

平成 17 年 9 月 15 日
内閣官房情報セキュリティセンター (NISC)

第2回情報セキュリティ政策会議の開催について

- 政府機関及び重要インフラの情報セキュリティ対策強化のための施策決定 -

1. 本日、「情報セキュリティ政策会議」(議長:内閣官房長官)の第2回会合が開催され、
 - (1) 政府機関の情報セキュリティ対策を強化するための「政府機関の情報セキュリティ対策のための統一基準(2005年項目限定版)」及び
 - (2) 国民生活・経済活動の基盤となる重要インフラの情報セキュリティ対策の強化に向けた「重要インフラの情報セキュリティ対策に係る基本的考え方」の2点につき、政策会議決定を行いました(本日の検討内容の全体像については、別紙1をご参照下さい)。

「情報セキュリティ政策会議」は、本年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.bits.go.jp/press/pdf/050530seisaku-press.pdf>)。

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)ホームページ(<http://www.bits.go.jp/>)において公表しています。また本日の議事要旨は、後日、同ホームページにて公表いたします。

2. 本日決定された「政府機関の情報セキュリティ対策のための統一基準(2005年項目限定版)」の概要は以下の通りです。

「政府機関統一基準(2005年項目限定版)」の詳細は、内閣官房情報セキュリティセンター(NISC)ホームページ(<http://www.bits.go.jp/>)において公表していますのでご参照下さい。

(1) 位置付けと主な内容(別紙2-1、2-2参照)

政府機関(各省庁)の情報セキュリティ対策については、1)情報セキュリティ水準の高い省庁と低い省庁の格差が大きい、2)急激に変化するIT環境に対応した情報セキュリティ対策を実施する人材が全体的に不足している等の問題が指摘されています。

また、昨今、政府機関へのサイバー攻撃が増加し、国内の企業等においては、重要情報の漏洩問題が相次ぐなど、情報セキュリティ関連の事故が多発している

状況にあります。

こうした状況を受けて、今般、「政府機関統一基準(2005年項目限定版)」として、1)緊急度の高い対策を中心とし、2)政府機関全体として統一的にとるべきものについてとりまとめ、政府機関全体として早急に対策を実施することとしたものです。

< 政府機関統一基準(2005年項目限定版)に盛り込まれた内容の例 >

情報の格付け及び取扱制限の基準を明示する手順の整備
一定の情報システムに対する証跡管理機能の導入
サービス不能攻撃(Dos 攻撃)対策の実施
外部委託を実施する際の、情報セキュリティ監査の受け入れ等を含めた契約書の取り交わし
省庁外での情報処理実施の場合の一定の記録の取得 等

(2)今後の展開(別紙2 - 3参照)

今後は、まず、「政府機関統一基準(2005年項目限定版)」に基づいた対策の徹底を行うため、内閣官房情報セキュリティセンター(NISC)が、各省庁において本基準に従った対策が行われているか否かの状況を検査し、情報セキュリティ政策会議に報告する予定です(本年度内を目処)。

また、1)今般とりまとめた「緊急度の高い対策」に加えて、システムの開発・整備に関する対策項目などを追加した「政府機関統一基準(2005年12月全体版初版)」を策定するとともに(年内を目処)、2)各省庁における具体的なレベルでの対策実施を支援するための「個別ガイドライン群」(例;Webサーバ設置ガイドライン、モバイルパソコン管理ガイドライン等)を順次策定する予定です。

3. 本日決定された「重要インフラの情報セキュリティ対策に係る基本的考え方」の概要は以下の通りです。

(1)位置付けと主な内容

「重要インフラの情報セキュリティ対策に係る基本的考え方」は、IT戦略本部情報セキュリティ基本問題委員会第2次提言(平成17年4月22日)を踏まえ、「重要インフラのサイバーテロ対策に係る特別行動計画(平成12年12月)」及びこれに基づく取り組みを発展・強化させた新たな行動計画をとりまとめるための、基

本的方向性を示したものです。主な内容については、別紙3 - 1及び3 - 2をご参照下さい。

(2)今後の展開

今後は、本日決定された「基本的考え方」に基づき、また本日同時に設置が決定された「重要インフラ専門委員会」()における検討を行い、**本年内を目処に、重要インフラの情報セキュリティ対策に係る新しい行動計画を策定する予定**です。

