「第２次情報セキュリティ基本計画」（仮称）に係る検討の視点（例）

2008年1月16日（水）

※　本資料は、情報セキュリティ政策会議有識者構成員、基本計画検討委員会委員のコメントなどを取りまとめた段階のものであり、各々のコメントの中には、マクロ・ミクロの様々な視点のものが含まれている。

資料5

検討の視点（概要）　（１）

１．基本認識　（P3～）

○　現在の社会環境とITが果たす役割
- ―　ここ数年の社会環境の変化の特徴、
- ―　ITが社会環境の変化に果たす役割の評価
- ―　ITの社会における位置付け

○　情報セキュリティ政策に関する現状認識と評価
- ―　「IT安心利用環境」の構築という第１次計画の目標をどう考えるか
- ―　確保すべき「IT安心利用環境」の変化
- ―　「IT安心利用環境」の効率的な実現に向けて政府、市場、社会規範、技術が果たす役割
- ―　情報セキュリティの定義
- ―　Preparedness（準備できていること）、Response（対応）、Recovery（回復）という段階で見て、第１次計画の政策の評価

２．総論（P5～）

○　情報セキュリティ政策の理念
- ―　「費用対効果」の視点
- ―　「利便性」の視点
- ―　「不祥事」・「恥」意識から、原因究明による「再発防止」優先への転換
- ―　100%事前防止意識の払拭
- ―　「対策疲れ」と責任限界点の不存在、対策と免責の関係
- ―　「市場原理」の活用
- ―　外部不経済として他者に及ぶ影響
- ―　人的要因による問題発生に対する対策と意識作り
- ―　外部委託のメリット・デメリット
- ―　社会・産業界の円滑な活動維持に加え、国家安全保障
- ―　国際～諸外国の政策との整合性、海外の最善事例の取入れ
- ―　社会変革の予測とそれへの対応

検討の視点（概要）　（２）

○ 第2次基本計画の枠組み
- 主体（政府機関、重要インフラ、企業、個人）の分類の妥当性
- 「重要インフラ」の対象の範囲
- 「企業」の分類の要否
- 「個人」における未成年者、高齢者の扱い
- 大都市と地域の問題
- 他分野（リサイクル、防災、個人情報保護等）との整合性
- 横断的分野（技術、人材、国際、犯罪取締り及び権利利益）の妥当性

3. 各論 （P8～）

○ 政府機関
- 今後どのような政府機関対策が必要か、 対策は、予算面、人員面で十分と言えるのか
- 安全保障・外交等の機密情報を扱う場合の対応、 小規模自治体の対策

○ 重要インフラ
- 事業継続のための情報セキュリティについてどう考えるか

○ 企業
- 企業における対策をどう評価するか。中小企業を対象とした対策は必要か。
- IT提供企業は、情報セキュリティ確保にどのような役割を果たすべきか。

○ 個人
- 個人に対する情報セキュリティ対策をどう評価するか。将来予想される課題をどう考えるか。

○ 技術開発

○ 人材育成

○ 国際連携・協調

○ 犯罪取締り、権利利益の保護・救済

○ その他
- 情報セキュリティ基本法は必要か。情報保護に関する法制度は必要か。外部委託における情報セキュリティ確保のための一般法制度は必要か。

現在の社会環境とＩＴが果たす役割について

現在の社会環境についてどのように認識するのか。そこにおいてITが果たす役割をどのように評価するのか。

1．ここ数年の社会環境の変化は何によって特徴付けられるか。

（例）グローバライゼーションの深化、伝統的価値観からの転換の浸透と一部回帰（文化、国家観など）、
人・モノ・金の移動／移転の高速度化、ビジネス活動の効率化？？

2．ITが社会環境の変化に果たす（果たしてきた）役割はどのように評価されるか。

（例）かつて：大量の事務を効率的かつ正確に処理する手段（単純労働の代替、IT=作業の機械化）

→ 現在：顧客・市場等の経営情報を収集・蓄積・分析し、その効率的活用を図る手段
（頭脳労働の補助、IT=情報の活用）

3．このようなITは社会においてどのような存在として位置付けられるのか。

（例）かつて：社会経済活動をITで効率化／各主体のシステムが単独で機能

→ 現在：社会全体にITが浸透・ITへの依存が拡大／外部のシステムを含めて相互に接続されて機能
社会経済活動の一部がサイバー空間で行われる（電子商取引、WEB2．0）

