参考資料2

次期情報セキュリティ基本計画に向けた
第1次提言

情報セキュリティ政策会議
基本計画検討委員会
2008年6月19日

「次期情報セキュリティ基本計画に向けた第一次提言」をまとめるに当たって

基本計画検討委員会　委員長
須藤　修

わが国におけるＩＴ（情報通信技術）の利用・活用は、新たな段階に入り始めている。２００１年の「e-Japan 戦略」では、世界最先端の IT 国家を目指し、ＩＴの社会導入を積極的に推進する政策プログラムであった。その後、２００５年の「ＩＴ新改革戦略」においては、ＩＴの社会導入は広く実現されたとの認識が示され、従来から認知されていたＩＴによる生産性改善、コスト削減効果を期待するだけではなく、ＩＴを汎用的な可能化装置と捉え、その積極的な活用で生み出される、さまざまな創造的成果の獲得も政策目標に組み入れられた。さらに、「ＩＴ新改革戦略」策定時点からさらに３年が経過した現在、ＩＴの社会基盤化が進むとともに、ほぼ全ての産業でＩＴがビジネスを駆動する状況となり、近年の情報サービスは、急激な進化を遂げている。

この状況は、情報セキュリティに新たな課題を生み出している。

一つは、これまでの情報セキュリティの「常識」が通じない状況が増えてきたことだ。その典型例として、組織境界を越えて情報を積極的に交換することで、新しいサービスを構成することが当たり前になってきていることが挙げられる。ＳＣＭシステムやＢ２ＢのＥＣシステムでは、組織境界を越えた情報交換が急速に進みつつある。さらに、クラウドコンピューティングやマッシュアップなどの新しい情報サービス構成スキームは、他者が提供するサービスをも取り込んで情報システムを構成することが当たり前となる。このような、新たなサービス構成方法は、これまでの情報セキュリティでの「常識」が通じないものであり、新たな技術、新たな管理手法、新たな常識を生み出し、社会に展開しなければならない。

二つ目は、情報システムが企業、組織、個人の活動を広く支える構造により、リスク管理の対象として、情報システムを本格的に組み入れる必要がでてきたことだ。ところが、知見不足、人的資源不足から、そのための計画策定が困難であることなどが明らかになり始めている。特に、大規模災害発生時の情報システムの取扱いや、個人情報漏洩などの新種のリスク増大に対応する時に、投資合理性を確保するとともに、ＩＴ活用のメリットを維持しつつ、同時に十分なセキュリティ対策を実施することに苦労している組織も多い。しかし、単に

「○○は禁止」といった単調な対応・対策では、ＩＴから得られるメリットを放棄するだけでなく、組織構成員のモラルハザードを起こす可能性もある。このため、知恵、知力を最大限動員して、ＩＴに関するリスク管理を実現しなければならない。

三つ目は、情報セキュリティの課題の多くは、その解決のために、複数かつ重層的な施策の実施を要求するものであることだ。これは、そもそも問題が固定してない、つまり、リスクは変化するものであり、変化に応じて対応を機動的に行う必要があることに起因する。リスク変化は、異なる時係数を持った構成要素の収斂によって発現する。したがって、異なる時係数を持つ、複数の重層的な対策を要求するのは自明である。しかし、政府を含めた多くの組織において、時係数の異なる複数の重層的な対策を調和的に実施することは困難を極める。これまでの組織構成は、問題を分割し、個別に解決方法を生み出すことに最適化されており、変化する問題に対して、複数の組織内ユニットが機動的に、かつ、調和的に対応する構造とはなっていないのだ。

我が国においては、２００６年、情報セキュリティ政策会議が２００８年度までの国家戦略を描いた「第１次情報セキュリティ基本計画」を決定し、政府全体として本格的な対策が始まった。しかし、この基本計画は、国全体として調和ある対策実施を始める第一歩としての意味はあったが、ここ数年の情報システムの進化によって明らかになった新たな課題には十分対応しているとは言えないのではないか。

現在、２００９年度以降の政策の在り方を総合的に検討する場として、基本計画検討委員会が設置されている。私は、その委員長として、委員諸氏とともに体系的な戦略の構築に尽力している。特に、「第１次情報セキュリティ基本計画」の成果を評価しつつ、先に述べた新たな課題をどのように解決するのかを、委員諸氏に積極的に議論してもらうよう運営し、今般、この「第一次提言」としてまとめることができた。

「第一次提言」は、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、かなり踏み込んだ形でまとめることができた。特に、情報セキュリティ基本計画は政府における政策プログラムであることから、政府が何をなすべきであるかという点だけでなく、政策の受益者、特に国民からの視点での政策構造の在り方にも留意している。さらに、社会における積極的な情報交換によるサービス構成の広がりにも対応している。

「第一次提言」をまとめる過程で、多くの委員が述べたのは、わが国がＩＴに関係する多種多様なリスクに対して、リスク低減を積極的に行い、仮にリス

クが顕在化したとしても、柔軟に対応することができるようになる社会を目指すことが重要だということであった。この提言では、これを表す「事故前提社会」という言葉を使っている。しかし、これは事故が起きることに対するあきらめを表明するものではない。事故発生を積極的に抑えることに努力し、そして、仮に事故が発生しても、その影響を最小化するための対応をしなやかになせることを表しているのだ。

また、情報セキュリティ対策の合理性追求が大きな課題であることも、委員会において何度も議論された。過度の情報セキュリティ対策の実施は、利用者のモラルハザードを誘発する可能性がある。一方、情報セキュリティ対策が過小投資状態になることも避けなければならない。このため、リスクアセスメント結果に応じた効果的な対策実施が求められるが、適切投資を判断するための組織力、あるいは、組織内人的資源の強化も併せて行わなければならない。

この観点から、特に現在の政府機関における情報セキュリティ対策については、民間の最先端の動向を参照しつつ向上させ、将来的には政府における情報セキュリティ対策が世の中の手本となるように、さらに積極的な取組みを展開する必要がある。迅速かつ国民に有用な電子政府構築を目指している現在、情報セキュリティについても、政府は取組みの拡大が必要である。

さらに、ＩＴを活用する個人の力をどのように伸ばすかも課題であろう。社会基盤化する現在のＩＴは、情報セキュリティの観点からはＩＴを使う個人の強い判断力を要求する。このためには、ＩＴを活用する個人が、情報セキュリティについて能動的かつ主体的な行動をすることができるようにするためにはどのようにしたらよいか。さらに、そのような行動をとれない個人に対しても、提供される IT 側でセーフティネットのような機能を持つようにするにはどうしたらよいのか。このような観点からの議論も、継続的に必要であることも、委員会では議論された。

この「第一次提言」は、現時点までの議論をまとめたものであり、最終的な政策プログラムまでは、より多くの検討、議論、調整が必要である。このプロセスにおいて、多くの意見を頂き、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政策をとりまとめることが必要である。多くの意見をいただけることを期待したい。

今回、これまでの検討状況を「第一次提言」の形で取りまとめ、情報セキュリティ政策会議に報告する取り運びとなったことは大変喜ばしい。多くの時間を割いた委員諸氏に感謝するともに今後も活発な議論をお願いし、私の序文に代えさせていただきたい。

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

目次

はじめに

(1)　次期情報セキュリティ基本計画の検討の背景

我が国の情報セキュリティ問題への取組みは、２００５年４月に内閣官房に情報セキュリティセンター（以下「ＮＩＳＣ[1]」という。）が、同年５月に高度情報通信ネットワーク社会推進戦略本部（以下「ＩＴ戦略本部」という。）に情報セキュリティ政策会議が設置され、抜本的な強化が開始された。

具体的な強化策は、e-Japan重点計画等の一部となっている「情報セキュリティ」の問題を個別重点的に捉えた上で、戦略的思考に基づいた体系的な計画を構築すること、すなわち、２００６年度から２００８年度までの３か年の中長期の戦略である第１次情報セキュリティ基本計画[2]（以下「第１次基本計画」という。）の策定という形で結実した。