()「重要インフラ専門委員会」の委員には、別紙5の方々に委嘱を行う予定としています。

4. なお、本日の会合において、「第1次情報セキュリティ基本計画(仮称)」の方向性についての自由討議が行われました。本日の会議での意見、先般設置された専門委員会()での検討内容を踏まえ、**本年内を目処に「第1次情報セキュリティ基本計画(仮称)」を策定するための検討を行っていく予定**です(別紙1、4参照)。

()情報セキュリティ政策会議の下に、「セキュリティ文化専門委員会」(委員長;安田浩 東京大学国際・産学共同研究センター教授)及び「技術戦略専門委員会」(委員長;佐々木良一 東京電機大学教授)を設置して検討を行っているところです。

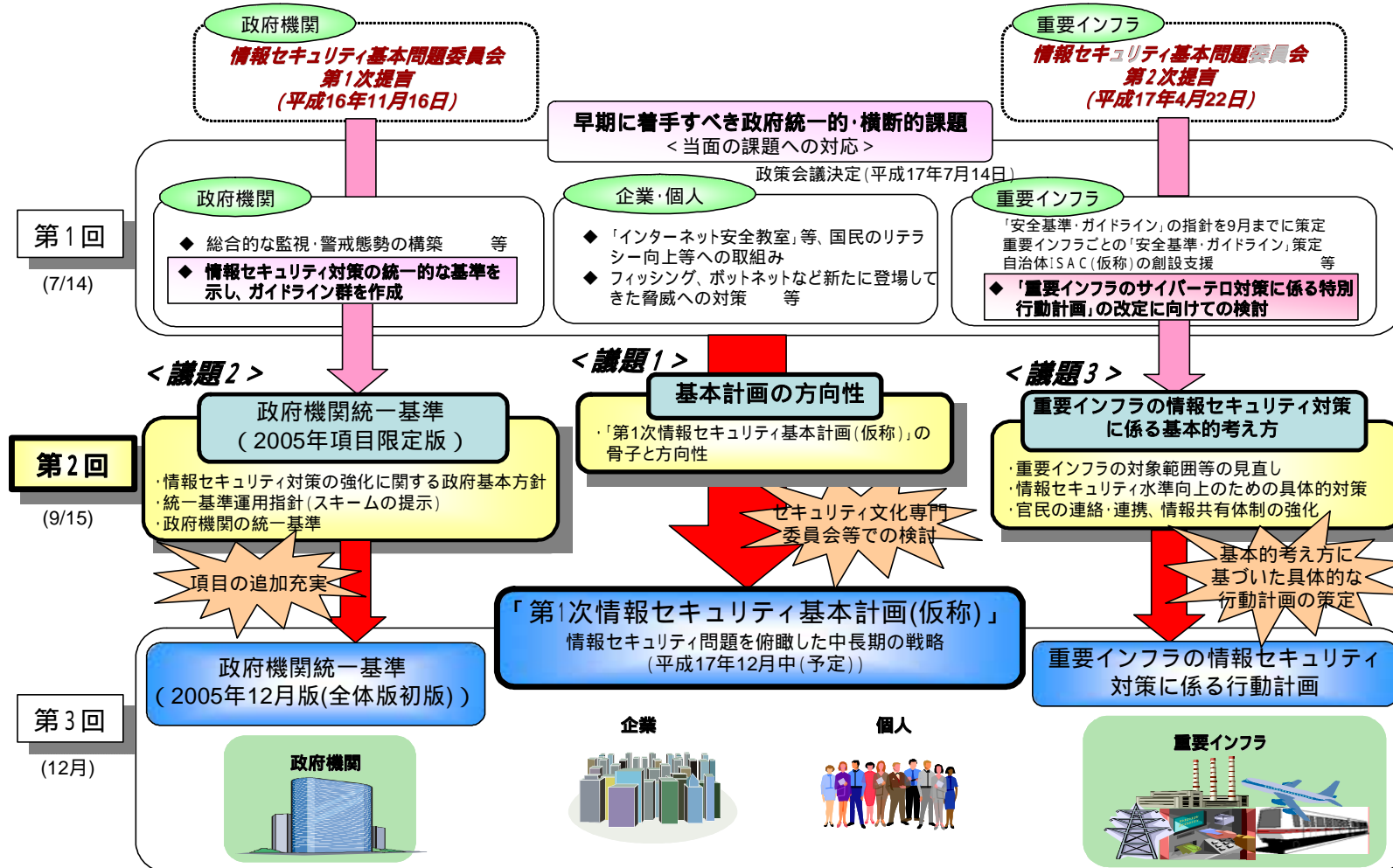
【本件に関する問い合わせ先】

内閣官房情報セキュリティセンター

山口補佐官、大矢参事官、山崎参事官補佐

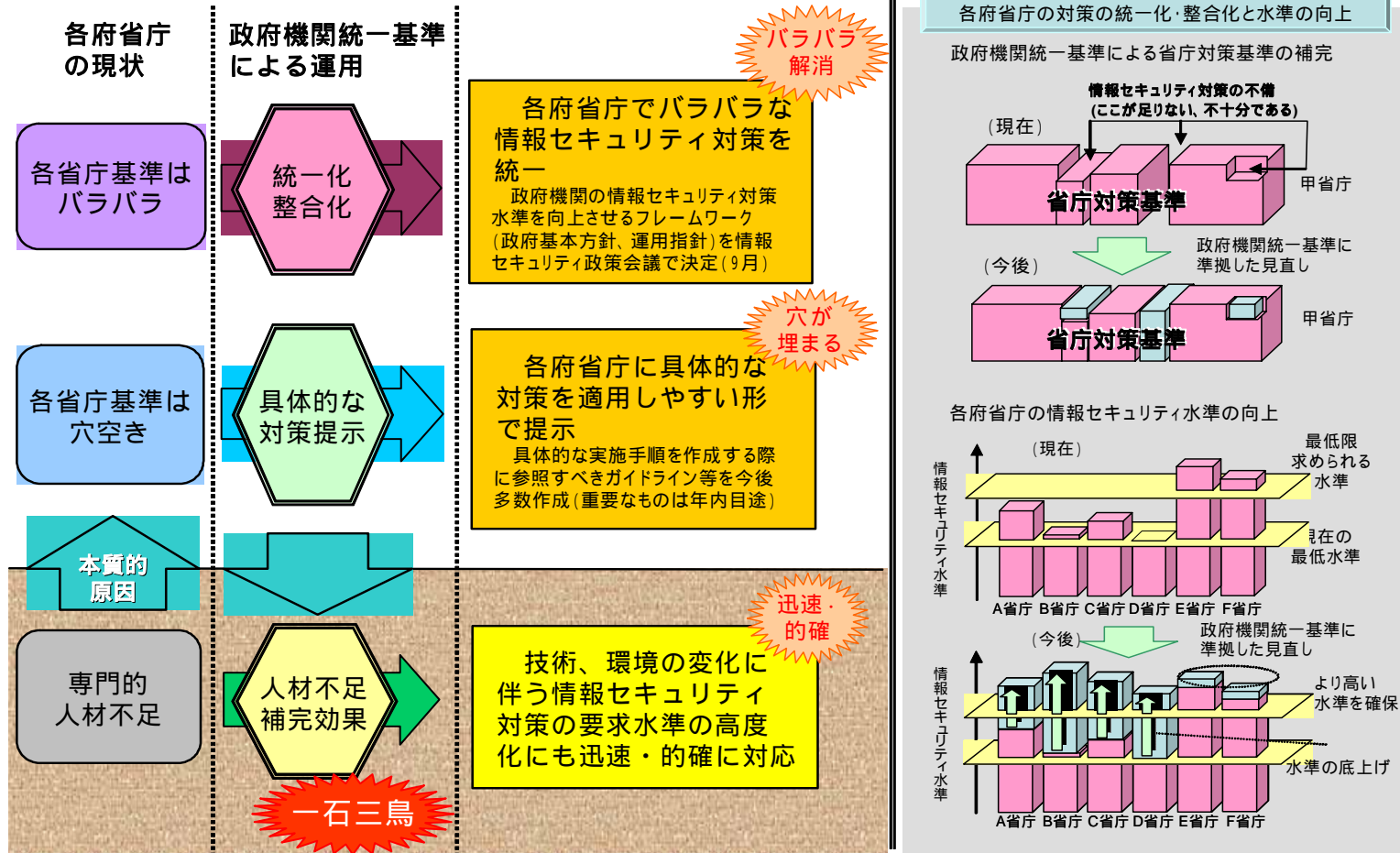
電話 03-3581-3768(室直通)

