報道発表

平成 20 年6月19日
内閣官房情報セキュリティセンター（NISC）

第18回情報セキュリティ政策会議の開催について

－「セキュア・ジャパン 2008」の決定等－

本日、「情報セキュリティ政策会議」（議長：内閣官房長官）の第18回会合が開催され、その概要は以下のとおり。

なお、本会合では、「セキュア・ジャパン 2008（SJ2008）」が決定されるとともに、次期情報セキュリティ基本計画へ向けた「第１次提言」についての報告がなされた。

1. セキュア・ジャパン 2008 の決定

（1）パブリックコメントの結果について

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）（以下、「第１次基本計画」という。）に基づき、各府省庁が実施する施策の年度計画であるセキュア・ジャパンの 3 年目の計画である「セキュア・ジャパン 2008(案)」について、第17回情報セキュリティ政策会議（平成 20 年4月 22 日）においてパブリックコメントに付すことが決定し、下記要領にて１ヶ月間意見の募集を実施。

寄せられたコメントの内容は、施策実施に当たっての要望が多く、セキュア・ジャパン2008自体の大きな修正には至らなかった。

今後、寄せられたコメントをセキュア・ジャパン2008の施策実施をはじめ、情報セキュリティ政策の推進にあたって適切に対応していく。

（2）セキュア・ジャパン2008の決定について

本日決定されたセキュア・ジャパン2008では「セキュア・ジャパン2007」に基づいた取組みへの評価と分析を踏まえ、基本計画の実現に向け「情報セキュリティ基盤の強化に向けた集中的な取組み」をまとめている。

（セキュア・ジャパン 2008 のポイント）

○ セキュリティ対策を推進する体制の維持や、対策が不十分な部分の底上げを含めて対策推進の安定化を図る。

○ 2008 年度に実施する具体的行動計画と、2009 年度の重点施策の方向性を示す。

○ 総施策数 179 施策（内新規 19 施策、継続 138 施策、2009 年度の重点 22 施策）

（パブリックコメント概要）

○ 期間：平成 20 年4月 22 日～5月 22 日

○ コメント総数：63 件（内 2 件は同一コメント）

【内訳 企業・団体 ： 62 件、 個人 ： 1件】

（昨年実施した SJ2007 へのパブリックコメントでは 39 件のコメントが寄せられた。）

○ コメントの概要等： 基本的方向性についての評価・賛意の表明、具体的な施策実施における配慮・要望等に係る意見の提出が中心的であった。

○ 寄せられたコメント（概要・抜粋）

- SBD（Security by design）の検討を加速化すべき。
- 重要インフラ連絡協議会の創設を早急に実現すべき。
- 研究開発に係る産官学の連携を情報セキュリティ全般に広げていただきたい。
- 「安全・安心」がキーワードになっているが、「安全」面に重点が置かれており、「安心」面における課題についても明確にして取組むべき。
- 誤字・脱字の指摘

（別紙 1 参照）

2. 次期情報セキュリティ基本計画策定に向けた「第１次提言」

現在の我が国の情報セキュリティ政策における基本計画である第 1 次基本計画は 2006 年度から 2008 年度までの 3 カ年の計画であるため、2009 年度以降の次期基本計画を定めるべく、「基本計画検討委員会」を設置。平成 20 年 1 月 16 日の第 1 回会合から計 7 回、次期基本計画の理念や目標等について検討、関係者からのヒアリング等を実施。その結果を、主に情報セキュリティ政策の構造と、実施における留意点についてまとめたものとして、「第 1 次提言」を報告。

また、「第 1 次提言」に対し、本日から 1 ヶ月間広く国民から意見を募集し、今後の議論に生かしていく予定。政策の受益者である国民にとって、意味のある情報セキュリティを取りまとめるため、多くの意見をいただけることを期待。

今後、「第 1 次提言」に寄せられたコメント等をもとに、さらに各論について議論を深め、「第 2 次情報セキュリティ基本計画（仮称）」を来年 2 月を目途に取りまとめる予定。