4．情報セキュリティとして取り組むべき範囲についてどう考えるのか。

情報セキュリティ政策に関する現状認識と評価について

第1次基本計画期間中の我が国の情報セキュリティ政策をどのように評価するか。第1次基本計画以降、どのような環境（IT利用環境、それに伴う社会経済環境）の変化が生じており、政府としてどのように対応していくべきか。

1．第１次情報セキュリティ基本計画の基本目標「ITを安心して利用可能な環境」の構築について、どのように考えるか。

（例）基本計画の対象（スコープ）、メッセージ性、等の観点から。

2．基本計画策定時とのIT利用環境の変化に伴い、確保すべきIT安心利用環境にどのような変化が生じているか。

（例）情報家電、NGN、RFID、オンラインゲーム、SNS、電子マネー等のIT利用を通じ、社会経済活動の変化。

3．IT安心利用環境の最も効率的な実現のために、政府、市場（市場原理）、社会規範、技術が果たす役割についてどう考えるか（これらの要素が働きかける個人をどうとらえるか＝ITを用いて大量の情報を受発信する個人（「覚醒する個人」）への対策）。

4．情報セキュリティの定義（国際的な議論との整合性）についてどのように考えるか。

（例）Cyber SecurityとInformation Security, IT安心利用環境の相違。

5．Preparedness、Response、Recoveryという段階で考えた場合、第1次計画で取り組んでいる政策をどう評価するか。将来必要とされる取組みにはどのようなものがあるか。

情報セキュリティ政策の理念について（１）

情報セキュリティ政策の理念として検討すべきことは何か。また、戦略としてのメッセージ性は必要か。どこに置くべきか。

１.「費用対効果」の視点。

－情報セキュリティ対策の自己目的化の回避。守るべきもののコスト把握は可能か。

２.「利便性」の視点。

－利便性を過度に犠牲にすると現実から遊離しないか。利便性と情報セキュリティの均衡に関する社会的合意形成は可能か。

３.「不祥事」・「恥」意識から原因究明による「再発防止」優先への転換（後掲）。

－「事故・被害隠し」から「情報の共有」へ。隠すのではなく明らかにする方向での意識改革はできるのか。対応に取組むことが「常識」・「良いこと」である文化・社会規範の形成が必要ではないか。

４. １００％事前防止意識の払拭。

－問題発生を前提としたResponse, Recovery段階での対応の明確に意識して準備すべきではないか。

－技術革新が速いこの分野では、「完璧」を求めないという社会的合意を形成すべきではないか。むしろ、失敗しつつも進めていく対応が必要ではないか。

情報セキュリティ政策の理念について（２）

5. 何をどこまで行えば良いか。「対策疲れ」と責任限界点の不存在／対策と免責の関係。

－ベースラインの設定は可能か。リスク管理の体系化により「容認できるリスク」と「容認できないリスク」の仕分けができないか。
－計画段階で目標・達成水準の設定がなければ対策の限界がなくなるのではないか。
－情報セキュリティのレベルについての意識の共有なくして議論できないのではないか。
－ある種の免責がないと対策へのインセンティブが働かないのではないか。
－過度の責任追及は問題の隠蔽につながるという問題意識が必要ではないか。

6. 「市場原理」の活用の視点（特に企業の場合）。

－市場原理が働く領域と働かない領域の仕分けは可能なのか。

7. 外部不経済として他者（顧客・取引先等）に及ぶ影響（社会的コスト）について、どう考えるか。

8. 人間系（運用する人）の問題　［人的要因に対する対策と意識作り］。

9. 外部委託のメリット・デメリットの明確化（後掲）。

10. 社会・産業界の円滑な活動維持の面に加え、国家安全保障の視点（後掲）。

－国が守るべきもの、企業・個人のリスクに任せられないものは何か。

11. 国際の視点、諸外国の政策との整合性、海外の最善事例の取り入れ。

12. 社会変革の予測とその変革への対応という視点。

第２次情報セキュリティ基本計画の枠組みについて

第1次基本計画は、新たな官民連携の構築を掲げ、対策実施領域として、政府、重要インフラ、企業、個人の4領域と、横断的分野として、技術、人材、国際、犯罪対策・権利利益の保護の4つの枠組みを設けている。政策の継続性と環境変化への対応の間でどのような見直しが必要か。