第2回情報セキュリティ政策会議の議題 ～全体像の中での位置付け～

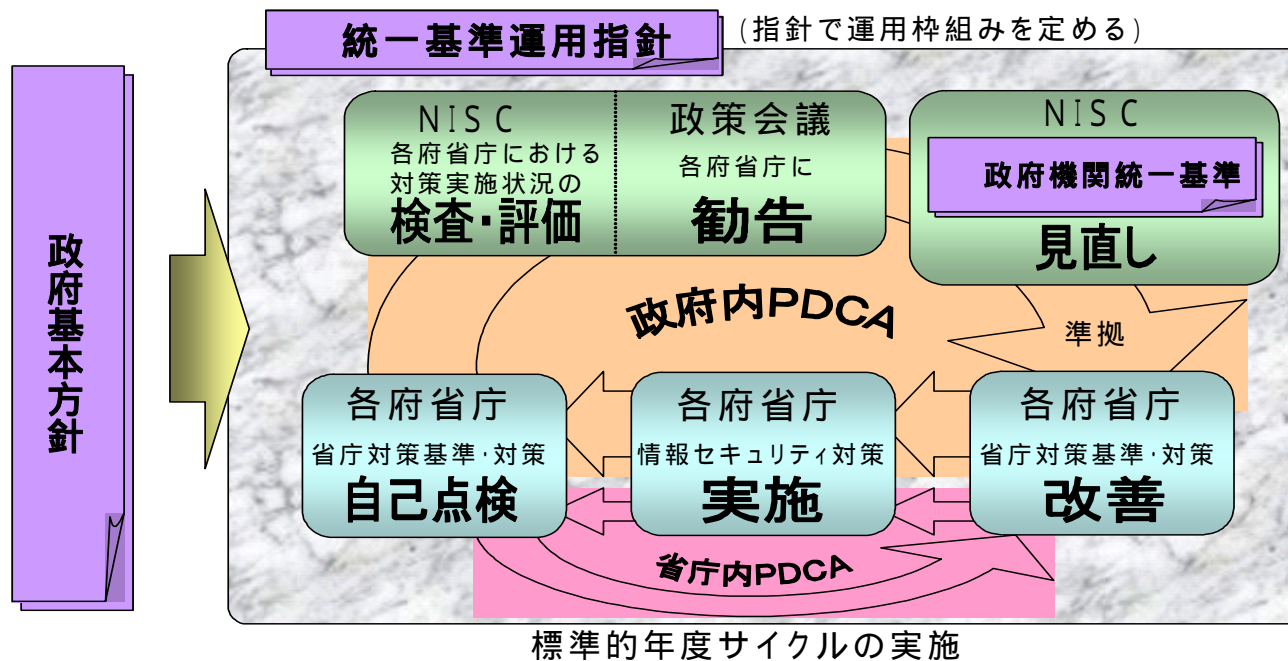


政府機関統一基準の策定の目的

世界最先端のIT(情報技術)国家にふさわしい情報セキュリティ水準を目指して、統一基準を運用



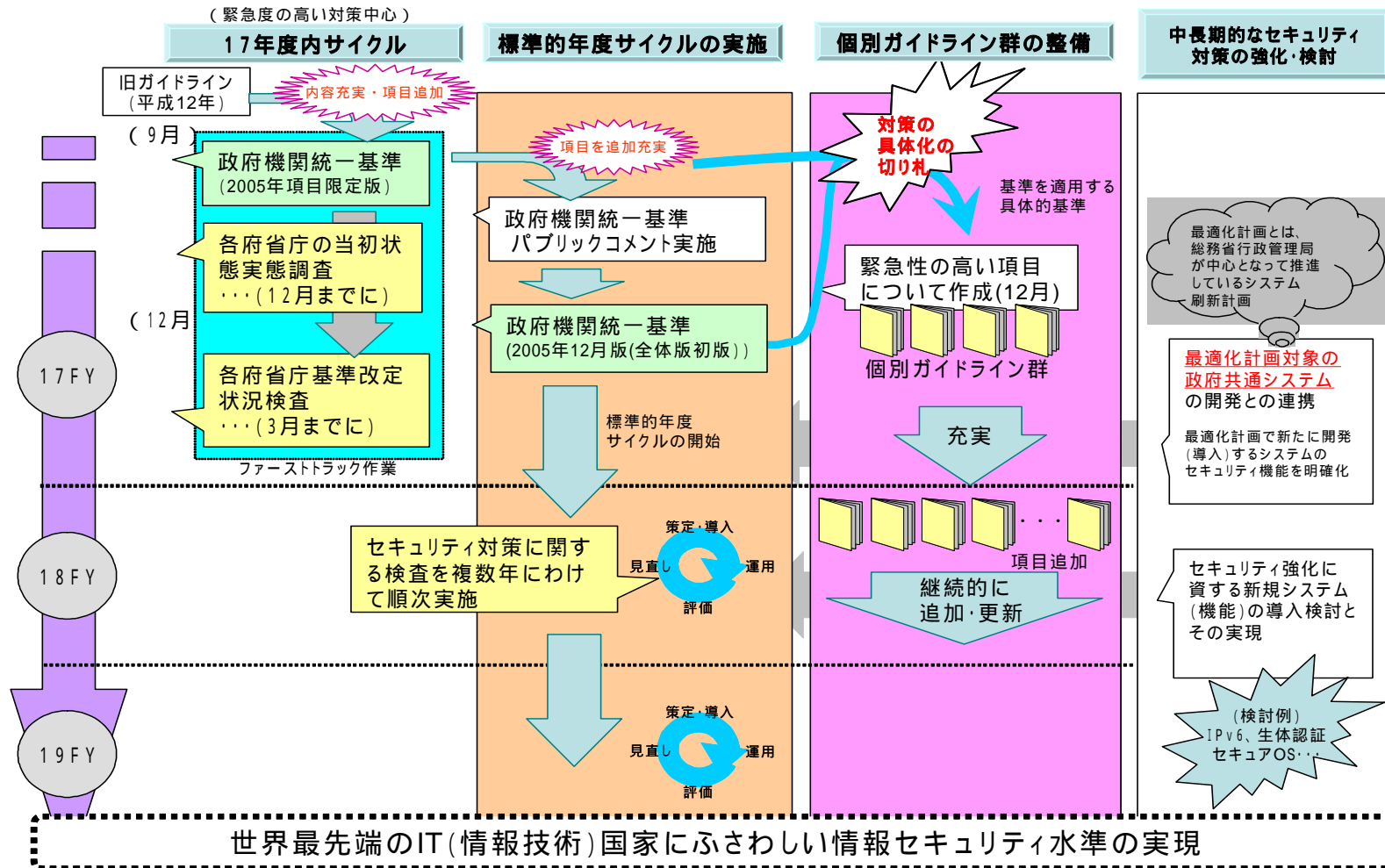
今後の政府機関の情報セキュリティ対策枠組み



今回作成する文書

- 政府基本方針:**
「政府機関の情報セキュリティ対策の強化に関する基本方針」
政府として基本的な方針を定めたもの
- 統一基準運用指針:**
「政府機関の情報セキュリティ対策における統一基準の策定と運用等に関する指針」
政府機関統一基準を運用する具体的な枠組みを示すもの
- 政府機関統一基準:**
「政府機関の情報セキュリティ対策のための統一基準」
各府省庁の情報セキュリティ対策内容の整合化・共通化を促進するために、各省庁が採るべき情報セキュリティ対策を定めたもの