（「第１次提言」のポイント）

○ 「事故前提社会」への対応力強化
　事前予防の継続的な推進に加え、事後対応力の強化を図る。

○ 合理性に裏付けられたアプローチの実現
　情報資産の重要度とリスクの評価（アセスメント）に基づく対策の実施。

○ 成熟した情報セキュリティ立国に向けたITルネッサンス
　より現実に即して実効的な情報セキュリティ対策が冷静に実現され、IT に踊らされず、ITを安全・安心に最大限利活用することができる社会の実現。

（今後の検討スケジュール（予定））

- 平成20年6月19日～7月18日：パブリックコメントの募集
- 平成20年7月下旬以降：概ね月2回の割合で委員会を開催
- 平成20年12月上旬：「第２次基本計画（仮称）」（素案）を情報セキュリティ政策会議に報告。同素案に対するパブリックコメントの募集。
- 平成21年2月上旬：「第２次基本計画（仮称）」を情報セキュリティ政策会議において決定。

（別紙2参照）

【本件に関する問合せ先】
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、安部参事官補佐
電話　03-3581-3768（センター代表）

※ 本日の会議資料は、内閣官房情報セキュリティセンターのホームページにおいて公表します。
（http://www.nisc.go.jp/conference/seisaku/index.html#seisaku18）

※ 「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）

「セキュア・ジャパン2008（案）」に対するパブリックコメントの結果について

経　　緯

第10回情報セキュリティ政策会議（H19.2.2）

○「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（政策会議決定）
○ 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（政策会議了解）

評価等の実施

「情報セキュリティ政策　2007年度の評価等に向けた作業方針」（第14回政策会議（ H19.10.3 ）報告）

第17回情報セキュリティ政策会議（H20.4.22）

○「2007年度の情報セキュリティ政策の評価等
　　－「真の情報セキュリティ先進国」を目指す取組みの2年目の評価－」（評価2007）
　を政策会議に報告。
○「セキュア・ジャパン2008（案）」について審議を実施、パブリックコメントに付すことを決定。

パブリックコメントの結果

■ 実施期間　　：　平成20年4月22日（火）　～　平成20年5月22日（木）
■ コメント総数　　：　63件（内2件は同一のコメント）【内訳　企業・団体　：　62件、　個人　：　1件】
■ コメントの概要等：　基本的方向性についての評価・賛意の表明、施策実施における配慮要望等に係る意見が中心的。

- SBD（Security by design）の検討を加速化すべき。
- 重要インフラ連絡協議会の創設を早急に実現すべき。
- 研究開発に係る産官学の連携を情報セキュリティ全般に広げていただきたい。
- 「安全・安心」がキーワードになっているが、「安全」面に重点が置かれており、「安心」面における課題についても明確にして取組むべき。
- 誤字・脱字の指摘

⇒セキュア・ジャパン2008の施策実施をはじめ、今後の情報セキュリティ政策の推進にあたって適切に対応。

別紙1－1

「セキュア・ジャパン2008」（案）のポイント

- 「セキュア・ジャパン2007」に基づいた取組みへの評価と分析を踏まえ、「第１次情報セキュリティ基本計画」の実現に向けた3年目（最終年度）の取組みをまとめる。
- セキュリティ対策を推進する体制の維持や、対策が不十分な部分の底上げを含めて対策推進の安定化を図る。
- 2008年度に実施する具体的行動計画と、2009年度の重点施策の方向性を示す。

＜基本計画を実現するための取組みの底上げ＞

－「第1次情報セキュリティ基本計画」（2006年度～2008年度）の実現に向け、取組みの底上げを含む三年目（最終年度）の取組み

＜2007年度末の状況認識・評価を踏まえた取組みの方向性＞

- 現行の対策推進体制や対策枠組み、技術水準に照らし限界点に達していると考えられる諸点について、ブレークスルーをもたらす方法を検討
- 中長期にわたり取り組むべき方策、加速化が必要な方策、迅速かつ集中的な取組みが必要な方策を強力に推進
- これまでに整備されてきたツール・体制といった取組基盤を活用し、情報セキュリティ政策の社会的効果（アウトカム）を発現

重点

取組みの方向性

＜「セキュア・ジャパン2008」のポイント＞

電子政府等の情報セキュリティ強化のための総合的な取組み

【主な具体策】
- 「政府機関統一基準」に基づくPDCAサイクルの定着・本格的な評価の推進及び結果の公表
- 電子政府の情報セキュリティを企画・設計段階から確保する（SBD）ための方策の強化
- 政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）の本格運用・能力強化