1. どのような分野にどのような目標を設定すべきか。
2. 政府、重要インフラ、企業、個人以外の分類はあるか。
3. 重要インフラの対象拡大は必要か。対象を拡大すると別の問題が生じないか。
4. 「企業」は一括りで良いのか。
   （例）IT利用企業（一般企業）とIT提供企業（機器事業者、ソフトウェア・ASP・SaaS、通信事業者等）に分類
   一般企業をさらに大企業と中小企業に分類
5. 「個人」では、未成年者を別扱いとするべきか。高齢者はどうか。
6. 中身のある外部委託（アウトソーシング）のあり方（専門性の活用、ブラックボックス化の回避、委託先のリスク管理等）。
7. 大都市と地域の問題をどう考えるか。
8. リサイクル、防災、個人情報保護等の他分野の政策との整合性をどう取るか。
9. 横断的分野として新たに取り上げるべき分野はないか。

政府機関・地方公共団体における情報セキュリティ対策について（１）

政府機関等については、政府統一基準とその遵守に係るPDCAサイクルによって、情報セキュリティの確保を図る仕組みを取っているが、今後どのような対応が必要か。

１．政府機関の規模、利用可能な資源などから、よりきめ細かな対応が必要ではないか。

２．統一基準の策定・遵守に加え、各府省庁への助言等の他に対応すべきことはあるか。

３．各府省庁は自らのセキュリティ対策をチェックできる仕組み（監査体制等）が構築できているか。その仕組みを踏まえた上で、各府省庁の対策の評価の仕組みはどうあるべきか。

４．公共性の高い政府機関・地方公共団体は、どの水準まで情報セキュリティを保証するべきか。

５．担当に任せきりの幹部は存在しないか。意識を高めるにはどうすべきか。

６．対策を推進するにあたって、最も効果的かつ健全な政府機関内の体制をどのように考えるべきか。

政府機関・地方公共団体における情報セキュリティ対策について（２）

7. 各政府機関の情報セキュリティ対策は、予算面・人員面で十分といえるのか。
また、担当部署の機関内での位置づけ（ステイタス）はどうあるべきか。

8. 担当者のキャリアパスが必要ではないか。長期的に担当する仕組みが必要ではないか。
各府省とは別の組織を作る案はどうか。各府省庁の実務との乖離や処遇、勤労意欲、
採用面での問題など、多くの新たな課題が生じないか。

9. 安全保障・外交等の機密情報を扱う場合をどうするか。CI（カウンターインテリジェンス）
との関係。

10. 効果的・効率的な対策推進に向けた取組みのパッケージについてどのように考える
べきか。

11. 人材も予算もない小規模自治体の対策をどうするか。

重要インフラにおける情報セキュリティ対策について（１）

国民生活や社会経済活動に不可欠なサービスを提供する重要インフラにおいても、情報システムは不可欠なものになっている。事業継続のための情報セキュリティについて、どのように考えるべきか。

１.「重要インフラ」というカテゴリーの範囲（事業の種類や規模等）をどのように考えるか。また、利用者（国民等）の視点からの「事業継続」をどう考えるか。

２. OECD等の場で議論されている重要情報インフラ（Critical Information Infrastructure）の概念について、我が国としてどのように対応を行っていくか。

３. 重要インフラに係る事業継続性の観点からの情報セキュリティについて、その共通課題と個別課題、及びそれに対する対応をそれぞれどう考えるか。

４. 重要インフラの情報セキュリティ対策について、部分最適と全体最適の差異はあるのか。あるとしてどのような対応が必要か。また「個々の利用者」の視点と「社会全体」の視点との差異はどうか。