統一基準による情報セキュリティ対策の実施



「重要インフラの情報セキュリティ対策に係る基本的考え方」の概要

目的

IT戦略本部情報セキュリティ専門調査会情報セキュリティ基本問題委員会第2次提言(平成17年4月22日)を踏まえ、重要インフラの各事業において発生する「IT障害」から重要インフラを防護し、重要インフラ事業者の事業継続性を確保するため、「重要インフラのサイバーテロ対策に係る特別行動計画(平成12年12月)」及びこれに基づく取り組みを発展・強化させた新たな行動計画をとりまとめるための、基本的方向性を示す。

これまでの対策とその問題点

「重要インフラのサイバーテロ対策に係る特別行動計画(平成12年12月)」について、IT利用度の高まりにより、想定脅威等を抜本的に見直す必要。

対象範囲

(1)対象範囲の見直し

従来重要インフラ分野(情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス)に、新たに「医療」、「水道」、「物流」を追加し、10分野とする。

(2) 想定脅威の見直し

サイバー攻撃等の意図的要因だけでなく、非意図的要因、自然災害など、多種多様な脅威の全てを対象

情報セキュリティ水準の向上のための具体的対策

- (1) 分野横断的な状況把握(相互依存性解析等)の実施
- (2) 分野ごとの「安全基準・ガイドライン」の作成・評価

官民の連絡・連携、情報共有体制の強化とその実効性の確保

- (1) 情報共有体制の強化(重要インフラの各分野別の「情報共有・分析センター」(仮称)の創設等)
- (2) 連絡・連携する「情報」の充実及び質の向上
- (3) IT障害発生時対応の強化
- (4) 分野横断的演習を通じた機能・体制の検証と見直し