中期的取組みを必要とする課題への集中的な取組み

【主な具体策】
- 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」のテーマの検討
- アジア地域における情報セキュリティ政策会合の創設
- 分野横断的な情報共有促進のための「重要インフラ連絡協議会(仮称)」創設の促進

持続的な対策の推進体制の構築に向けた基盤整備

【主な具体策】 *→ 2009年度の重点施策の方向性*
- 情報セキュリティ人材の重点確保
- 各専門分野情報共有スキームの連携性及び情報交換モデルに関する検討

別紙1－2

「基本計画検討委員会」の設置について

1．検討のための専門委員会の設置

（1） 3か年の中長期戦略「第1次情報セキュリティ基本計画」は平成20年度（2008年度）が最終年度。

（2） 残された課題
政府機関における情報セキュリティ事故、重要インフラにおけるIT障害の発生などは後を絶たず、企業等における情報セキュリティの具体的な対策や体制作り、人材の確保といった面でも解決すべき課題が多く残されている。

（3） 専門委員会設置
第1次基本計画が最終年度を迎えるにあたり、官民における各種取組み、技術革新や制度改正等を含めた社会環境の変化などを踏まえ、平成21年度（2009年度）からの情報セキュリティ政策の在り方・方向性について検討を行うため、情報セキュリティ政策会議の下に、「基本計画検討委員会」を設置。

2．専門委員会の構成と検討の進め方

（1） 下記のような各分野の者から構成する予定。

（法律分野専門家、技術分野専門家、サプライヤー（SIer、ISP、ベンダー）、ユーザ企業（重要インフラ、大企業、中小企業）、監査関係者（公認会計士）、国家安全保障論専門家、人材育成・資格制度関係者、電子政府・電子自治体専門家、消費者、NPO・NGO、メディア等）

（2） 情報セキュリティ政策会議の有識者構成員は、専門委員会に出席して、意見を述べることができるものとする。
また、専門委員会の検討状況については、適宜、政策会議・有識者会議等に報告するものとする。

別紙2－1

基本計画検討委員会　委員名簿

委員長	須藤　修	東京大学大学院情報学環・学際情報学府教授
委員	有賀　貞一	株式会社CSKホールディングス代表取締役
	井川　陽次郎	読売新聞東京本社論説委員
	井上　雅博	ヤフー株式会社代表取締役社長
	筧　捷彦	早稲田大学理工学術院教授
	木内　里美	大成建設株式会社社長室理事情報企画部長
	重木　昭信	株式会社NTTデータ代表取締役副社長執行役員
	下村　正洋	NPO日本ネットワークセキュリティ協会事務局長
	神保　謙	慶應義塾大学総合政策学部准教授
	関　正樹	関彰商事株式会社代表取締役社長
	高橋　伸子	生活経済ジャーナリスト
	富永　新	日本銀行金融機構局参事役・上席考査役
	中尾　康二	テレコム・アイザック推進会議委員（KDDI株式会社情報セキュリティフェロー）
	深谷　聖治	東日本旅客鉄道株式会社総合企画本部システム企画部長
	満塩　尚史	環境省情報化統括責任者（CIO）補佐官 （各府省情報化統括責任者(CIO)補佐官等連絡会議情報セキュリティワーキンググループリーダー）
	宮地　充子	北陸先端科学技術大学院大学情報科学研究科教授
	三輪　信雄	綜合警備保障株式会社参与
	安冨　潔	慶應義塾大学大学院法務研究科（法科大学院）・法学部教授
	和貝　享介	監査法人トーマツ

このほかに情報セキュリティ政策会議有識者構成員（その代理人を含む）も必要に応じ会議に出席し意見を述べることができる。

別紙2－2

基本計画検討委員会：これまでの検討状況等について

NISC

第1回 【1月16日水曜日　13時00分～15時00分】

- ○ 検討項目例の紹介及び今後のスケジュールについて（事務局説明）
- ○ ヒアリング事項の検討
- ○ 自由討議（各委員意見開陳）

第2回 【2月14日木曜日　15時00分～18時00分】

- ○ 関係者ヒアリングの実施（日弁連／全国市長会（藤沢市）／経団連／重要インフラ専門委員会）
- ○ 自由討議

第3回 【2月21日木曜日　16時00分～19時00分】

- ○ 関係者ヒアリングの実施
  （日本商工会議所／消費者団体（日本消費生活ｱﾄﾞﾊﾞｲｻﾞｰｺﾝｻﾙﾀﾝﾄ協会等）／政府機関（国交省・外務省））
- ○ 自由討議

