を行う際に必要な具体的目標を情報セキュリティ基本計画に規定している4領域（政府機関・地方公共団体、重要インフラ、企業、個人）ごとに、可能なものについては数値目標を設定するなどして定めたものです。今後のスケジュール等については、別紙3をご参照ください。

5．我が国の情報セキュリティ分野における国際協調・貢献（国際戦略）（仮称）について（会議資料については検討中のものであるため非公表）

本日報告された、「我が国の情報セキュリティ分野における国際協調・貢献（国際戦略）（仮称）」については、近年、国民生活、社会経済活動がボーダレスに世界とつながっているＩＴ基盤への依存度をますます高めている状況を踏まえ、地球規模、すなわちグローバルな「ＩＴを安心して利用可能な環境」の構築に向けた我が国からの国際連携・協調のための戦略の策定に関する検討状況の報告が行われるとともに、議論が行われました。

今回の国際戦略は、各地域または情報セキュリティ政策領域に応じて、我が国が国際協調・貢献をどのように進めていくのかの政府横断的な基本方針となります。

また、国際戦略に関しては、本日の議論を踏まえ、経済のグローバル化が進展する中での我が国の安定的な成長や、国際社会全体における課題解決に向けた骨太な戦略となるよう引き続き検討してまいります。

なお、国際戦略の検討の背景については別紙4をご参照ください。

6．その他

上記2から5までの他に、「内閣官房情報セキュリティセンター（NISC）のこれまでの取組み」及び「技術戦略専門委員会報告書2006」について報告が行われました。前者の詳細な内容については、別紙5を、後者については、別紙6をご参照ください。

【本件に関する問い合わせ先】
内閣官房情報セキュリティセンター（NISC）
山口補佐官、関参事官、中田参事官補佐
電話　03-3581-3768（センター代表）

※「情報セキュリティ政策会議」は、平成17年5月30日のIT戦略本部決定によって設置されました（http://www.nisc.go.jp/press/pdf/050530seisaku-press.pdf）。