これ以降、ＮＩＳＣが主導的な役割を担う形で、官民の各主体によって２年以上にわたって様々な取組みが進められ、対策は着実に進展してきた。

一方、昨今の社会情勢を見ると、証券取引システムや金融機関の現金自動預け払い機、自動改札システム等におけるＩＴ障害の発生、不正アクセスによるカード情報の大量窃取、ファイル共有ソフト及びコンピュータ・ウィルスによる重要情報の漏えいなど、もはや社会基盤化したと言える情報技術（以下「ＩＴ」という。）を利活用する上でのリスクは依然として存在している。また、ボットネット等による脅威の深刻化や、ソーシャルエンジニアリングを駆使し、特定の組織・個人を狙う標的型攻撃（スピア型攻撃）のような新たな攻撃手法など、新たなリスクも日々発生している。さらに、社会におけるＩＴの活用方法は、例えば、地上波デジタル放送の展開とともに、家電利用におけるネットワーク活用が国民生活にとって極めて重要になってきていることや、カーナビのネットワーク接続の進展が一般的になっていること、日常生活で必要な行政手続の電子化推進など、年々進化を遂げ、第１次基本計画策定時とは大きく変化している。こうした状況に連動して、情報セキュリティが対象とするべき事項も変化してきている。

このため、第１次基本計画に基づく各種の取組みの進展や社会環境の変化などを踏まえ、引き続き我が国全体として情報セキュリティ問題への取組みを力強く推進するために、２００９年度以降を念頭に置いた次期の情報セキュリテ

---

1 National Information Security Centerの略。

2 ２００６年２月２日　情報セキュリティ政策会議決定。

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した。

⑵　第2次情報セキュリティ基本計画の検討体制

第２次基本計画の検討にあたっては、２００７年１２月に情報セキュリティ政策会議の下に、基本計画検討委員会（以下「検討委員会」という。）が設置され、第２次基本計画の策定に必要な情報セキュリティ政策のあり方及び方向性に関して、１９名の委員で検討を行うこととなった（参照：別添１）。

⑶　第2次情報セキュリティ基本計画の検討過程における第1次提言の位置付け

第２次基本計画の検討は、２００８年１月以降、随時、検討委員会が開催され、同年６月までの７回の会合において、様々な論点の検討が行われた。

７回の会合のうち、第２回、第３回においては、日本弁護士連合会、神奈川県藤沢市、日本経団連、情報セキュリティ政策会議重要インフラ専門委員会、日本商工会議所、消費者関連団体（主婦連合会、東京都地域婦人団体連盟、全国消費者団体連絡会、日本消費生活アドバイザー・コンサルタント協会)、国土交通省、外務省といった各分野を代表する様々な主体（ヒアリング順）からのヒアリングを実施した。本文書（以下「第１次提言」という。）は、こうした各主体からの意見なども踏まえ、７回の議論の総括としてとりまとめたものであり、第２次基本計画の策定に向けた中間的な提言である。

基本計画検討委員会における第１次提言までの検討は、メッセージや、理念・哲学など、第２次基本計画の大きな方向性に係る部分を中心に行った。検討にあたっては、第１次基本計画の下で様々な施策を実施した状況を踏まえ、２００９年度から先の将来に、我が国が情報セキュリティの観点からどのようにあるべきかといった大局的な観点から集中的な議論を行った。すなわち、第１次提言は、主として具体的な施策の方向性などを検討する前の、計画の根幹部分に関する委員会としての考えをとりまとめたものである。

⑷　今後の検討について

基本計画検討委員会は、第１次提言を情報セキュリティ政策会議に報告を行なうこととしており、第１次提言については、政策会議による議論を経た後に、

今後の検討の重要な参考とするべく、国民全般から意見が募集される予定である。

その後、検討委員会としては、２００８年７月を目途に検討を再開し、様々な意見などを踏まえながら、重点政策の方向性について議論を深めていくこととなる。

第1章　第1次情報セキュリティ基本計画と第2次情報セキュリティ基本計画の関係

(1)　第1次情報セキュリティ基本計画の下での取組みと第2次情報セキュリティ基本計画の位置付け

①　第1次情報セキュリティ基本計画の下での取組み

第１次基本計画は、言わば、我が国における情報セキュリティ政策の立上げと、全ての主体にとっての「気付きを与える」ための戦略であった。我が国は、第１次基本計画によって、情報セキュリティをＩＴ関連の政策の中でも個別重点的な政策分野として立ち上げ、以降、政府機関・地方公共団体、重要インフラ、企業、個人といった官民の各主体が、国民生活・社会経済活動において依存度が高まってきているＩＴの安心・安全な利用を可能とするべく、知見を集中し、様々な主体ごとに取組みを進めてきた。

具体的には、官民の各主体は、高品質[3]、高信頼性[4]、安心・安全を実現するために、情報セキュリティ上の問題が生じない水準[5]までの結果を目指し、毎年度の年度計画である「セキュア・ジャパン」に基づいて積極的に取組みを進めてきた。結果、２００７年度までの取組み[6]及び２００８年度の取組みの見込みを踏まえると、第１次基本計画に基づく取組みは、おおむね当初の計画どおり実現できてきていると考えられる。

しかし、現実の社会情勢を見ると、情報セキュリティ確保のための取組みは着実に進む一方で、情報セキュリティ上のリスクは減少しているとは必ずしも

---

3 例えば、バグが発生しないとか、想定外の操作に対しても何らかの対応が可能なことが挙げられる。

4 例えば、攻撃などによって負荷がかかっても止まりにくい、壊れにくいという状態や、止まったり、壊れたりしても迅速に復旧できることが挙げられる。

5 政府機関に関しては「１）２００８年までに政府機関統一基準のレベルを世界最高水準のものとし、かつ２）２００９年初めには、すべての政府機関において、政府機関統一基準が求める水準の対策を実施していることを目指し」、重要インフラに関しては「２００９年度初めには、重要インフラにおけるＩＴ障害の発生を限りなくゼロにすることを目指し」、企業に関しては、「２００９年度初めには、企業における情報セキュリティ対策の実施状況を世界トップクラスの水準にすることを目指し」、個人に関しては「２００９年度初めには、「ＩＴ利用に不安を感じる」とする個人を限りなくゼロにすることを目指」すこととされている。

6 ２００７年度までの取組みでは、第１次基本計画に基づいた３年間のＰＤＣＡサイクル及び年度計画に基づいた１年間のＰＤＣＡサイクルを構築し、政策・対策の実施・評価を行ってきた。具体的には、例えば政府機関分野では政府機関統一基準に基づく対策の実施・評価等や「政府機関情報セキュリティ横断監視・即応調整チーム（ＧＳＯＣ）」の整備、重要インフラ分野では行動計画に基づく取組みなどを推進した。また、横断的な情報セキュリティ基盤分野では、技術戦略専門委員会や人材育成・確保専門委員会で一定の提言を示すとともに、これに基づく取組みの推進、国際連携・協調に関しては今後の活動の基本方針の策定を行い、取組みを本格的に始動した。

言えない。これは、第１次基本計画に基づく包括的な情報セキュリティの取組みは有効であるものの、取組みの開始から２年間が過ぎたにすぎない現時点では、単に政策の社会的効果（アウトカム）が現れるまでにタイムラグがあるということかもしれない。しかし、少なくとも、ＩＴの社会基盤化の更なる進展やサイバー攻撃の巧妙化などによって、より目に見えにくく、より大規模なサイバー攻撃やＩＴ障害の発生の可能性へと問題が変質し始めているということは明らかである。

こうした課題への対応については、まずは、第１次基本計画の下での３年目の取組みを着実に進めることが不可欠である。

また、より根本的な対応として、第１次基本計画の下での取組みを、現実を踏まえつつ精緻な検討を更に行うことで、より良いものとする余地があると考えられる。

さらに、第１次基本計画の下で、情報セキュリティ上の問題が生じない水準、すなわち、特に事前予防に焦点を当てて無謬性[7]の追求と言っても過言ではない水準の取組みを目指した点について、事後対応にも十分な目配りを行うことも重要である。こうすることで、情報セキュリティ政策が我が国社会にとって、より有用なものへと発展し、情報セキュリティ上のリスクを減少させる上で、更に大きな効果を発揮する可能性が十分にある。ただし、政府機関における情報セキュリティ対策のように、国民全体からの信頼維持の観点から、事前予防の重要度が特に高いものについて、引き続き留意することも不可欠である。