重要インフラにおける情報セキュリティ対策について（２）

5. 各業法でカバーしていない部分の情報セキュリティをどうすべきか。民の自主的な取組みによる成果をいかにして確保していくべきか。

6. 重要インフラにおける連携体制が自律的に推進される仕組みは作れないか。

7. 同一分野内では競合関係にある他社との情報共有は可能か。

8. 不祥事意識・「恥の文化」の中、原因究明と再発防止対策（教訓）を１社内でなく広く共有する方法はあるか。

9. 分野を超えた協力を進める上での障害は何か。

10. 重要インフラ分野内での相互作用（システム障害の連鎖等）をどう考えるか。

11. 問題発生に関して、調査報告を行う権限を有する体制（事故調査委員会のようなもの）は必要か。

12. 経営者をはじめ組織全体として、情報セキュリティについて十分な関心を持っているか。

一般企業における情報セキュリティ対策について（１）

我が国の企業における情報セキュリティ対策について、どのように評価するか。将来予想される課題について、どのように考えるか。

１．我が国の企業における情報セキュリティ対策をどのように評価するか。第１次基本計画下における我が国の政策が企業の取組みの向上にどれだけ影響を与えているか。

（例）市場原理の活用（損害情報（コスト）の可視化、情報セキュリティ対策の評価、対策レベルの可視化。

２．情報資産の保護に関する制度や企業コンプライアンスに関連する諸制度が、企業の情報セキュリティ対策の向上に向けてどのようなメリット、デメリットをもたらしているか。

（例）個人情報保護法、知的財産法、J-SOX法、不正競争防止法、等。

３．企業活動がグローバル化、複雑化する中で、政府として情報セキュリティ対策にどのように取り組む必要があるか。

（例）外部委託、オフショアリングの活用、雇用形態の複雑化、人材の流動化がもたらす対策への影響について、等。

４．我が国の競争力維持に向けて企業の技術情報等の重要情報の流出対策をどのように検討すべきか。また、情報セキュリティ対策が競争力強化に貢献する施策をどう進めるか。

一般企業における情報セキュリティ対策について（２）

５．企業におけるレスポンス、リカバリー段階の取組みの現状をどう考えるか。我が国の政策としての取組みをどのように評価するか。

６．システム上のトラブルに関する関係者間の責任（損害の負担）分担のあり方が検討されていないのではないか。他方、様々なトラブルの中で責任分担方式の一般化は可能なのか。

７．企業と従業員との関係（責任分担、懲戒等）をどう考えるか。派遣社員の場合はどうか。

８．経営者にコストがかかり生産性が上がらないという意識はあるか。どう対応すべきか。

中小企業における情報セキュリティ対策について（１）

大企業とは別に、中小企業を対象とした情報セキュリティ政策は必要か。どのような点が特殊なのか。

1. 中小企業における情報セキュリティ対策をどのように評価するか。また、当該分野における政府の役割をどのように考えるべきか。

2. 情報の取扱いに注意すべき点は企業の規模に関係ない。特別扱いすべき、という訳にはいかないのではないか。

3. 中小企業は、情報セキュリティに関する認識（気づき）不足だけでなく、資源（人材、技術、資金）の制約が大きい。中小企業に可能な対策の検討と優先順付けが必要ではないか。

4. 情報セキュリティ対策のために初期投資が大きくなると、ベンチャーが育たない。新たな事業の育成、ベンチャー支援という視点からの対策が必要ではないか。

中小企業における情報セキュリティ対策について（２）

５．情報セキュリティから見た下請け関係の問題はあるか。

（例）大企業の過剰な対応が取引先の中小企業の経営を圧迫している問題（中小企業への無限責任の押し付け）に対し、責任分担のあり方の検討が必要ではないか。

６．損害保険制度は活用できないのか。リスクの見積りが難しいか。

７．独自対策ができない場合には、SaaS等を活用したシステムコストの軽減等を推進することができないか。

ＩＴ提供企業の情報セキュリティ対策における役割について（１）

我が国のIT提供企業は、情報セキュリティの確保にどのような役割を果たしていくべきか。

１．オープン系のシステム（誰でも接続できるインターネットの世界とレガシーシステムと対比する［同一ベンダーに閉じない］意味でのオープンシステムの２種類）の発展は、どのように情報セキュリティ政策に影響してくるのか。

２．外部委託を受ける場合（受託側）に求められるものは何か。

３．ソフトウェアの品質を確保する視点が必要ではないか。バグがあるのは仕方がないという意識で良いのか。品質基準を設定できないか。

４．品質が可視化・明確化されていないために、安全性の評価ができないのではないか。

５．いわゆるITゼネコン（システム構築における多重委託構造）に由来する情報セキュリティ上の問題は何か。どのような対策が必要か。

ＩＴ提供企業の情報セキュリティ対策における役割について（２）

6. ソフトウェアにおいて、パッケージ型の単一製品普及による脆弱性、作り込み型の継ぎ足し化のリスクなどをどう考えるか。

7. セキュリティ対策のビジネスモデルは構築可能か。
（例）企業に対する情報セキュリティ・コンサルタント、企業ネットの監視代行のようなサービス。

8. 売り手・サービス提供者としてのベンダー・ISP等が個人・企業に代わって（ビジネスの一環として）情報セキュリティ強化を担う仕組みをもっと奨励できないか（ベンダー・ISP等による対策の市場原理への組込み方法は？）。