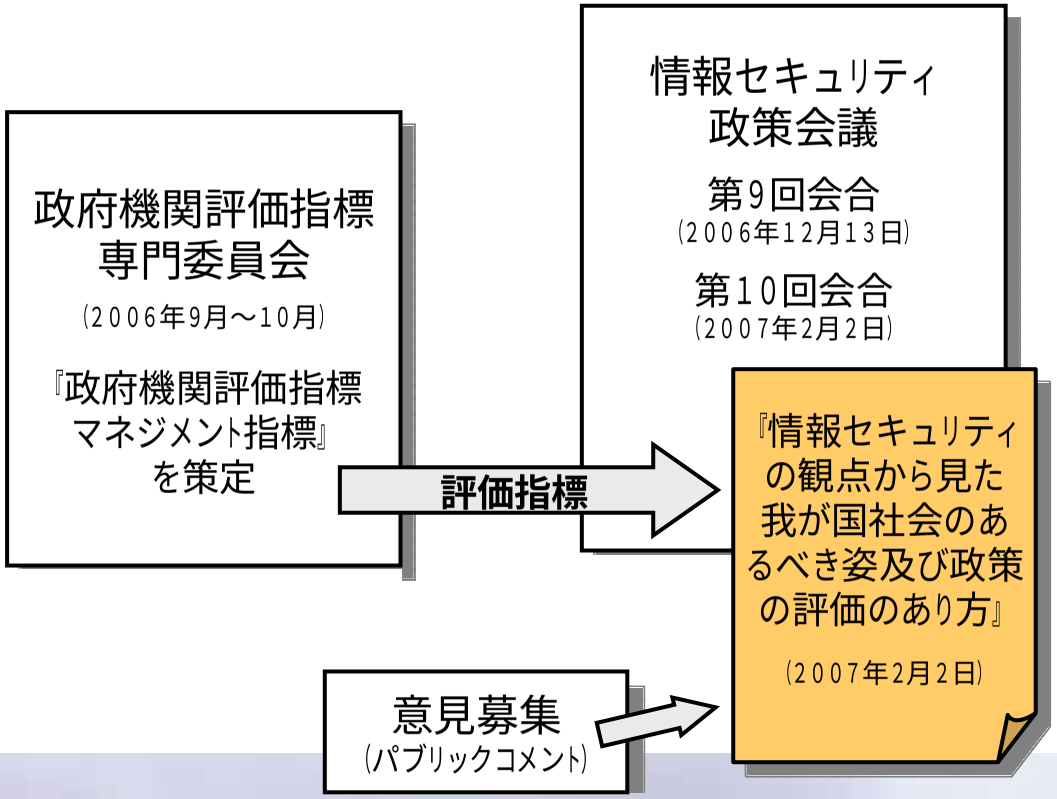
政府機関の情報セキュリティマネジメントの総合的な評価

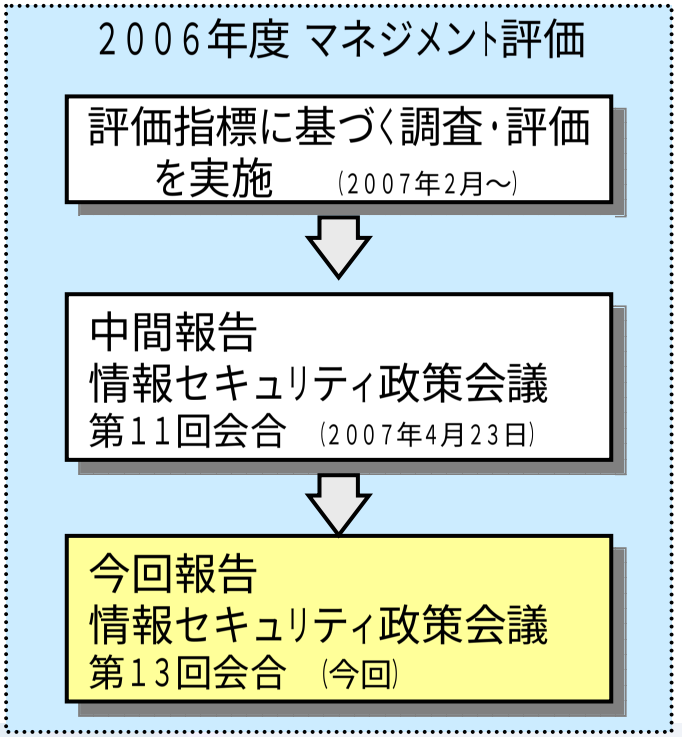
NISC

「マネジメント評価」

- 府省庁における情報セキュリティマネジメントがPDCAサイクルの各段階で確実かつ効果的におこなわれているかを評価
- 「計画」「周知」「実施」及び「評価と改善」の各段階にわたる45の評価指標に基づき府省庁におけるプラクティスを抽出し、評価

★★★ 政府内外を問わず模範となる先進的な取り組みを実践している
★★ 政府機関の模範となる工夫が見られる
★ おおむね適切に行われている





別紙1－1

政府機関の情報セキュリティマネジメントの総合的評価　～2006年度～

- 2006年度 情報セキュリティ・ベストプラクティス

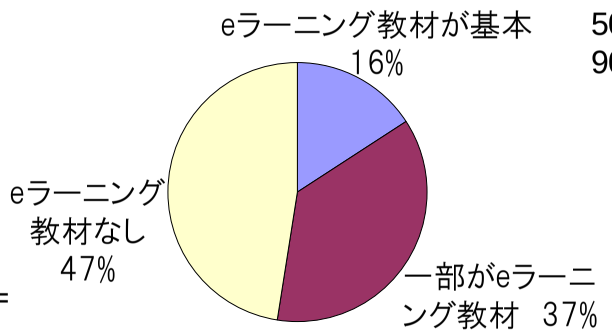
★★ 省内ネットワークを活用した職員の支援
・eラーニングシステム　・実施手順等の運用　**総務省**　**経済産業省**

★★ 幹部職員の下で全庁一体となった対策の推進　**警察庁**

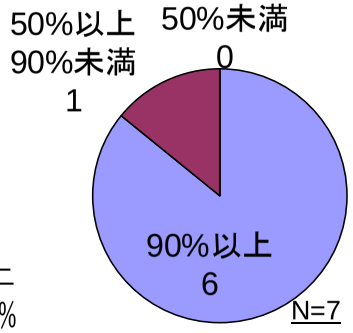
★★ 外部委託における情報セキュリティの確保　**外務省**　**防衛省**

  - 政府機関の模範となるプラクティス（★★）は「計画」及び「周知」を中心に44件。
  - 政府内外を問わず模範となる先進的な取り組み（★★★）は見られなかった。

- 各府省庁の体制等の調査結果　（政府機関の全体状況については別紙1－3を参照）
  - 情報セキュリティ担当者（常任）の職員に占める割合：
    2%超=4府省庁、0．5%以下=7府省庁
  - 情報セキュリティ担当者（常任）の平均経験年数：
    1年～3年が中心
  - eラーニング導入は府省庁全体では部分的：
    「eラーニング教材が（一部でも）ある」=10府省庁



eラーニング教材の整備状況　N=19



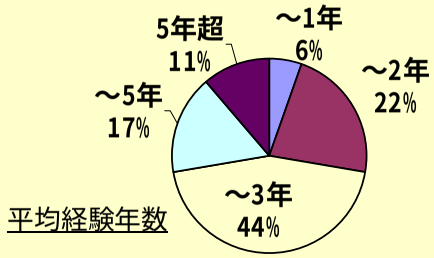
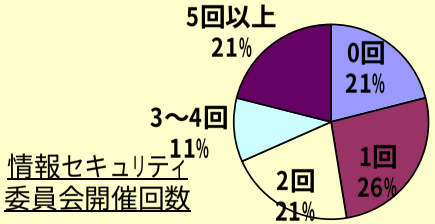
N=7
eラーニング教材が利用可能な職員の割合