② 第2次情報セキュリティ基本計画の位置付け

以上を踏まえ、第２次基本計画は、情報セキュリティ政策をより現実に即して実効的な政策、すなわち課題の把握から事前の対策、さらには問題が発生した際の解決までの一連の対応能力が高い政策へ発展させるために、引き続き我が国全体を俯瞰した中長期的な戦略とするべきである。第２次基本計画が、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であることは自明である。

⑵　第1次情報セキュリティ基本計画からの「継続」と「発展」

[7] 本文書において、「無謬性」とは、一切誤りはなく完璧であることを意味する。情報セキュリティ分野において、重要な要素としてしばしば挙げられるintegrity（完全性：情報や情報の処理方法が、正確で完全であるようにすること）を意味するわけではない。

第１次基本計画の「継続」の観点からは、第２次基本計画は、基本的に第１次基本計画の精神を継承すべきである。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については、第２次基本計画の下でも引き続き実現されることが望ましい。その実現に向けて各主体が最大限尽力するべきであることについては、更に前向きに取組む必要がある。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て水準を向上することが不可欠な状況である。

他方、情報セキュリティに係るリスクの状況に鑑みると、上述のような情報セキュリティ上の問題が生じない水準の事前予防を実現することは、実現可能性や、結果を追求するためのコスト及びセキュリティの確保と引換えになる可能性のある利便性とのバランスの観点から、現実には容易でない[8]。このことを十分に考慮しつつ、情報セキュリティ政策をより充実するには、事前予防を中心とする従来の取組みを引き続き着実に推進するとともに、従来よりも柔軟で、現実に即した対策を実施できる政策体系の構築が効果的であると考えられる。

したがって、第１次基本計画の「発展」の観点からは、日々変化する情報セキュリティに係るリスクが現実化する可能性も念頭に置き、その際に様々な主体がより実際的な対応をとるという観点に十分に目配りすることが必要である。

第２次基本計画は、第１次基本計画を以下の３つの観点に基づいて継続・発展させるべきである。

① 具体的取組みの持続的な推進

第一に、第２次基本計画の下でも、各々の主体が、持続的に努力を継続する必要があることは言うまでもない。

他方、第１次基本計画の下での取組みは、情報セキュリティ分野の立上げ期ということもあり、具体的取組みの下地となる基盤（枠組み）作りが少なくなかった[9]。第２次基本計画では、第１次計画の下で構築された基盤（枠組み）を

---

8 「情報セキュリティ上の問題が生じない水準の事前予防」の実現が、「現実には容易ではない」としている趣旨は、「どれほど対策を実施したとしても、失敗や問題が生じることはあり得る（完璧であるという結果の実現は難しい）ということを認める、すなわち容認せざるを得ないリスクは存在し、これをacceptable riskとして捉える」という意味であり、「必要な対策を行う体制や対策の内容などの改善を含め、対策を徹底的に行うことは容易ではない（ゆえに、適切な水準の対策であっても対策の徹底を行わなくても良い。）という意味ではない。基本計画検討委員会として、「適切な水準の対策については徹底するべき」、という考えであることについては、ここに改めて強調する。

9 例えば、政府機関の横断的監視・即応体制の整備や、重要インフラのＣＥＰＴＯＡＲ－Council創設に向

活用し、具体的取組みを機能させていくことが重要である。

以上から、具体的取組みの持続的な推進が重要である[10]。

② 「事故前提社会」への対応力強化

第二に、より実際的な視点に立ち、事前予防の取組みにもかかわらず情報セキュリティ上の問題が生じた際に、迅速かつ実効的に対応することで、事業継続性などを確保することが必要である。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、それでも万が一の事態が有り得ることを認識し、これに向けた準備を怠らないとともに、万が一の事態においては事実関係を明らかにできるよう取組むこと、すなわち「事故前提社会」への対応力強化が重要である。

ここで、「事故前提社会」とは、事故が有り得るから諦めて事前予防に向けた対策を行なわないとか、どのような被害にあっても、それは仕方ないものであると諦めさせるとかいうことを意味するものでは決してない。

「事故前提社会」への対応力強化に向けては、事故の可能性を完全に排除することを目的とした、完璧な情報セキュリティ対策の実現は容易ではないという点に関する理解（気付き）を社会全体で増進する必要がある。また、万が一問題が顕在化しても、気付きを持って自ら考える主体が過敏な反応を起こさず、事実を冷静に受け止めて適切な対応を迅速に行うための取組みが不可欠である。別の言い方をするならば、万が一問題が発生したとしても適切に対処すること、つまり、発生した問題に対して許容可能な水準を、各々の主体ごとに定めていくこと、あるいは我が国として設定していくことの実現が必要である。

③ 合理性に裏付けられたアプローチの実現

第三に、「事故前提社会」において、最適な水準（常に変化し続けるリスク[11]に柔軟に対応し、各々の主体及び社会全体にとって客観的に許容可能な範囲内

けた検討、人材育成分野における官民連携の協議会創設に向けた取組み、国際会議における新たな会議創設の提案などが挙げられる。

10 なお、政府機関の情報セキュリティ対策のための統一基準（以下「政府機関統一基準」という。）に基づく対策など、依然取組みを強化することが必要な水準であるとは考えられるものの、短期間で一定の状況改善を実現できたものも存在している。これらについては、的確な対策を持続的に実施しつつ、ＩＴを巡る技術革新や社会制度の変化等を踏まえ、柔軟に対策の修正・向上を図っていくことが必要である。

11事故前提社会では、脅威によってリスクが現実のものとなり得る事態を想定し、リスクを予見・予防するとともに、生じる損害や障害を極力小さくするべく、対処の手立てなどを検討するというリスク・マネジメント手法が重要となる。

にリスクを管理できる水準）の対策を効果的・効率的に実施すること[12]、すなわち合理性に裏付けられたアプローチの実現が重要である。なお、アプローチの合理性についての客観性を保つため、併せて対策の内容や水準に関する説明責任などを確実に果たすことが求められる。

具体的には、リスクの把握と変化するリスクへの柔軟な対応を行う機能の強化や、最適な対策水準の設定、説明責任の明確化といった取組みを実現するべきである。

[12] より具体的には、情報資産の重要性とリスクの的確な評価（アセスメント）に応じた対策を確実に実施することを意味する。

第2章　第2次情報セキュリティ基本計画の基本理念（我が国のあり方）について

(1)　我が国の国家目標と情報セキュリティ

①　第1次情報セキュリティ基本計画の下での位置付け

第２次基本計画の基本理念（我が国のあり方）を検討するにあたって、そもそも我が国の国家目標との関係で情報セキュリティ政策がどのように位置付けられるのか、改めて整理する。

第１次基本計画では、「ＩＴの利活用と国家目標の実現」との関係で情報セキュリティの位置付けが述べられている。具体的には、１）ＩＴの利活用を通じた経済の持続的発展[13]、２）ＩＴの利活用を通じたより良い国民生活の実現[14]、３）ＩＴの利活用によって発生する脅威からの安全保障[15]に関連し、情報セキュリティを「ＩＴ基盤を、真に依存可能で強固なものにする」ためのものとして位置付けている。

また、「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[16]」においては、ＩＴ利活用を通じた文化創造や文化発信の機能といった、文化との関係で、情報セキュリティの取組みの必要性について言及がなされている。

---

13 経済大国日本の持続的発展とＩＴの利用・活用との関係で、「・・・企業活動のグローバル化と分散化に対応して、強固な国際競争力と高い生産性を維持するためには、ＩＴの利用・活用 が不可欠であるということは言うまでもない。ＩＴを社会インフラとして他国以上に一層有効に使いこなし、我が国の経済活動の持続的発展を遂げることが重要な国家目標である。」 とされている。

14 より良い国民生活の実現とＩＴの利用・活用との関係で、「経済活動だけではなく、２１世紀の我が国が直面する社会問題の解決のためにも、ＩＴの利用・活用が不可欠となり始めている。・・・ＩＴを重要な手段として利用・活用し、我が国が直面する社会問題を解決し、安全・安心で、より良い国民生活を実現していくことが重要な国家目標である。」とされている。