第4回 【3月19日水曜日　13時00分～16時00分】※政策会議有識者構成員出席

- ○ 第2次情報セキュリティ基本計画の検討範囲の設定
- ○ 大括りの検討項目の設定

第5回 【4月4日金曜日　9時00分～12時00分】

- ○ 大括り項目毎の検討論点の抽出・列挙
- ○ 第1次提言に向けた議論（検討論点毎）

第6回 【5月13日火曜日　17時00分～20時00分】

- ○ 第1次提言に向けた議論（検討論点毎）

第7回 【5月27日火曜日　17時00分～20時00分】

- ○ 第1次提言案の議論

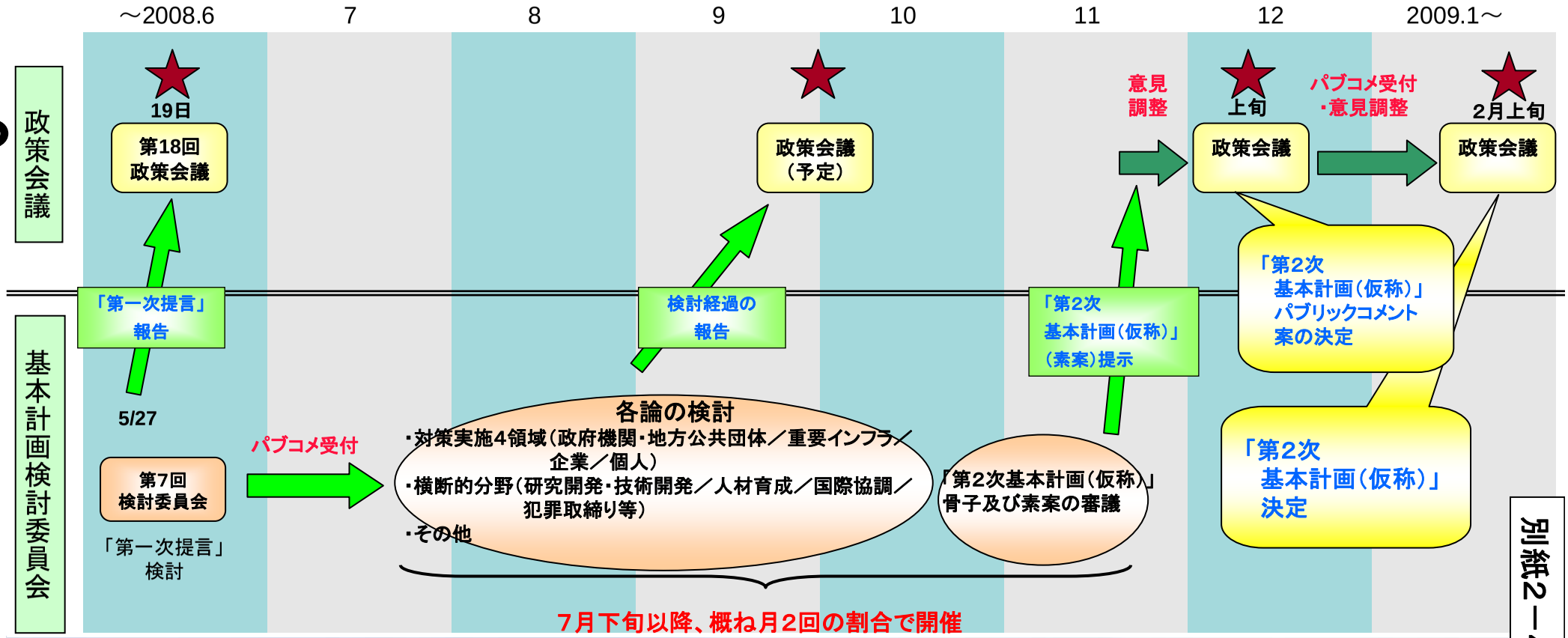
別紙2－3

「第１次提言」策定以後の委員会検討スケジュールについて（案）

○　政策会議への報告後、委員会としてパブリックコメントに付し、広く国民の御意見を伺う。

○　パブリックコメント終了後、その意見内容も踏まえつつ、委員会の検討を再開（７月下旬予定）。年末まで概ね月２回の割合で委員会を開催し、各論の検討を進めていく。

○　12月の政策会議において「第２次情報セキュリティ基本計画（仮称）」のパブリックコメント案を決定、パブリックコメントに付した後、平成21年２月を目途に、「第２次情報セキュリティ基本計画（仮称）」を決定する。