※eラーニング：コンピュータネットワークなどを活用して教育を行うこと

別紙1－2

政府機関の情報セキュリティマネジメントの状況　～2006年度～

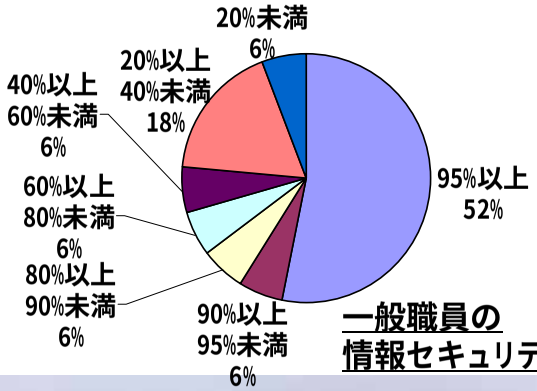
NISC

大分類	小分類	観点	調査結果
計画	資源	情報セキュリティ対策管理部門に適切な人的資源が割り当てられているか  	○ 情報セキュリティ担当者(注)（常任）の人数と職員に占める割合： (注)　情報セキュリティを含む情報システムに係る業務を主たる担当業務とする者 ・4府省庁で2%超　　7府省庁で0.5%以下 ・6府省庁で4名以下 府省庁内共通システム担当等が情報セキュリティ推進も兼務 ・7府省庁で100名超 各情報システムの担当が情報セキュリティ対策も実施 ○ 8府省庁で、常任と同数以上の一時的な担当者が従事している。 ○ 情報セキュリティ担当者の平均経験年数： ・府省庁内平均の分布は1年～3年が中心。
	組織	基準で定める責任者等が指名されているだけでなく、実態において組織として機能し得るものであるか  	○ 各府省庁において、責任者等の指名に加えて、推進体制が存在。 ・PMO、CIO補佐官、最高情報セキュリティアドバイザー等 ・6府省庁において情報セキュリティの専門家を登用し、対策推進における助言、技術仕様の整備等で実績 ○ 情報セキュリティ組織の活動に加え、府省庁の幹部が指示・決定を行っている例は一部にとどまる。 ○ 情報セキュリティ委員会の運営は、一部の府省庁で不足している。 ・4府省庁で開催なし、5府省庁で開催1回
	規程	情報システムに適用する規程は、それぞれの情報システムの特性や取り扱う情報等を考慮して策定されているか	○ 各府省庁において、情報システムに適用する規程を、情報システムセキュリティ責任者の確認を受けて概ね整備している。
		現場への適合性を適時に評価し、必要に応じて見直しをしているか	○ 各府省庁において、規程の見直しの必要性有無を適時検討している。 ○ 判断を行う仕組みとしてPMOや情報セキュリティ委員会を活用する例もある。

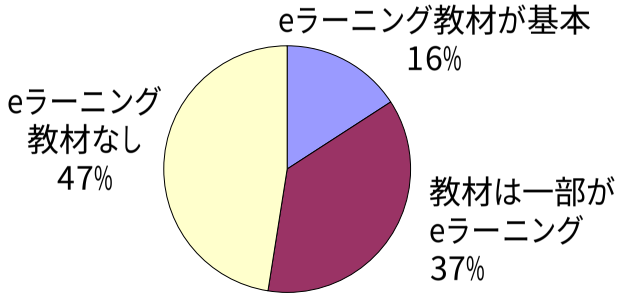
別紙1－3

政府機関の情報セキュリティマネジメントの状況　～2006年度～

大分類	小分類	観点	調査結果
周知	啓発	規程が定められているだけでなく、職員一人一人まで理解しうるものであるか	○ 規程を理解しやすいものとし、また参照・利用の利便を図る施策が採られている。 ・策定時に利用予定者が査読 ・府省庁内のウェブサイトに掲載 ・FAQ、ガイドブックの整備、質問対応体制　等
		規程がその利用者にとって容易に参照・利用できるようになっているか	
		組織内外のヒヤリハット情報を事例として活用しているか	○ 多くの府省庁で障害等の事例を収集する仕組みがあるが、ヒヤリ・ハット情報収集を意図した組織的な活動まではしていない。 ○ 収集した事例を対策、規程、教育等の改善に活用している例がある。
	教育	情報セキュリティ教育を適切に実施し、また試験等により職員の理解度を確認しているか	○ 教育については、より組織的な実施に向けて課題がある。 ・計画の不備、受講不徹底、受講状況管理・理解度確認不足 ・6府省庁で一般職員の教育受講率が80%未満 ○ eラーニングの活用は、現状では一部に限られている。 ・3府省庁で教材を概ねeラーニングにより整備し、7府省庁で一部の教材をeラーニングで整備している ・6府省庁でeラーニング教材が地方支分部局等でも広く利用可能