15 我が国の安全保障におけるＩＴに起因する新たな脅威への対応との関係で、「・・・ＩＴの利用・活用の拡大によって新たな脅威が発生していることを認識し、これに十分対応していけるよう、関係機関がその体制を強化しつつ連携し、我が国の安全保障を確保していくことが重要な国家目標である。」とされている。

16 ２００７年2月2日情報セキュリティ政策会議了解では、「第３章　２００６年時のリスクの認識　第２節　リスクの可視化（総論）　（１）我が国全体としてのリスク　（ア）ＩＴ利用の客観的・主観的信頼性に関するリスク」において、「・・・国際社会における国家の存在感（プレゼンス）にも大きな影響を及ぼす文化面では、近年、ＩＴを用いた新しいコミュニケーションの発達を例とする（ＩＴによる）文化創造、ＩＴを用いた我が国文化の世界への発信、更に、ＩＴ技術のイノベーションに率先して取組んで我が国の優れたＩＴ技術力という文化を世界に発信するような機会が増えてきている。つまり、ＩＴはその文化創造・発信機能によって我が国の存在感向上に大きく貢献している状況にある。情報セキュリティ対策の充実によるＩＴの客観的・主観的信頼性の維持・向上は、こうした文化の創造・発信のための当然の前提となるが、これができない場合、ＩＴそのものに不安感が生まれ、新たな文化活動等への取組みが阻害される可能性がある。」とされている。

② 第2次情報セキュリティ基本計画に向けての検討

第１次基本計画によって、情報セキュリティ分野が我が国ＩＴ政策の個別重点分野として立ち上がったことを踏まえると、第２次基本計画では、「ＩＴの利活用と国家目標の実現」との関係での情報セキュリティの位置付けのみならず、情報セキュリティが我が国の国家目標との関係で持つ意義をより直接的に捉えながら政策を検討し、国民にとってより有益な政策とするべきである。主要な国家目標と情報セキュリティの関係について、国民との関係で直接的に関係の深い順番に、国民生活、経済活動、安全保障、文化[17]の順で考察する。

(ア) 国民生活の側面との関係

ＩＴの社会基盤化を踏まえると、１）電子政府サービスをはじめ、国民生活に密接なサービスを提供するための社会基盤を維持することで、生活の利便性を維持・向上するとともに、２）国民が社会基盤であるＩＴを安心・安全に利用し、生活をより充実したものにできることが不可欠である。この意味で、情報セキュリティはそもそも安心・安全な国民生活の根幹の一つとなっている。

結果、我が国ではこのための国民の支出、すなわちＩＴを利用する国民の情報セキュリティ面での支出はほぼ不可避となっている。このため、国民生活の維持・向上の観点から、必要な水準の情報セキュリティを確保するための製品やサービスが、可能な限り低いコストで提供されるような環境が必要である。その上で、国民生活に関連して、社会的に、また個人的に支出することが不可欠な費目が様々に存在する中で、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）を向上していくべきである。

情報セキュリティは、より良い国民生活の実現に向けて勘案することが不可欠な要素の一つであると言える。

(イ) 経済活動の側面との関係

ＩＴの社会基盤化の進展とともに、ビジネス活動におけるＩＴの利用が所与となっている現在、１）ＩＴの不適切な利用やＩＴ利用の前提となる情報管理の不徹底による情報漏えい、２）情報システムの障害などによる事業の停止といった事態が発生した場合は、事業者の信頼失墜や損害賠償による経済的損失へつながる可能性が高まっている[18]。また、重要インフラに関しては、ＩＴ障

17 本書では、社会風土を意味する言葉として、文化の語を用いる。社会風土は、国民の様々な活動の背景として活動に影響を及ぼす、若しくは様々な活動の結果として形成されるものであることから、上記の順番に位置付ける。

18 『2005年　企業における情報セキュリティ事象被害調査報告書』（独立行政法人情報処理推進機構　ウィ

害による事業停止などが社会に及ぼす影響の大きさに鑑みると、社会責任の観点から事業継続性確保などを更に進めることが極めて重要となっている。

このため、情報セキュリティに係る取組みは、事業者にとって、もはや経営上のガバナンスの一部とまでなっている。適切な情報セキュリティ対策は、事業者が顧客からの信頼を確固たるものとし、経済のグローバル化が進展する中で国際的に競争力を維持・強化するために不可欠となりつつある。

情報セキュリティは、経済先進国日本の持続的発展のための重要な要素の一つであると言える。

(ウ) 安全保障の側面との関係

［サイバー空間］

今日のＩＴ利用においては、コンピュータを通じた様々な社会経済活動は、基本的にバーチャルなサイバー空間[19]を介して行われる。このため、サイバー攻撃などからサイバー空間自体の安心・安全を確保することが不可欠となっている。現在、このための取組みは、官、民それぞれによる取組みや、両者が連携した取組みを含めて、様々な主体[20]によって行われており、今後もこれらの主体が、各々の役割を着実に果たしながら、協力・連携を更に進めることが重要である。

また、現状が既にそうであるように、国家の強制力が必ずしも存在しないサイバー空間の安心・安全の確保は、防衛や外交といった国家機能的側面が中心になって実現されるというよりも、むしろ、官民の、役割を持った様々な主体の独自の取組みや、自発的・協調的な参加による取組みで実現されるものである。

安全保障と情報セキュリティとの関係では、サイバー空間の安全保障は、官

ルス被害算出モデル研究会 2006 年 11 月）では、検討するウィルス被害額算出モデルの評価（アンケート調査や既存公表データを用いた被害額の算出）を行い、平均的な被害額（参考値）を中小企業（従業員 300 名未満）4.3 百万円／社、大手・中堅企業（従業員 300 名以上）130 百万円／社と算出している。平均被害額（参考値）にはウィルスによるECサーバ停止、重要システム停止による逸失売上、復旧コストが含まれる。

また、『2007 年　国内における情報セキュリティ事象被害状況調査』（独立行政法人情報処理推進機構　2008 年 4 月）では、Winny のウィルス感染による情報漏えい時の対応に係る費用についてのヒアリング調査を行い、情報流出の顕在化・初動対応 33,000 円、被害状況調査 1,320,000 円、対外説明 800,000～1,400,000 円（訪問費用）、5,600,000 円（電話対応費用）という事例があったとしている。その他お詫びとして対象者に金券を配布する企業もある。これらは複数事例から抽出し、費用は作業量（人・日）に、厚生労働省「平成 18 年賃金構造基本統計調査（全国）結果」より算出した大企業情報管理部門の人件費単価を乗じている。

19 ここでは、サイバー空間を「コンピューター・ネットワークなどの電子メディアの中に成立する仮想空間。特に人間の身体知覚と電子メディアが接合して生まれるメディア環境」とする。

20 サイバー空間を管理する通信事業者（サイバー空間を作り出す情報通信ネットワークを管理するという意味で、サイバー空間を管理すると言う）、サイバー空間とユーザーの接点となるＩＴ機器や情報セキュリティ製品を製造する事業者、サイバー空間においてコンピュータ・ウイルスなどに対して緊急対応を行う組織、サイバー空間を悪用する犯罪者に対応する法執行機関、国境を越えるサイバー空間への対応に係る国際協調のための意思形成・政策推進を進める機関、サイバー空間の安心・安全の確保に向けて国際的に情報交換を進める機関、これらの様々な主体の活動に関し、各々の主体性を損なわない形で調整を行う機関など。

民の様々な主体によって実現される開かれた安全保障であると言える。また、こうした取組みは、我が国の国家の安全保障にも大きく貢献するものである。

［政府機関］

政府機関、とりわけ特別に秘匿すべき情報（特別管理秘密）を扱う機関や、国家の根幹に関わる行政活動を行う機関においても、業務におけるＩＴの利用は所与となっている。他方、近年、エストニアに対するサイバー攻撃のように国家機能の中枢を脅かし得る攻撃の発生や、裏口（バックドア）[21]が仕掛けられたＩＴ製品の市場への流入の可能性など、ＩＴに関連して国家の安全保障上のリスクが増してきている。このため、こうした組織において、合理性に裏付けられた情報セキュリティ対策を進め、組織が有する機密性の高い情報を確実に守るとともに事業継続性を確保することは、国内外からの信頼確保につながるとともに我が国の安全保障の観点から極めて重要となってきている。