別紙２－４

次期情報セキュリティ基本計画に向けた第１次提言の概要

NISC

第１次情報セキュリティ基本計画

- 我が国の情報セキュリティ政策の立ち上げ
- 「気付きを与える」ための戦略
- 官民各主体のＩＴの安心・安全な利用へ向けた取組み

『情報セキュリティ立国』の思想

高品質・高信頼性・安心安全

『ジャパン・モデル』の確立・世界への展開

『情報セキュリティ先進国』の実現

目指すべき結果

情報セキュリティ上の問題がない水準

「継続」の観点

- 情報セキュリティ上の問題がない水準は目指す
- 各主体最大限の尽力は更に進める
- 対策の推進、水準の向上

「発展」の観点

- 具体的取組みの持続的な推進
- 「事故前提社会」への対応力強化
- 合理性に裏付けられたアプローチの実現

第２次情報セキュリティ基本計画（仮称）

基本理念

『成熟した情報セキュリティ立国』

より現実に即した実効的な情報セキュリティ対策

- 冷静で迅速な対応
- 最適な水準の対策の効果的・効率的な実施
- 説明責任の明確化

ITルネサンス

世界との協調・イニシアティブの発揮

基本目標

「ITを安心して利用可能な環境」の構築

●基本目標に向けて考慮すべき諸点

■「事故前提社会」への対応力強化

・理解（気付き）の推進、判断力の向上
・事後対応への更なる注力
・主体間の共通理解、信頼関係の構築
・事実把握と被害拡大防止・再発防止への情報共有

■ 合理性に裏付けられたアプローチの実現

・脅威の把握、リスクへの柔軟な対応
・コスト・利便性とのバランス
・最適な「水準」に関する認識の共有
・人的側面の対策　・説明責任の明確化

政策の枠組

対策実施主体

政府機関・地方公共団体

- 高機密性情報の保護の方策
- 国民への説明責任の範囲・方法
- 地方公共団体の役割、位置づけ
- 「国立大学法人等」の扱い

重要インフラ

- 一般の「企業」との境界線

企業

- 規模・情報資産活用度による整理
- 海外企業による情報保有への対応

個人

- 「児童・生徒」「高齢者」への目配り
- 「敢えて対策しない者」への対応

主体同士の複合的な形態（上記主体間に限らない）

- 協働によるITサービス提供、他主体によるITサービス提供等の複合的形態での責任分担、規範性の要否

新たなアプローチ

情報提供主体

- 情報の受け渡しに関わる全主体の理解（気付き）
- 自身の情報への所有意識（ownership）⇒ 自身の情報保護、生活・福利厚生への活用

対策支援主体

- 政府機関・地方公共団体
- 教育機関・研究機関
- 情報関連事業者・情報関連非営利組織
- メディア

横断的な情報セキュリティ基盤

- 技術戦略の推進
- 人材の育成・確保
- 国際連携・協調の推進
- 犯罪の取締り及び権利利益の保護・救済

別紙2－6

次期情報セキュリティ基本計画に向けた第１次提言

［概要］

●次期情報セキュリティ基本計画の検討の背景

○ ２００６年度からの３か年の中長期戦略である「第１次情報セキュリティ基本計画（以下「第１次基本計画」という。）」のもと、我が国の情報セキュリティ政策は、着実に進展。