一般職員の情報セキュリティ教育受講率
N=19

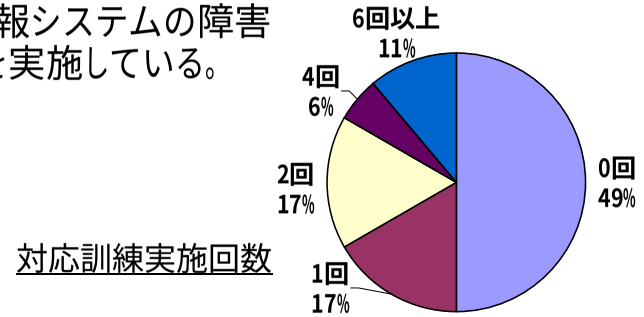
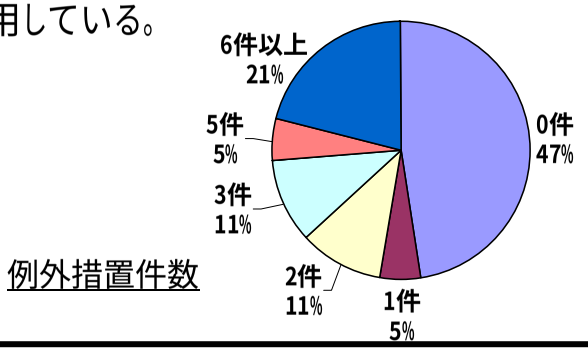


eラーニング教材の整備状況 N=19

別紙1－3

政府機関の情報セキュリティマネジメントの状況　～2006年度～

NISC

大分類	小分類	観点	調査結果
実施	業務改善	先端的技術の活用（対策のシステム化等）等により、情報セキュリティ対策が業務プロセスにシームレスに組み込まれているか	○ 各府省庁において、情報セキュリティ対策の確実な実施等を目的としてITを活用している。
	異常・障害等への対応	府省庁外からの脅威情報を周知しているか	○ 各府省庁において、脅威情報（ウイルスに関する警告等）を府省庁内の職員に適時に周知している。
		障害等（インシデント及び故障を含む）への対応が適切に行われるか	○ 各府省庁において、障害等の対応手順が整備されている。 ○ 9府省庁において、情報システムの障害等に備えた対応訓練を実施している。  対応訓練実施回数
		障害等の事後策を実施しているか	○ 各府省庁において、障害等の再発防止策を策定している。
	例外措置	基準への例外事項をあまねく把握し、例外措置を適用できているか	○ 規程等への例外措置は10府省庁で適用実績がある。このうち8府省庁では代替措置も検討し適用している。  例外措置件数

別紙1－3

政府機関の情報セキュリティマネジメントの状況　～2006年度～

大分類	小分類	観点	調査結果
実施 (続き)	調達・外部委託	調達及び外部委託における情報セキュリティ確保のために十分な対策が採られているか	○ 調達仕様書及び契約に関して、情報セキュリティ関連事項の標準を示した手順等や雛形が概ね用意されている。ただし、会計課等の雛形で省庁基準等の要件に対応している府省庁は一部にとどまる。 ○ 多様な調達案件に対応するため、調達仕様等についてCIO補佐官による確認や助言を組織的に採り入れている例もある。
評価と改善	評価と改善	自己点検が有効に行われ、必要な改善が図られているか	○ 各府省庁において、自己点検結果に基づく改善指示が行われている。
		情報セキュリティ監査が有効に行われ、必要な改善が図られているか	○ 各府省庁において、情報セキュリティ監査の計画策定、実施、報告及び改善指示が概ね行われている。

別紙1－3

端末及びウェブサーバに関する情報セキュリティ対策の総合評価

NISC

重点検査の項目

端末に関する重点検査項目	
不正プログラム対策	・OSのパッチ等の適用状況 ・主要APのパッチ等の適用状況 ・アンチウイルス対策ソフトの運用状況
情報保護対策	・モバイルPCの暗号化機能の運用状況
端末管理	・端末の物理的対策状況

ウェブサーバに関する重点検査項目	
不正プログラム対策	・OSのパッチ等の適用状況 ・ウェブサーバAPのパッチ等の適用状況等
不正アクセス対策	・不正アクセス対策状況
情報保護対策	・利用者に対する権限管理等の実施状況
サーバ管理	・管理者に対する権限管理等の実施状況 ・データ復旧対策状況

・府省庁の調査に基づく結果
・平成19年3月末時点

総合評価	端末			ウェブサーバ		
	H18		H19	H18		H19
内閣官房	B	▷▷	B	B	▷	B
内閣法制局	C	▷▷	B	B	－	B
人事院	C	▷▷▷	A	B	▷▷	B
内閣府	C	▷▷▷	B	C	▷▷	B
宮内庁	D	▷▷▷▷	A	C	▷▷▷	A
公正取引委員会	C	▷▷▷	A	A	－	A
警察庁	D	▷▷▷▷	A	B	▷▷	A
金融庁	B	▷▷	B	B	▷	A
総務省	C	▷▷▷	B	B	▷	B
法務省	D	▷▷▷▷	B	C	▷▷▷	B
外務省	D	▷▷▷▷	A	B	▷▷	B
財務省	C	▷▷	B	B	▷▷	B
文部科学省	C	▷▷▷	A	B	▷▷	A
厚生労働省	D	▷▷▷	B	B	▷	B
農林水産省	C	▷▷▷	A	B	▷	A
経済産業省	C	▷▷▷	A	B	▷	A
国土交通省	D	▷▷▷	B	C	▷▷	B
環境省	B	▷	B	B	▷▷	A
防衛省	C	▷▷▷▷	B	B	▷▷	A