こうした機関の情報セキュリティ対策では、技術開発の推進や情報インフラに対する重点的な投資とともに、情報を取扱う関係者のセキュリティ意識・モラル・規律の維持・強化が不可欠である。また、ＩＴは国境を越えた情報流通を容易化することから、こうした取組みに際しては、国際的な水準を意識することが不可欠である。このため、国際連携という視点も重要である。なお、対策にあたっては、その業務の特殊性から、独立に取組みを進めることが認められるべきであるが、同時に国家の安全保障について、広く国民の理解を得ることも必要である。このため、国民に対する説明責任の義務を果たすべく、説明責任や情報公開の範囲に係る検討も今後必要である。

(エ) 文化の側面との関係

我が国は、従来、世界一安全な国との評価を世界から受け、また、伝統的にものづくりを尊ぶ精神から、高品質・高信頼な工業製品を生産して世界に送り出してきた。我が国では需要者・利用者としての国民は、安心・安全な社会で、必要以上に気にかけず、ある意味、受動的な姿勢でいたとしても安心・安全な製品を入手して暮らすことができた。つまり、我が国の伝統的な文化は、受動的であっても安心・安全が確保される、というものであった。

他方、比較的新しい技術であるＩＴの利活用においては、情報通信ネットワークが、我が国とは異なる文化を有する様々な国・地域と常時つながっていること、ＩＴ自体が様々な国の異なる文化の中で開発された技術であること、相手の顔が見えないことが多いために抑止効果が効きにくいこと、さらに、国内

21 一般的に、コンピュータシステムへの侵入者が侵入後、そのシステムに再侵入するために準備する仕掛けを意味する。本文においては、このバックドアを当初から製品に仕掛けられている場合を意味している。

の社会が全体として、暗黙の信頼に基づいて安心・安全を提供する社会から、契約によって明示された責任に基づいて安心・安全が実現される社会へ変質してきたことなどから、従来のような受動的であっても安心・安全が確保されるという文化との不適合が生じてきていると考えられる。

情報セキュリティに係る取組みは、以上のような状況において、ＩＴの分野で我が国にセキュリティ文化（Culture of Security）[22]という概念を普及・定着させることにより、製品やサービスの提供者側のみならず、これまで安心・安全に受動的であった需要者・利用者としての国民側の意識向上や対策実施も進めている。

つまり、情報セキュリティは、とりわけＩＴの利活用に関連して、主として提供者側の努力によって受動的であっても安心・安全が確保されるという我が国の伝統的な文化では対応しきれなくなってきている部分を、補完するために必要な要素と言える。また、同時に、このような我が国の従来からの文化を、現在の社会情勢に適合するよう変質させるものでもあり、他の分野での流れとも整合するものである。

このため、情報セキュリティは我が国の文化面に多大な影響力を有していると言える。

(2)　情報セキュリティ政策の取組みを通じた我が国のあり方
～成熟した情報セキュリティ立国における「ITルネサンス」と世界との協調･イニシアティブの発揮～

①　成熟した情報セキュリティ立国の思想へ

第１次基本計画では、「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）に基づく取組みを推進し、我が国が「情報セキュリティ先進国」となることを謳ってきた。

第２次基本計画では、「「事故前提社会」への対応力強化」及び「合理性に裏付けられたアプローチの実現」の観点に基づいて政策を発展させていくことを考えると、「セキュリティ立国」の思想には、１）冷静で迅速な対応、及び、

---

[22] 経済協力開発機構（ＯＥＣＤ[Organisation for Economic Co-operation and Development]）が策定した「情報システム及びネットワークのセキュリティのためのガイドライン－セキュリティ文化の普及に向けて－（２００２年）」には、リスクの認識を持つこと、リスクアセスメントを行うこと、情報システムやネットワークの設計や実装にセキュリティを組込むこと、リスクマネジメントを行うことといった趣旨の要素が、原則という形でとりまとめられている。

２）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という要素が新たに加わるべきである。また、高品質や高信頼性といった概念は、第１次基本計画の下では、抽象的に完璧を求めることを意味してきたが、第２次基本計画ではより現実に即して、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、と考えるべきである。

情報セキュリティに関して、第２次基本計画の下で目指すべき我が国のあり方は、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』という概念のもと、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」である。

② 成熟した情報セキュリティ立国への道と「ITルネサンス」

「成熟した情報セキュリティ立国」の実現に向けて、「冷静で迅速な対応」や「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」を確立するには、様々な側面からの対応が必要である。この対応は、ＩＴに係る技術や制度の側面の具体的な対策が中心となる。

しかし、これらに加えて、情報セキュリティ対策を実施しながらＩＴを利活用する際の、社会や国民の意識改革も不可欠である。つまり、我が国社会や国民が、セキュリティに関する無謬性の追求から脱却し、１）（対策に係る最大限の努力は必要であるが）事故の可能性を完全に排除する事前対策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と理解すること、２）実際に情報セキュリティ上の問題が発生したとしても、当事者は適切に対処して問題を解決し、周囲は問題の本質及び被害の規模を理解しながら、事態の深刻度合いを捉えられることが必要である。

これは、言い換えると、ＩＴの利活用に関して、セキュリティ上の問題発生の可能性がない完璧なセキュリティは容易に実現できないと一人一人が理解することで、必要以上には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、すなわち「ＩＴからの人間性解放[23]」を意味する。そして、コストや利便性とのバランスをとりながら、最適な水準のセキュリティ対策を実施することで、可能化装置[24]であるＩＴを最

23 ここで、「ＩＴからの人間性解放」とは、ＩＴの利活用を放棄するという意味ではない。

24 ＩＴは、その利活用によって人間が考える様々なアイデアを現実のものとすることができるという意味で、

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、すなわち「ＩＴによる人間性解放」が実現されることとなる。

ＩＴに係るこれら二つの人間性解放、いわば「ＩＴルネサンス」を実現することで、人間がＩＴに踊らされず、逆に最適な水準でセキュアなＩＴを使いこなすことによって人間の潜在能力を最大限発揮して生活の向上に資する環境を構築し、成熟した情報セキュリティ立国へと発展するべきである。

③ 世界との協調･イニシアティブの発揮へ

成熟した情報セキュリティ立国の思想に基づく取組みによって、我が国の情報セキュリティ政策は、より現実に即した政策となる。これを以て、我が国の情報セキュリティの取組みは、国際社会との関係でもより理解されやすくなり、真にＩＴ先進国として発信や貢献を行える水準の取組みが実現されている状態へ到達したと言えるようになると考える。

我が国は成熟したセキュリティ立国の思想の下、自国の取組みに自信を持って世界と協調し、その中でＩＴ先進国として相応しいイニシアティブをとっていくべきである。

また、我が国の情報セキュリティに係る技術を高めていくことはもちろんであるが、同時に、世界における最高水準の取組みや、最先端の技術の動向などについても、情報収集など十分目配りを行い、我が国の取組みが世界の水準に遅れをとらないような留意も必要である。

可能化装置と言う。

第3章　第2次情報セキュリティ基本計画下で達成すべき基本目標について

(1)　情報セキュリティが達成すべき基本目標

ここでは、第２次基本計画の基本理念の下で、実際に達成すべき基本目標についての検討を行う。

①「ITを安心して利用可能な環境」の構築

我が国の情報セキュリティ分野における最重要目標は、ＩＴ利用に際して、安心・安全を確保することである。第２次基本計画においても、第１次基本計画で基本目標とされた「ＩＴを安心して利用可能な環境（以下「ＩＴ安心利用環境」という。）」の構築を中心に据え、構築のために解決が必要な政策課題への対応を図るべきである。

第１次基本計画よりも、より現実に即して、ＩＴ安心利用環境の構築に向けた実効的な取組みを行う観点からは、以下のような実際的な諸点を考慮するべきである。

②「ITを安心して利用可能な環境」の構築に向けて考慮すべき実際的な諸点

(ア)「事故前提社会」への対応力強化に関連して

(a) 理解（気付き）の推進と判断力の向上

情報セキュリティ対策を実施しても、事故発生の可能性を完全に排除することは容易でないことを、社会及び国民全体が十分に理解すること、すなわち気付きが必要である。
その上で、情報セキュリティ上の問題が生じた際に、問題及び被害の規模を理解し、問題の適切な対応について判断できるよう、判断力を向上することが重要である。