- 取組みは、内閣官房情報セキュリティセンター（ＮＩＳＣ）が主導的な役割
- ２年以上にわたって官民の各主体によって進捗

○ ①これらの取組みの進展や、②第１次基本計画策定後のＩＴの活用方法の変化及びＩＴに対する脅威・リスクの変化などの発生

- ２００９年度以降を念頭に置いた次期の情報セキュリティ基本計画（以下、便宜上「第２次基本計画」という。）の策定に向けた検討を開始。

●第１次基本計画からの「継続」と「発展」

○ 第２次基本計画は、第１次基本計画の「継続」と「発展」の二つの側面を併せ持つべき

- 「継続」の観点からは、情報セキュリティ上の問題が生じないようなセキュリティ水準を実現するべく、各主体が更に前向きに取組むべき
  - ✧ 政府機関など、少なくとも現時点の情報セキュリティ水準が十分であるとは言えず、引き続き対策を推進し、水準を向上することが不可欠な分野も少なくない。
- 「発展」の観点からは、
  - ✧ 第一に、第１次基本計画の下で構築された具体的取組みの下地となる基盤（枠組み）を活用して、取組みを機能させるべき
  - ✧ 第二に、「事故前提社会」への対応力強化を図るべき
    - ● 第１次基本計画が重点を置いた事前予防の取組みによって、事故を完璧に防

止しきるという無謬性の追求は必ずしも容易ではない

- このことへの理解を社会全体で深め、万が一にも情報セキュリティ上の問題が現実となる際に備えることも必要
- あらゆる主体が情報セキュリティ上の問題の発生を防止するべく最大限の努力を行いつつも、事後対応（事業継続性の確保など）にも注力することが必要

✧ 第三に、合理性に裏付けられたアプローチを実現するべき

- 情報資産の重要性とリスクの的確な評価（アセスメント）に基づいて、合理性を担保した形で最適な水準の対策を効果的・効率的に実施することが必要
- 合理性についての客観性を保つため、対策の内容や水準に関する説明責任を果たすことなどが求められる

●第２次基本計画の基本理念について

○ （主要な国家目標である）国民生活、経済活動、安全保障、文化（社会風土）の観点と情報セキュリティ政策の関係

➢ 国民生活面

✧ 国民にとって情報セキュリティ面での支出が不可欠となり、①関連製品やサービスが可能な限り低いコストで提供できる環境を整備するとともに、②国民自身が支出の優先度に係る費目間のバランスを確保しつつ、生活の質（Quality of Life）を向上できるようにすることが必要

➢ 経済活動面

✧ 情報セキュリティに係る取組みは、もはや経営上のガバナンスの一部。顧客からの信頼を確固たるものとし、国際的に競争力を維持・強化するために不可欠な要素

➢ 安全保障面

✧ ①サイバー空間の安心・安全確保は、官、民それぞれの取組みや、官民連携による自発的・協調的な取組みを含めて、様々な主体によって対応。結果、開かれた安全保障と言える状況

✧ ②政府機関（特別管理秘密を扱う場合や、国家の根幹に関わる行政活動を行う

場合）において、合理性に裏付けられた情報セキュリティ対策を進め、機密性の高い情報を守るとともに事業継続性を確保することが重要。対策にあたっては、独自の取組みの必要性と国民に対する説明責任への目配りが必要

- 文化面
  - ✧ 情報セキュリティは、リスクの認識を国民自らが持つことを要求するセキュリティ文化を普及・定着させる。結果、従来、受動的な姿勢でいたとしても、安心・安全な社会において、安心･安全な製品を入手できたという我が国の社会風土を、情報化の進展などにともなって変質しつつある現在の社会情勢に適合

○ 第２次基本計画の下での我が国のあり方

- 第１次基本計画の「セキュリティ」立国の思想（『高品質、高信頼性、安全・安心』の代名詞としての「ジャパン・モデル」の確立と、その世界への展開を視野に入れること）からの発展形を目指すべき
- 無謬性の追求ではなく、『冷静で迅速な対応、最適な水準の対策の効果的・効率的な実施と説明責任の明確化、主体ごとに求められる最適なセキュリティ水準を達成できる高品質や高信頼性、利用者にとっての安心・安全の確保』という概念に基づくべき
- そして、目指すべきは、より現実に即して実効的な情報セキュリティ対策が冷静に実現される「成熟した情報セキュリティ立国」