評価	実施率	評価	実施率	評価	実施率	評価	実施率
A	x＝100%	B	80%≦x＜100%	C	60%≦x ＜80%	D	x＜ 60%

上昇率		上昇率		上昇率		上昇率		上昇率		上昇率	
▷▷▷▷	x＞ 40%	▷▷▷	x＞ 30%	▷▷▷	x＞ 20%	▷▷	x＞ 10%	▷	x＞ 0%	－	x＝ 0%

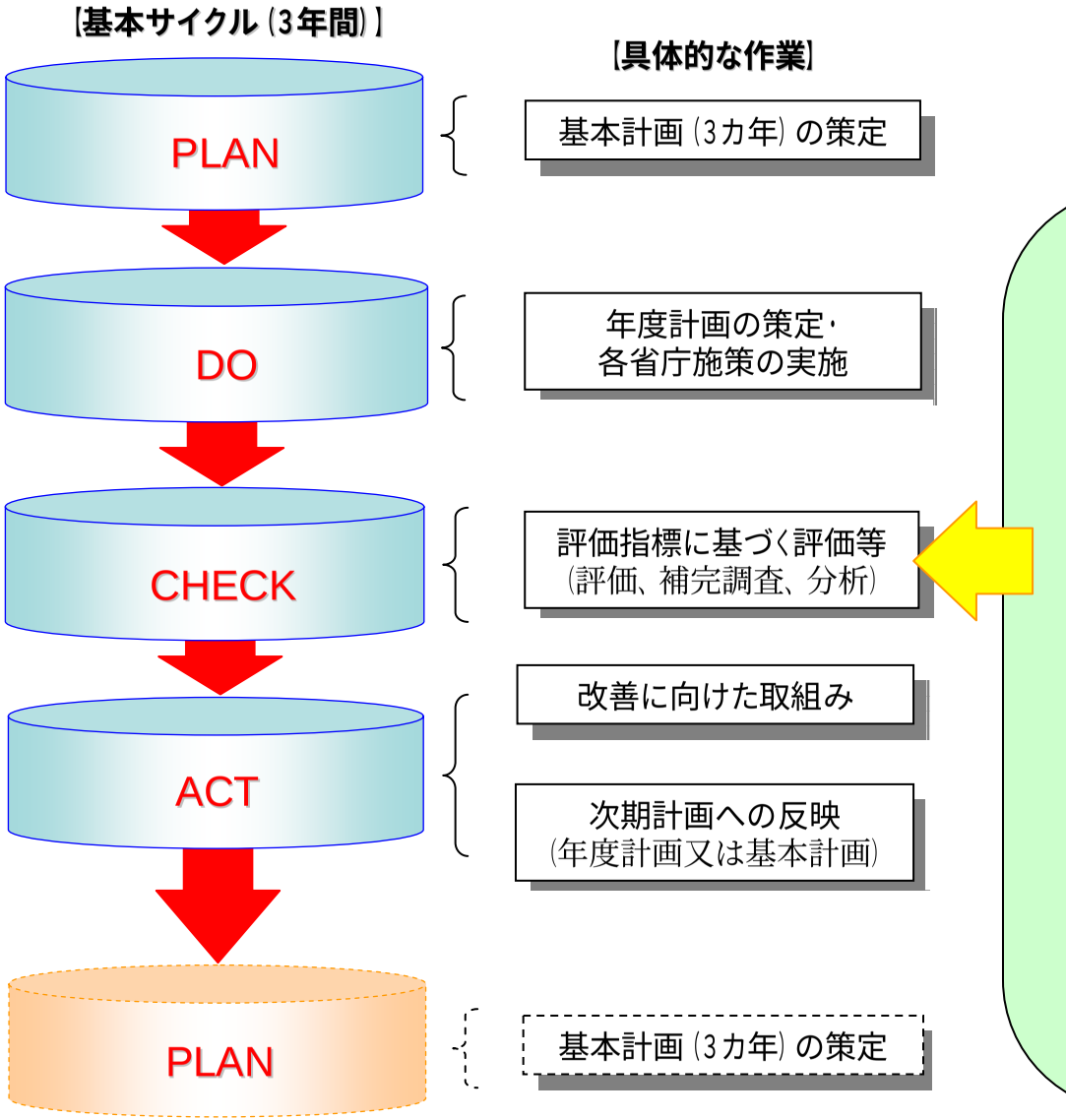
別紙２－１

評価結果を受けての対応予定

	端　末	ウェブサーバ
内閣官房	平成２０年度	平成２０年度
内閣法制局	今年度	今年度
人事院	実施済み	実施済み
内閣府	平成２０年度	平成２０年度
宮内庁	実施済み	実施済み
公正取引委員会	実施済み	実施済み
警察庁	実施済み	実施済み
金融庁	今年度	実施済み
総務省	平成２０年度	平成２０年度
法務省	平成２０年度	平成２０年度
外務省	実施済み	今年度
財務省	平成２０年度	平成２０年度
文部科学省	実施済み	実施済み
厚生労働省	平成２０年度	平成２０年度
農林水産省	実施済み	実施済み
経済産業省	実施済み	実施済み
国土交通省	平成２０年度	平成２０年度
環境省	今年度	実施済み
防衛省	今年度	実施済み