情報セキュリティ基盤の強化

- (1) 人材育成・研究開発
- (2) 事案対処省庁の取り組みの強化
- (3) 地域レベルの取り組みの促進
- (4) 国際連携

重要インフラの情報セキュリティ対策に係る行動計画の策定

「重要インフラ専門委員会」を設置し、平成17年末を目処に、行動計画を策定。

重要インフラの情報セキュリティ対策に係る基本的考え方の 施策の実施予定

平成17年度

重要インフラの情報セキュリティ対策に係る行動計画の策定（年末を目処）

「安全基準・ガイドライン策定のための指針」の決定（年末を目処）

内閣官房からの早期警戒情報提供の枠組みの整備（年度末を目処）

内閣官房におけるインフラ分野間のコーディネーション機能の整備
（年度末を目処）

平成18年度

「安全基準・ガイドライン」の策定・見直し等（9月末を目処）

重要インフラ横断的な演習の企画・実施（年度中）

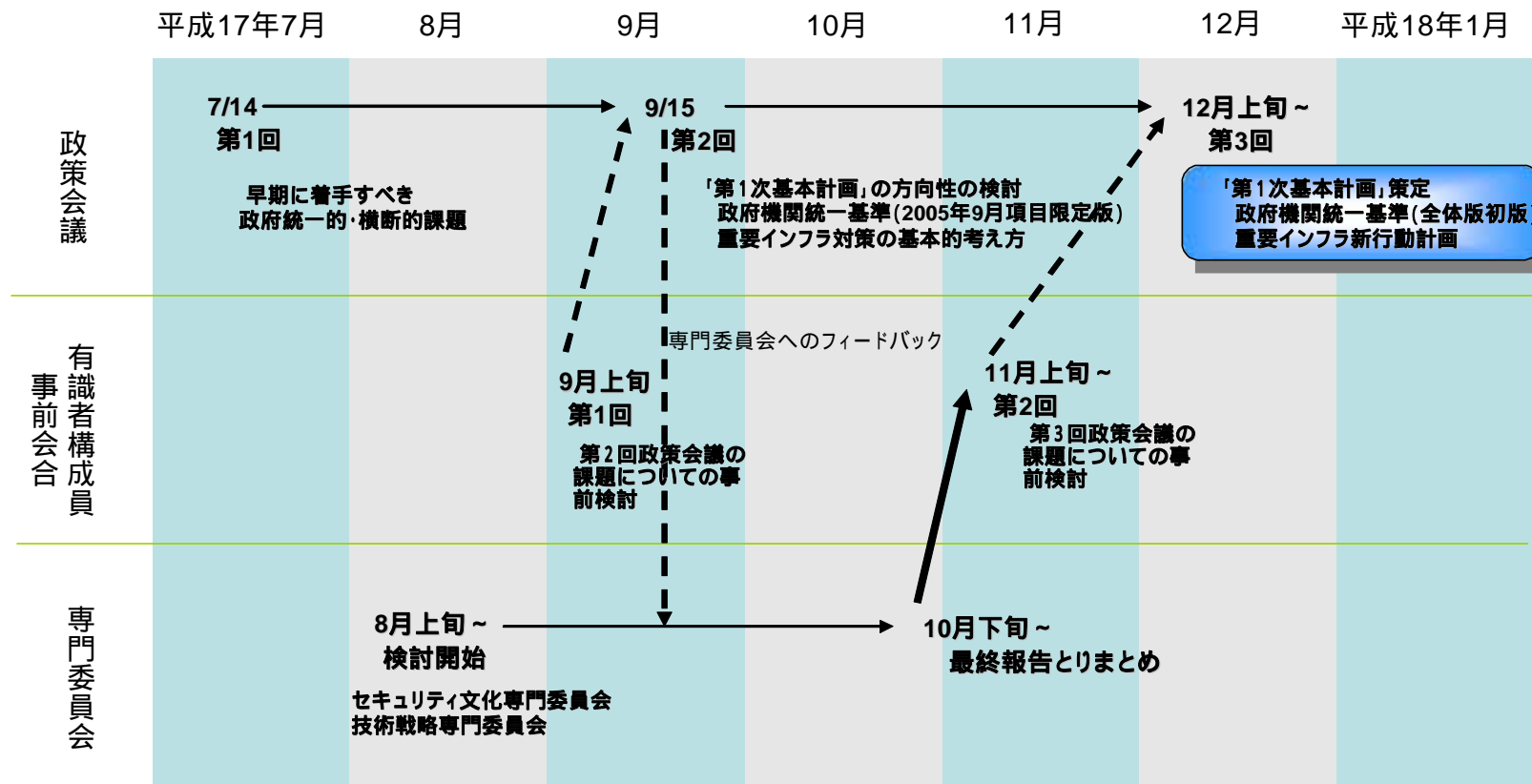
相互依存性解析の実施（年度末を目処）

重要インフラの各分野別の「情報共有・分析センター」（仮称）の創設
（年度末を目処）

「重要インフラ連絡協議会」（仮称）の整備の推進（年度末を目処）

「第1次情報セキュリティ基本計画(仮称)」検討スケジュール

- ▶ 本年(平成17年)末を目処に、情報セキュリティ問題を俯瞰した中長期の戦略としての「第1次情報セキュリティ基本計画(仮称)」を策定。
 - ▶ 政府機関及び重要インフラに対する対策については、情報セキュリティ基本問題委員会の第1次提言及び第2次提言を踏まえ、先行的に具体策を検討し、本年末、基本計画と同時に全体版をとりまとめ。



重要インフラ専門委員会委員名簿(案)

浅野 正一郎	情報・システム研究機構国立情報学研究所教授
伊藤 友里恵	有限責任中間法人 JPCERT コーディネーションセンター経営企画 室業務統括
稲垣 隆一	弁護士
神保 謙	慶應義塾大学湘南藤沢キャンパス総合政策学部専任講師
土居 範久	中央大学理工学部教授
中尾 康二	KDDI(株)技術開発本部情報セキュリティ技術部長
松田 栄之	新日本監査法人公会計本部
渡辺 研司	長岡技術科学大学経営情報系助教授

(五十音順、敬称略)

情報通信分野	(委員選定中)
金融分野	(委員選定中)
航空分野	(委員選定中)
鉄道分野	(委員選定中)
電力分野	(委員選定中)
ガス分野	(委員選定中)
政府・行政サービス分野(地方公共団体を含む。)	(委員選定中)
医療分野	(委員選定中)
水道分野	(委員選定中)
物流分野	(委員選定中)