「事故前提社会」そのもの、及びそこでの望ましい対応の仕方などについて、一般の個人にもわかりやすい形で、意識及び実際の取組みを向上するための施策などを検討するべきである。

⑹ 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

セキュリティが完璧ではない可能性があることを国民及び社会全体が総論的に理解したとしても、実際に情報の受け渡しなどを行う関係の深い主体の間（例えば、政府機関と国民の間や、企業と当該企業の情報セキュリティ対策のパートナー企業（アウトソーシング先など）の間、企業とその下請け企業の間、情報セキュリティ対策を行う個人と対策ツールを提供する企業の間など）では、さらに、１）共通理解を醸成するとともに、２）信頼関係を構築することが必要である。

したがって、主体間の様々な関係に応じた望ましい共通理解のあり方や、信頼関係構築の推進について検討し、これを実現するための方策を検討することが必要である。その上で、実際に情報セキュリティ上の問題が生じた際の責任分担をどのように考えるかという点について、責任分担の要否も含めて検討を行うべきである。

⑺ 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

事前対応（準備：Preparedness）を進めることは極めて重要であるが、情報セキュリティ上の問題が現実化する可能性も念頭に置くと、障害対応や事業継続性確保などの事後対応（対応：Response、回復：Recovery）への更なる注力が必要である。事後対応に向けては、時系列的な対応事項や、対応時の官民様々な主体の役割分担、対応が必要な範囲といった点について十分な検討を行うとともに、事後対応の準備を進めておくことが不可欠である。

第２次基本計画では、第１次基本計画時の様々な取組みに、この視点を加えた形で情報セキュリティ政策を発展させるべきである。

⑻ 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

「事故前提社会」においては、万が一情報セキュリティ上の問題が発生した際には、事実関係を迅速に把握して事後対応へ注力すると同時に、混乱の防止

や被害の拡大防止のために、社会に対して事実関係や事業継続の状況などについて説明を行う必要がある。また、同様のケースの再発を防止するため、適切な情報共有も行われる必要がある。

事実関係の把握機能強化の方策の検討と、主体の特性に応じ、どの範囲までの説明が必要であるかの検討が必要である。また、他の主体との情報共有を更に進めるための施策の検討を、どういった情報をどの主体で共有するべきかを明確化しつつ行うべきである。

(イ) 合理性に裏付けられたアプローチの実現に関連して

ⓐ 変化し続ける脅威の把握とリスクへの柔軟な対応

対策の合理性を担保するためには、対策の前提となる脅威を把握することが不可欠である。リスクは常に変化し続けるとともに、新しいリスクも生じていることから、これに対応する様々な主体の判断を支えるべく、我が国全体を視野に入れながら、社会における情報セキュリティのリスクを的確に評価（アセスメント）するとともに、対応策を実装へつなげていく機能の検討が必要である。

また、変化し続けるリスクを的確に評価（アセスメント）するのみならず、そのリスクに対する対応を柔軟かつ迅速に行うことを可能とする方策の検討も必要である。特に、対策を実施する主体の規模が大きくなるほど、リスクの変化を含めた状況変化への柔軟な対応は難しくなりがちであるがゆえに、対策の実効性を大きく向上させるには、こうした方策の検討が必要である。

ⓑ コスト、利便性とセキュリティのバランス

コストを度外視した情報セキュリティ対策は現実的ではない。また、対策の推進によって利便性が失われる場合に、利便性とのバランスを無視することも問題である。どれだけ多くのリソースを投入したとしても、完璧な事前防止が容易ではないことに鑑みると、これらのバランスを崩してセキュリティのみに力を入れるべきでないことは、なお明らかである。

したがって、社会全体として、セキュリティを担う機能、利便性の向上を担う機能、コストの適正化を担う機能が互いに密接に連携して、総合的な対応を行うことが重要である。いずれかが突出してバランスが崩れることは、合理性

に裏付けられたアプローチの実現を遠ざけることとなる。

［情報セキュリティ対策に関する投資効率の把握］

このことを踏まえると、主体を問わず、対策に係るコストを投資という観点で捉えなおすことも、容易なことではないが一案であると考えられる。例えば、科学的な手法で投資効率を明らかにし、より効率の良い投資方法に対策を転換していくことも、合理性に裏付けられたアプローチの実現に向けた検討として必要である。情報通信ネットワークは社会全体でつながっていることから、検討の際には、個別の政府機関や企業、人の規模での投資効率というミクロの視点のみならず、ＩＴに係る知識が少ない個人も含む社会全体としての投資効率というマクロの視点も重要である。

［コストを低下させる手法の検討］

コストを低下させる様々な手法の検討も必要である。例えば、主体を問わず、ＳａａＳ[25]モデルやＡＳＰ[26]などの、セキュリティを確認した上での活用や、セキュリティ対策、とりわけ単純な作業を中心とする対策の集約的・統一的実施といった手法を検討し、規模の利益（スケールメリット）を追求することも一案である。また、対策に関して可能な部分の標準化を進めることで、誰でも容易に、かつ、比較的低コストで対策を行えるようにすることも考えられる。さらに、新たな技術開発・研究開発や、新技術の導入よるコスト低下も検討が必要である。

さらに、単独の政府機関や、企業、個人の規模で、効果的・効率的に対策を推進することは必ずしも容易ではないことから、現在でも市場で見られる委託・アウトソーシングビジネスの活用[27]によって低コストで対策を進める方策も、個々の主体の特性を考慮しつつ検討を行うことが必要である。ただし、その際には、委託・アウトソーシング元となる主体が、委託・アウトソーシングに適した事項を十分に見極める必要がある。つまり、本来、自身でなすべき取組みは、引き続き自身で対応するべきである。また、委託・アウトソーシングを行ったとしても、情報セキュリティ対策そのものの責任は、自身にあることを十分に認識することが不可欠である。

加えて、多くの対策実施主体が対策実施の意識を持つほど、需要が増大して

---

25 Software as a serviceの略。

26 Application Service Providerの略。

27 ただし、アウトソーシングの活用にあたっては、インソース（自組織内）の監督能力や人材の質の向上も同時に行うことが不可欠である。さらに、アウトソーシング先の最適なセキュリティ水準の確保が不可欠であることも言うまでもなく重要である。

市場が拡大するために、より低コストで充実した対策手段が現れることになり、逆に、低コストでより当該対策実施主体に適した対策手段が供給されると対策が進むこととなる。このため、個人を含めた様々な主体が、低価格で自身に合った対策を実施できるような取組み、すなわち、対策の推進と対策手法の充実が自律的に進むような環境整備の検討も有効であると考えられる。

［セキュリティのコストからメリットへの転換］

情報セキュリティ対策は基本的にコストとみなされがちであるが、セキュリティ対策を実施することがメリットを生み出すような取組みを進め、対策に投入できるリソースをそもそも増加させることも検討が必要である。

この観点から、単に「対策推進＝善、必要」として一義的に対策実施主体にコスト負担を求める倫理期待型の対策推進から、対策によって信用が失墜しにくくなることなども含め、「対策推進＝メリット、強み」であると対策実施主体が実感できるような利益認識型の対策推進へ軸足を移して行くことの検討も有効である。

(c) 最適な「水準」に関する認識の共有

合理性に裏付けられたアプローチを実現し、リスクに対して最適な水準のセキュリティを確保するには、最適な「水準」[28]に関する認識を、関係の深い主体間や社会全体で共有し、各々の主体はその水準の対策を確実に行うということが基本になるべきである。また、最適な「水準」に関する認識は、事故前提社会における判断力の向上にも寄与すると考えられる。

このため、第一には、事故が起きたときの社会全体としてのリスク管理の枠組み（Risk Management Framework）を考慮しつつ、法制度の可能性も含めて対策実施主体ごとの特性に応じた規範性の要否を検討し、また、規範の程度が十分に考慮された、対策の最低水準や基準を検討することも一案である。これらの最低水準や基準は、明確で恣意的なものではないことが不可欠である。いずれにせよ、この検討は、対策実施主体ごとにきめ細やかに行う必要がある。