別紙２－２

情報セキュリティ政策のＰＤＣＡサイクルと今回決定する事項等の関係



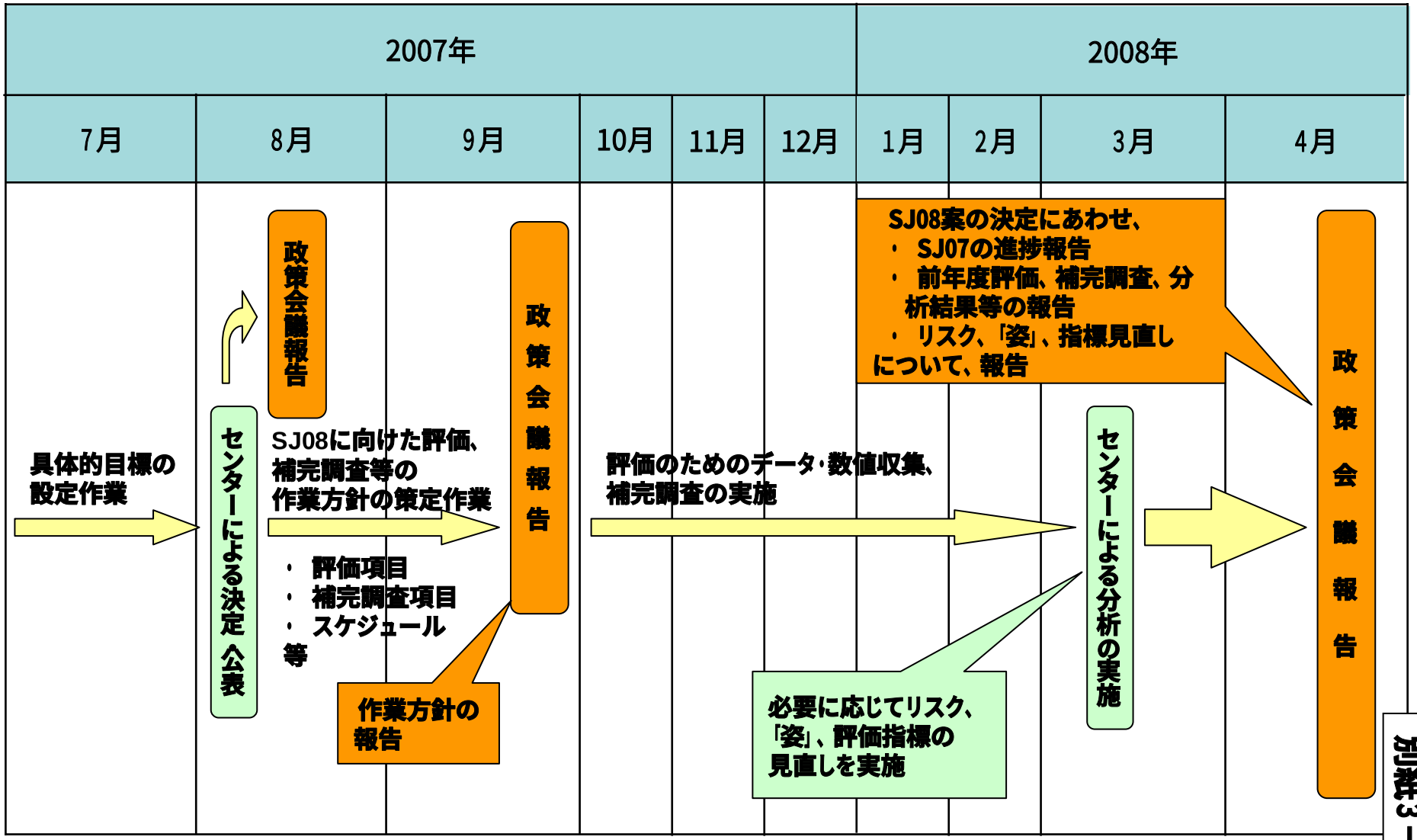
今回決定すべき事項
→　具体的目標の設定

（参考）
○「セキュア・ジャパンの実現に向けた取組みの評価等及び合理性を持った持続的改善の推進について」（平成19年2月2日政策会議決定）
2　センターは、必要に応じて各府省庁の協力を得て、各評価指標に係る具体的目標を設定するとともに、評価指標の見直しを行うものとする。

