参考資料2

「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）

【重要インフラ関連部分抜粋】

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。

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。

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。