また、第二には、関係の深い主体間での役割分担や、各々の主体が取組むべき対策の内容などについて、主体間の関係の様々な類型に配慮しつつ、社会全体として標準化を進めることも有効である。例えば、情報セキュリティ対策の少なからぬ部分はＩＴベンダー、セキュリティベンダー等の情報関連事業者によって支えられているが、こうした主体との間で、各々が取組むべき対策や責

28 最適な「水準」は、情報資産の重要性とリスクの的確な評価（アセスメント）に応じて決定されることとなる。

任分担について明確化を図る方策の検討が必要である。

⑷ 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

合理性に裏付けられたアプローチの下、最適な水準の対策を推進するにあたっては、情報システムに関する技術面・運用面の対策の水準が最適化されているだけでは不十分である。対策を実際に行う人間の能力の向上や、人間の能力の限界を考慮にいれた運用方法の確立など、人的側面に係る対策の更なる発展が重要である。

例えば、合理的な情報セキュリティ対策は、情報システム上の対策だけではなく、前提として適切な情報の管理が適切な人間によってなされていることが不可欠である。また、人間が運用に関わる過程においては、人間が起こすミスや悪質な行動などについて、対策がとられるべきである。

合理性に裏付けられたアプローチでは、技術面・運用面に加えて、人的側面の対策まで包括的に考慮されていることが重要であり、これが実現されて初めて国内外の関係主体からの信頼を得られることとなる。第２次基本計画では、こうした側面についても積極的な検討が必要である。

⑸ 説明責任の明確化

事前対応を進めることは極めて重要であるが、情報セキュリティ上の問題が現実化する可能性も念頭に置くと、社会的影響が大きい主体であるほど、セキュリティ対策の内容や、対策によって確保されるセキュリティ水準、事後対応の観点から事業継続性確保のために準備を行っている取組みなどに関し、適時適切に社会に対して説明する責任が高まる。

したがって、官、民の様々な主体において、どのような範囲で、どのような説明責任があるのか明確化を検討することが必要である。

なお、説明責任に関しては、例えば、そもそも対策を実施せず、記録も残していない主体が、記録がないことを理由として説明責任を免れるというような事態を防止するための検討も重要である。

また、政府機関においては、特別に秘匿すべき情報（特別管理秘密）を扱う場合など、業務によっては、その特性から独立性・秘密性を持ったセキュリティの取組みが一部で認められるべきであるが、合理的に説明責任を果たすべき範囲については、対応を行うことが不可欠である。加えて、一般的な情報を扱

う場合においても、情報セキュリティの取組み全般に関して、合理的に説明責任を果たす必要があるのは言うまでもない。

(2) 基本目標の実現に向けた「新しい官民連携モデル[29]」への補完

① 第1次情報セキュリティ基本計画における「新しい官民連携モデル」

第１次基本計画では、ＩＴ安心利用環境の構築の際の課題[30]解決の方向性として、「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「新しい官民連携モデル」の構築が挙げられていた。

第２次基本計画においても、基本的には、「新しい官民連携モデル」にのっとって政策を推進するべきである。

② 対策実施側と情報提供側の双方からの検討（2つのアプローチ）

他方、「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は、ＩＴ安心利用環境をより現実に即して構築する際に、対策を実施する側（情報を保有する側）だけを念頭に置くのでは不十分である。情報を預ける側も念頭に置き、情報の受渡しの過程に関わる主体全体が、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して理解を深めることが重要である。

また、情報を預ける側の自身の情報に関する所有意識（ownership）を高めることで、自身の情報を守ることに加えて、生活や福利厚生などに上手く活用することへの理解を深める必要もある。

したがって、第２次基本計画では、対策実施主体[31]を含めた対策推進側[32]以外

---

29 本文書において「新しい官民連携モデル」とは、全て第１次基本計画の下で盛込まれた「新しい官民連携モデル」を意味する。第１次基本計画の下での「新しい官民連携モデル」とは異なる官民連携モデルを新たに第２次基本計画の下で構築するべきと考えるわけではない。

30 課題として、「１）顕在化した問題のみに対する対症療法的な対応が支配的であること、２）ＩＴ社会を構成する各主体が、組織の縦割り構造の中で独自の対応に終始していること」が挙げられている。

31第１次基本計画では、対策を実施に適用し、実施する主体（対策実施主体）として、政府機関・地方公共団体、重要インフラ、企業、個人の４主体が挙げられている。

32ここでは、対策実施主体以外に、第１次基本計画における「問題の理解・解決を促進する主体（以下「対策支援主体」という。）を含む。

に、個人情報のような自己の情報等を預ける情報提供主体[33]（、及び、その逆側の立場で情報を預かる情報管理主体[34]）を観念し、新たに情報提供主体を視野に入れて具体施策の検討を行うことも一案である。

つまり、第２次基本計画では、１）対策を直接実施する主体や、対策を支援する主体を念頭に置いた第１次基本計画の下での従来のアプローチと、２）情報を預ける主体を念頭に置いた新たなアプローチの２つのアプローチを採るべきである。

⑶　政策の評価との関係について

情報セキュリティ政策は、第１次基本計画の下では、ＰＤＣＡサイクルに基づき、政策評価や、それを受けた改善処置という過程を辿りながら政策運営が行われている。第２次基本計画の下でも、この政策運営の方式は継続するべきである。

本章でとりまとめた「達成すべき基本目標」については、基本的に、政策運営段階で達成度の評価を行うべきである。他方、達成度を測ることが容易ではないと考えられる要素もあり、こうした点の取り扱いについても、今後検討を行うことが必要である。

33　潜在的にそうなり得る者も実際に情報を預けている者も双方を含む。結果、全ての主体が情報提供主体となり得る。

34 実質的には、対策実施主体と同じ範囲を指す。

第4章　第2次情報セキュリティ基本計画の下での政策の枠組みについて

(1)　対策実施主体について

第１次基本計画の枠組みの下での取組みが浸透してきていることを踏まえると、政策の整合性を確保し、様々な主体が対策を実施する際の効率を維持・向上することが有効である。第２次計画においては、第１次基本計画の下における政府機関・地方公共団体、重要インフラ、企業、個人の４領域という枠組みを基本的に踏襲するべきである。

他方、政策をより決め細やかで実効的なものとする要請にも応える必要がある。これに関して、基本計画検討委員会の検討では、少なくとも以下のような留意点が明らかになった。これらの点については、基本計画検討委員会として、引き続き検討が必要であるとの認識で一致したところである。

第一に、政府機関においては、特別に秘匿すべき情報（特別管理秘密）を扱う業務や、国家の根幹に関わる行政活動に係る業務について、情報セキュリティ対策の観点から、一般的な業務とは何らかの形で切り分けて考えるべきであるかどうかの検討を行う必要がある。この場合、切り分けの基準について、そもそもの切り分けの要否も含めて検討を行うべきである。

また、地方公共団体については、現在、政府機関・地方公共団体とされているとともに、重要インフラの一部でもある。地方公共団体として一括りにするべきであるか、国の政策の手の届く範囲（Government reach）も考慮しつつ、検討を行うことが必要である。

さらに、国立大学法人等も、独立行政法人等に含めて政府機関対策の一環として対策が進められているが、今後の扱いに関して具体施策の有無とともに検討することが必要である。

第二に、重要インフラについては、一般的な企業とは異なる重要インフラとしての対策の範囲をより明確にするべく、対策実施４領域の区分の下での「企業」との境界線を検討することが必要である。

第三に、企業においては、例えば企業規模と情報資産活用度に基づいて、必要に応じて整理を行った上で、中小企業に適した施策を、その要否も含めて重点施策の方向性を検討する段階で検討するべきである。その結果を踏まえ、中小企業を企業の中で一つの括りとするかどうかを検討する必要がある。

また、現在、海外の企業によって、国外からＩＴを介したサービスが提供されることも少なくない。結果、海外の企業が日本人の個人情報や日本企業の機密情報等を大量に保有することも有り得るため、こうしたケースへの対応についても、重点施策の方向性を検討する段階で検討するべきである。その結果を踏まえ、海外の企業を企業の中で一つの括りとするかどうかを検討する必要がある。