○「情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方」（平成19年2月2日政策会議了解）
（P37）…センターは、….可能なものについての数値目標の設定を含め、具体的目標の設定を行うこととする。
（P38）…センターは、２００７年度の年度計画の策定後、必要に応じて各府省庁の協力を得て、すみやかに、第1次基本計画が目標とする時点における各評価指標に関する具体的目標を設定する…
（P39）図4　7月から8月にかけて、具体的目標の設定を行うこととされている

別紙３－１

今後のスケジュール



別紙3－2

国際戦略の取組みの背景

○ 情報セキュリティ政策会議等における検討

・ 情報セキュリティ政策会議等の場で、有識者構成員等から、「我が国の情報セキュリティの取組みの国際展開が必要」との度重なるご意見。

・ 第1次情報セキュリティ基本計画をもとに、セキュア・ジャパン2007において、国際戦略の基本方針を2007年度に策定することを明記。

○ 経済財政諮問会議等における検討

・ 平成19年4月20日、官房長官から、「ITによる生産性改革を支えるセキュリティ基盤の重要性－国内対策の推進と国際的な政策展開－」を発表。

・ 「成長力加速プログラム」（平成19年4月25日）において、情報セキュリティ分野の国際戦略を7月までに策定を決定。

・ 「経済財政改革の基本方針2007」（平成19年6月19日、いわゆる骨太の方針）において、「情報セキュリティの向上に向け、（中略）各国との連携・協力等を推進する。」ことを明記。

別紙4

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）

副センター長（内閣審議官）

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　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

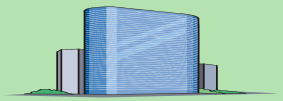
●相互依存性の分析
●横断的な対策基準の策定
●総合的演習の実施　等

国際戦略

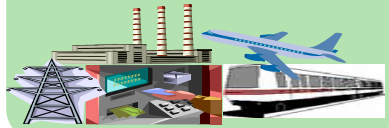
●情報セキュリティに関する我が国の国際戦略の立案
●諸外国の関係機関等との緊密な連携　等