9. 車、携帯電話、情報家電等で使用されるダウンロードで更新可能な「組込まれない組込みソフト」での情報セキュリティ問題をどう考えるか（問題発生時の供給側の責任と権限など）。

10. ベンダー・ISP等は、自己の扱う商品が伴う危険性について、もっと顧客に説明すべきではないか。

個人に対する情報セキュリティ対策について（1）

我が国の個人に対する情報セキュリティ政策について、どのように評価するか。将来予想される課題について、どのように考えるか。

1．現在の個人の普及啓発、教育の取組について、どのように評価するか。政府としての役割についてどのように評価するか。その他の主体（非政府組織、教育機関、研究機関、メディア等）による取組みについて、どのように評価するか。

（例）情報セキュリティの日、安心利用のための教室、等

2．膨大な数の個人に対する啓発手段とその浸透方法について、どうすべきか。

3．情報関連製品、サービスを提供する事業者による消費者保護の取組みについて、どのように評価するか。事業者の取組みを支援する立場として、政府にどのような役割を期待するか。

4．個人に対する情報セキュリティ政策として、インターネット上の違法・有害コンテンツ対策を盛り込むべきか。

個人に対する情報セキュリティ対策について（2）

5．IT利用率が低いユーザーや情報セキュリティに無関心な個人に対する情報セキュリティ対策をどのように考えるか。

（例）個人の情報セキュリティ対策に対してマイレージやポイント付与を考えられないか、等

6．生体認証の活用のあり方。変更が不可能なので、多数が利用するシステムに用いるのは新たなリスクを生むのではないか。

7．国家の安全保障と個人の権利とのバランスについて、どのように考えるか。

（例）テロ対策のための情報収集と個人のプライバシー保護、通信の秘密のバランスについて、等

8．個人のIT安心利用環境のための制度、技術（フィルタリング、認証制度等）と、既存のネットワークのアーキテクチャ（コンテンツの開放、匿名性等）との関係について、どのように考えるか。

9．基本計画で描かれていない主体による個人対策にはどのようなものがあるか。

情報セキュリティ分野における技術開発の取組みについて（１）

情報セキュリティ分野における技術開発の取組みについて、どのように評価するか。

１．情報セキュリティ分野における政府の技術開発戦略と我が国の情報セキュリティ技術向上との関係をどのように評価するか。

２．成果利用までを見据えた技術開発戦略による投資効率の向上について、我が国の取組みをどのように評価するか。

３．グランドチャレンジ型の研究開発・技術開発を通じた情報セキュリティ技術の向上という目標設定と効果をどのように考えるか。

４．情報セキュリティ分野における技術開発戦略と我が国のIT分野における競争戦略との関係をどのように考えるか。

５．情報セキュリティ技術開発の重点化と環境整備の在り方をどのように考えるか。

情報セキュリティ分野における技術開発の取組について（２）

6. 研究開発実施把握のあり方（公的研究機関、民間）をどう考えるか。

7. 公的資金の重点的投入方法のあり方をどう考えるか。

8. 民間との役割分担のあり方をどう考えるか。

9. 新たな学際領域への取組み拡大をどう考えるか。

10. 研究成果の政府による活用についてどう考えるか。

情報セキュリティ分野における人材育成について（１）

我が国の情報セキュリティ分野における人材育成について、どのように評価するか。

１．我が国で情報セキュリティに関わる人材の現状（質、量、分布など）について、どのように評価するか。第１次基本計画策定からどのような変化が見られるか。

２．社会のIT化が進展する中で、情報セキュリティに関わる人材の範囲をどのように捉え、どこまでを人材政策のターゲットとすべきか。

３．官・民・学により様々な情報セキュリティに関する教育プログラムが提供されているが、これまでの実績・効果をどう評価するか。どのような点について改善が求められるのか。

（例）大学・大学院が提供する学生・社会人向けプログラム、各種資格制度、研修事業に対する財政支援、等

４．情報システムや製品を提供する企業等においては、どのような人材の育成・確保が求められるか。

（例）多重委託構造でのシステムの信頼性確保、等

情報セキュリティ分野における人材育成について（２）

５．組織（行政機関や企業）において情報システム管理やセキュリティ対策に従事する者の処遇・キャリアパスや組織全体から見た経営資源の割り当て（要員の配置、研修等）の現状をどう評価するか。Risk Managementの観点から見て妥当か。