○ 成熟した情報セキュリティ立国を実現するために（「ＩＴルネサンス」の実現）

- ＩＴに係る技術や制度の側面での対策に加えて、社会や国民の意識改革も不可欠
- 具体的には、（１）人間が必要以上にセキュリティ問題に振り回されず、むしろ、冷静かつ主体的にＩＴを使いこなせるようになること（「ＩＴからの人間性解放」の実現）、（２）結果、最適な水準のセキュリティ対策を実施することで、人間が可能化装置であるＩＴを最大限使って、人間の英知に基づく様々なアイデアの実現が可能化・容易化されること（「ＩＴによる人間性解放」の実現）が必要
- これら二つの人間性解放は、いわば「ＩＴルネサンス」と言うべき取組み

○ 世界との協調

- 我々は自国の取組みに自信を持って世界と協調し、ＩＴ先進国として相応しいイニシアティブを発揮していくべき

●第２次基本計画の下で達成すべき基本目標

○ 第１次基本計画同様、「ＩＴを安心して利用可能な環境」の構築が基本目標

○ これに向けた取組みをより実効的に行う観点から、以下のような諸点の考慮が必要
- 「事故前提社会」への対応力強化の観点から
  - ✧ 理解（気付き）の推進と判断力の向上
  - ✧ 関係の深い主体との間での共通理解の醸成と信頼関係の構築
  - ✧ 障害対応や事業継続性確保などの事後対応への更なる注力
  - ✧ 事実関係の把握機能の強化と説明、及び被害拡大防止と再発防止のための情報共有
- 合理性に裏付けられたアプローチの実現の観点から
  - ✧ 変化し続ける脅威の把握とリスクへの柔軟な対応
  - ✧ コスト、利便性とセキュリティのバランス
  - ✧ 最適な「水準」に関する認識の共有
  - ✧ 情報システムに係る技術面・運用面の対策に加えた、人的側面の対策への更なる尽力
  - ✧ 説明責任の明確化

○ 「新しい官民連携モデル」に基づく取組みの継続と補完
- 取組みの継続
  - ✧ 基本目標の実現に向け、第１次基本計画で構築を図った「新しい官民連携モデル（ＩＴ社会を構成するあらゆる主体が、情報セキュリティ問題への取組みの重要性についての共通の認識の下、自らの責任を自覚しながら、それぞれの立場に応じた適切な役割分担の下で対策を実施する）」に基づく取組みを継続するべき
- 取組みの補完

- ✧ 「事故前提社会」への対応力を強化するとともに、合理性に裏付けられたアプローチを実現する観点から、対策を実施する側（情報管理主体）に加えて、情報を預ける側（情報提供主体）を念頭に置くべき
- ✧ そして、事故の可能性を完全に排除することを目指したとしても、結果がそうはならない可能性があることに対する理解を深める
- ✧ 第２次基本計画の下では、こうした双方の主体を視野に入れて対策を進めるという「２つのアプローチ」を採るべき

●第２次基本計画の下での政策の枠組み

○ 以下のような第１次基本計画の枠組みを基本的に踏襲するべき

- ➢ 対策実施主体
  - ✧ 政府機関・地方公共団体、重要インフラ、企業、個人
- ➢ 問題の理解・解決促進主体（対策支援主体）
  - ✧ 政策実施主体としての政府・地方公共団体、教育機関・研究機関、情報関連事業者・情報関連非営利組織、メディア、
- ➢ 横断的な情報セキュリティ基盤
  - ✧ 技術、人材、国際、犯罪対策

○ 他方、政策をより決め細やかで実効的なものとするべく、また、必要に応じて追加や修正も行うべく、

- ➢ 基本計画検討委員会として引き続き検討を進める必要あり

○ さらに、上述の「２つのアプローチ」の考え方に基づき、情報提供主体を念頭に置いた検討を進めるべき

●第２次基本計画の下での政策推進

○ 第２次基本計画に向けて以下のような検討が必要

- ➢ 政府機関の対策に係る人材、予算などの柔軟な確保のための工夫

- 政府機関を含む公的役割を担った機関総体として、政策の推進にあたって必要な技術的な知見及びそういった知見を有する人材を蓄積・活用できる機能

●第２次基本計画の実効性の確保に向けた今後の検討

○ 第１次提言は、第２次基本計画の総論に係る検討が中心

○ 今後、検討基本計画検討委員会では、各論部分の検討を進める予定。第１次提言・第６章に掲げた検討課題をはじめとする諸論点について、検討を深める