企業　個人

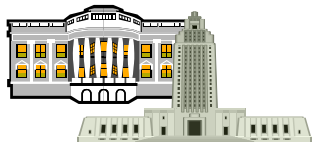
各政府組織



重要インフラ



諸外国関係機関



	現在数	本年度交代者数（着任2年超含む）
国の職員	37	28
非常勤職員	24	13
事務補助	2	2
計	63	43

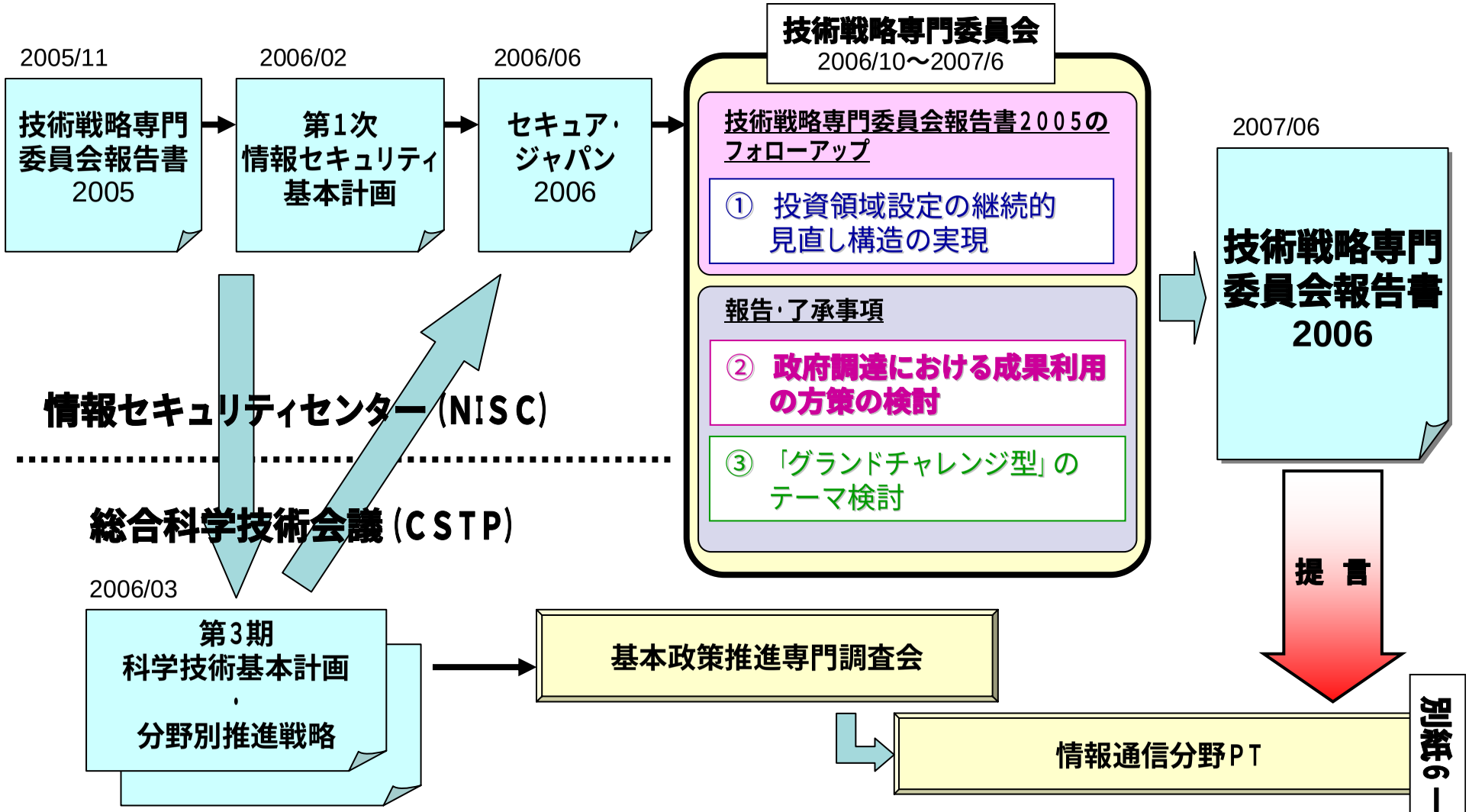
内閣官房の体制強化の変遷

2000年2月発足時 8名 → 2001年1月 9名 → 2004年7月 18名 → 2005年4月NISC設置時 22名 → 2007年8月 63名

別紙5

技術戦略専門委員会の活動経緯

◆ 2005年に「技術戦略専門委員会報告書2005」を策定した委員自らがフォローアップ作業を行うことを目標として議論を展開



①投資領域設定の継続的見直し構造の実現

◇ 基本的な考え方

- 限られた投資の中で効率的･効果的な研究開発･技術開発を実現するためには、情報セキュリティに関連する**研究開発･技術開発の実施状況の把握**及び**投資領域設定の継続的な見直し**が不可欠
- 狭義の情報セキュリティ分野に限定せず、情報通信全般を対象として把握、見直しを実施し、情報セキュリティ確保に留意することが重要

◇ 研究開発･技術開発の実施状況把握

- 情報セキュリティに関連する研究開発･技術開発を抽出し、分野ごとに整理
- 民間における実施状況の把握が課題

◇ 報告書２００５にて選定した重点化分野の見直し

- 「認証技術」は単に技術開発だけでなく、社会展開までを含めた研究が必要

電子認証技術の強化 → 見直し → 認証基盤のガバナンスの確立と高度化

- 問題の顕在化により新規追加

新規追加 → 情報通信構成要素の検査技術の高度化

情報通信基盤に対する依存性についての広範な検討

別紙６－２

②調達を通して成果を活用するガイドライン策定の検討

◇ 基本的な考え方

- 情報セキュリティを適正なレベルで確保する構造、いわゆる情報セキュリティガバナンスとそのデザインが重要
- 必要となる技術の開発、調達及び利用する組織、人間系の管理手法などの様々な要件を分析し、総合的な視点から検討の積み重ねが不可欠であり、情報セキュリティのガバナンス自体が情報セキュリティ技術における研究分野
- 研究開発・技術開発における成果を、調達を通して最大限、直接政府が活用し、組織・人間系の管理手法についても併せて提言するガイドラインを策定する

◇ ガイドライン策定の具体的手法

２００６年度から産学官の共同研究開発プロジェクトとして開始した「高セキュリティ機能を実現する次世代ＯＳ環境の開発」を通して、開発、調達及びその利用という政府における一貫した成果利用までを見据えた研究開発・技術開発を実施し、その過程において発生する様々なノウハウをガイドラインとしてまとめる。

◇ ガイドライン策定に関しての試案

- 技術利用の現場からのニーズの掘り起こしと、研究開発現場へのフィードバック、研究領域の調整という循環モデルを構築することが必要。
- 成果利用の可能性を評価する枠組みも必要。その際、成果の国際展開を視野に入れた評価、特に標準化、リファレンスモデル化などの取組みによる国際性を持った成果利用を積極的に推進することが不可欠。

③「グランドチャレンジ型」テーマ検討の場の設置

◇ 基本的な考え方

- 段階的に技術を伸ばしていく領域と、新たに領域を立ち上げるチャレンジの要素が大きい領域とをバランスよく保つ考え方が必要
- 目標を明確化し、研究の段階ごとに十分な評価を行いながら長期の研究を推進
- 大きな研究開発に至る前に、小規模で多様な萌芽的研究を広範囲に実施できる環境が必要

◇ グランドチャレンジWGでの検討事項

- 大目標の下で統合的に推進（ビジョナリィ・ゴール型）
  →長期的な研究を実施する意義、サブ課題間の関連性等の明確化
- 技術要素を精査して取組む（テクニカル・コンポーネント型）
  →情報セキュリティの技術要素の選定

◇ 研究開発・技術開発を推進する体制

大目標の下での多岐にわたる各種要素技術の統合管理と最適な資源配分を促進するための枠組み構築が最重要事項

◇「グランドチャレンジ型」プロジェクトの実行行程

2007年度中にグランドチャレンジWGを開催し、実施方法の詳細な検討を行い、その検討結果をふまえた具体的なテーマを選定する