６．規模の小さな組織や地方などにおける人材確保のために必要な政府・業界の取組みをどのように考えたらよいか。

情報セキュリティ分野における
国際連携・協調の推進に向けた取組みについて

我が国における情報セキュリティ政策に関する国際的な取組みについて、どのように評価するか

1. 我が国の情報セキュリティ政策と国際機関（OECD, APEC, ITU等）での取組みとの整合性について、どのように考えるか。

2. 世界の中でIT先進国としての日本の立場から、現状の国際的な取組み、情報発信等の現状についてどのように評価するか。どのような分野での情報発信が必要か。

3. ITを利用した社会経済活動が国境を越えるにつれて、情報セキュリティ政策が我が国の競争力向上への取組みにどのように貢献すると考えるか。

4. 情報セキュリティの分野でも、数多くの標準化作業が行われているが、我が国の政府機関、企業等の現状の取組みについて、どのように評価するか。

5. 国境を越えたサイバー攻撃への対応等の国家安全保障的な課題について、我が国としての取組みをどのように評価するか。

情報セキュリティ分野における
犯罪の取締り、権利利益の保護・救済について

情報セキュリティ分野における犯罪の取締り、権利利益の保護・救済のための我が国の取組みについて、どのように評価するか。

1. サイバー犯罪の取締りの現状について、どのように評価するか。今後想定されるサイバー犯罪の増加・巧妙化に対して、どのような取組みを進めて行くべきか。

（例）実体法及び手続法の整備状況、国際協力の必要性（サイバー犯罪条約の批准）、取締りの実績、等。

2. サイバー犯罪の取締りの強化を可能とする制度がネットワーク利用環境に与える影響について、どのように考えるか。

（例）追跡可能性の確保と通信の秘密、フィルタリングの導入とコンテンツ開放（表現の自由）、ログの保存と通信の秘密、プロバイダ制限責任法と損害賠償制度、等。

3. 情報セキュリティ基本計画の対象となるサイバー空間において保護・救済されるべき権利利益をどのように考えるか。既存の法制度との関係をどのように考えるか。

（例）個人情報、名誉、プライバシー、知的財産権、新たな権利としての情報セキュリティ権。

4. 現状のサイバー空間における権利利益の保護・救済のための制度について、どのように評価するか。今後の取組の可能性についてどう考えるか。

（例）ADRの設置、企業に対する消費者保護強化の徹底、等。

その他の検討の視点（１）

その他として、どのようなものの検討が必要か。

１.「情報セキュリティ基本法」は必要か。必要だとすればどのような内容を盛り込むべきか。他方、抽象的な基本法を作るために費やす資源があれば、その分を具体的な対策に費やす方が費用対効果の点で良いのではないか。また、IT基本法の条項を拡充する改正も考えられるのではないか。

２. 情報保護に関する一般的な法制度（罰則を含む）は必要か。必要とするならば、対象は政府のみか、民間（企業秘密など）も含めるのか。

　他方、個人情報保護、知的財産などの個々の情報の性格に着目した個別法との関係が難しいのではないか。適切な情報の分類（格付）はできるのか。

３. 外部委託における情報セキュリティ確保のための一般法制度は必要か。必要とするならば、対象は政府のみで足りるか。個別法による守秘義務やみなし公務員規定、契約による担保で足りるか。

その他の検討の視点（２）

４．安全性と利便性のバランスが取れた最善事例を収集・分析して広く提供すれば広まっていくのではないか。

５．情報セキュリティに関係する様々な法律が作られているが、その体系化・整合性の確保がなされているのか。

６．法制度だけでなく、社会規範やセキュリティ文化の醸成、人々の「常識」化をどのように進めていくべきか。

７．位置情報のあり方（プライバシー、米国依存など）をどう考えるか。

８．情報セキュリティの分野での被害が見えにくくなっているため、社会に対するメッセージ性が小さくなっている。どのようにして認識を高めるか。

８．次期基本計画が対象とする期間はいつまでとすべきか。（第１次基本計画は３年間）

９．情報セキュリティ政策の推進体制をどう考えるか。（情報セキュリティ政策会議・内閣官房情報セキュリティセンターのあり方、各府省の役割など）