第四に、個人においては、人格形成の途上段階にある児童・生徒[35]や、社会人となった以降も高齢者まで含めた目配りを、基礎教育や生涯教育のような形で行うべきであるか、重点施策の方向性を検討する段階で検討するべきである。また、こうした取組みは、社会として行われるべきであるかの検討も有効である。いずれにせよ、検討においては、具体的な施策の有無や実現可能性も含めて十分に検討し、結論を踏まえて、そもそも児童・生徒や高齢者を個人の領域の中で一つの括りとするか検討する必要がある。

また、情報セキュリティ上のリスクを認識しているにもかかわらず、あえて対策を実施しない者についても、個人の中の一括りとして対応を行うべきか、個別施策の有無などを踏まえた上での検討が必要である。

なお、これらの検討に際しては、ネットワークが社会全体でつながっていることから、対策が手薄なところから被害が広がることで社会全体の厚生を下げないために最も効率的な手法を追求するという視点を考慮するべきである。

加えて、現在、ＩＴサービスを複数の主体が協働して提供するケースや、アウトソーシング等によって、他の主体からＩＴ関連のサービスの提供を受けるケースが少なくない。このため、（必ずしも対策実施主体に限らない）様々な主体同士の複合的な形態を括り出した上で、責任分担等に関する検討を、規範性の要否も含めて行うことが必要である。検討にあたっては、例えば、政府機関と国民、サービス提供者とユーザー、ビジネスパートナー同士、事業者と下請け事業者、親会社と子会社など、様々な類型が存在することから、類型ごとにニーズを十分に見極めつつ行うことが必要である。

⑵　問題の理解･解決促進主体（対策支援主体）について

第１次基本計画の下では、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、メディアの４つが対策支援主体として位置付けられている。第２次基本計画でも、基本的にこれらの主体の位置付けは維持しつつ、必要に応じて主体の追加や修正、精緻化を図

35 本文書では、初等中等教育対象者を視野に入れて、「児童・生徒」とする。

るべきである。

具体的には、対策支援主体としての地方公共団体の役割に関して、地方自治の本旨を十分に踏まえつつ、具体施策の有無の検討を含め、今後検討することも一案である。

また、情報関連事業者の役割に関して、市場原理の下で情報セキュリティに係る事業活動を進めるような取組みができるか検討を行うのも一案である。
加えて、情報関連事業者が、セキュアな情報システムをユーザーに確実に提供できるようにするための検討を行うべきである。具体的には、発注者側が求めるべき最適なセキュリティ水準を明らかにできることを実現した上で、供給者である情報関連事業者と要求仕様書を書く発注者が共通理解をもってやり取りを行えるようになるような、両者の間での合意形成の方法や、情報関連事業者が負うべき役割と責任を明確にすることなどについて、検討を行うべきである。

さらに、メディアの情報発信は、啓発や情報共有を進め、社会全体のＩＴリテラシーを向上させるとともに、情報セキュリティ対策を推進させる観点から、非常に大きな効果を有すると考えられる。また、例えば、社会において情報漏えいが発生した際に、漏えいの背景や要因、合理的な対策によって防止し得たものであるのか、合理的な対策が十分になされていたのか、漏えいの社会的影響がどの程度のものであるのかといった情報の発信を通じて、「事故前提社会」への対応力強化及び合理性に裏付けられたアプローチの実現に向けて、大きな役割を果たすことも期待される。

⑶　情報提供主体について

前述の「２つのアプローチ」の考え方に基づき、対策実施側（情報管理側）だけではなく、情報を預ける側も念頭に置くべきである。
このため、情報提供主体も視野に入れた啓発や、情報提供主体と情報管理主体との間での情報の受渡しに関する模範的な例の提示などの具体的な施策についての検討を行いつつ、情報提供主体の役割や責任を明らかにしていくべきである。

⑷　横断的な情報セキュリティ基盤について

第１次基本計画では、情報セキュリティ技術戦略の推進、情報セキュリティ

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・救済の４領域が横断的な情報セキュリティ基盤として設定されていた。

第２次基本計画においても、基本的にはこの枠組みにしたがうこととする。なお、「地方」を横断的な情報セキュリティ基盤に位置付けるか否かについては、個別施策の検討段階で、「地方」を念頭に置いた施策の有無も含めて決め細やかに検討を行った上で、結論を得るべきである。

第5章　第2次情報セキュリティ基本計画の下での政策推進について

(1)　政策の推進体制の強化について

第１次基本計画においては、ＮＩＳＣの強化[36]と各府省庁の強化[37]を掲げていた。第２次基本計画においても、こうした推進体制の強化は引き続きなされるべきである。

特に、政府機関の情報セキュリティ対策の推進の取組みを通じ、各府省庁の情報セキュリティ部門の担当者の不足が指摘されている。また、各府省庁の担当者の人事異動ローテーションは、２～３年という短期間を基本としており、十数年を越えることも決して珍しくない民間組織に比べて、専門性の涵養や経験の蓄積がされにくいという問題も見られている。

また、政府機関においてセキュリティ対策を更に推進するにあたって、特に事後対応のような対策は、当初から全てを計画して実施するという性質のものではないことから、予算面におけるより柔軟な対応も重要である。

第２次基本計画に向けては、こうした課題へ対応すべく、例えば、インソースの強化として、担当部門における担当者数の確保や人事制度の改善、人材育成の強化、コンサルタントのような専門家の派遣による補完や能力向上、比較的少ない人数でも対策を確実に推進できるよう、簡易な作業の標準化や集約化などを検討することが必要である。また、専門分野におけるアウトソーシングの戦略的な活用といった対策についての検討も必要である。

さらに、何らかの指標を活用するなど合理性に基づく形での柔軟な予算制度について、検討を進めることも重要である。

また、政府機関の現状を見ると、政策の推進にあたって、技術的な知見[38]、及びそういった知見を有する人材の蓄積が不足していると考えられる。合理的に情報セキュリティ政策や対策を推進するべく、こうした技術面の知見を蓄積・活用できる構造について、検討を行うことが必要である。

---

36 第１次基本計画では、「国際的にも国内的にも、最高の英知を結集していくための体制として、政府全体の推進体制を有効に機能させるための中核として強化することを目指す。さらに、・・・民間の人材を積極的に活用することに努め、同時に、政府職員の人材育成の中核拠点として機能することを目指す」とされている。

37 第１次基本計画では、「内閣官房情報セキュリティセンター（ＮＩＳＣ）を中核とした、政府全体の情報セキュリティ対策を積極的に推進すべく、自府省庁の情報セキュリティ体制の充実・強化を図るとともに、従来の縦割りになりがちな推進体制を改め、官民における統一的・横断的な情報セキュリティ対策の推進が行われるよう、各種政策の実施に努めることとする」とされている。

38 ここでは、科学技術（Scientific technology）という意味で「技術」の語を用いている。

例えば、社会全体を視野に入れながら、情報セキュリティの観点からのリスクを的確に評価（アセスメント）する機能[39]や、政府機関や社会全体として、どの程度の取組みを行えば最適な水準の対策を行っていると言えるかといった水準を示す機能、政府機関における様々な情報セキュリティの取組みについてコンサルテーション等の支援を行う機能、実際にＩＴ障害などが発生した際に、厳密なアクセス権の設定の下、背景を確認したり、再発防止を促進したりすることで、情報システムなどの信頼性を高める機能、政策や対策の取組み状況や効果を測るとともに取組みの向上を支える機能、などについて、第２次基本計画に向けて検討を行うべきである。

これらは、ＮＩＳＣの強化によって対応するべき機能であるかは別途検討が必要であるが、政府機関も含めた公的役割を担った機関総体として持つべき機能である。また、こうした機能を様々な機関が分散的に有する場合は、機能同士、また機関同士の連携強化を図ることも必要であると考えられる。この機能によって蓄積された技術面の知見は、公的役割を担った機関だけに留まらず、民間企業等での活用も期待される。

また、政府機関に限らず、企業などの様々な組織、個人において具体的な取組みを推進するには、強い動機付けと具体的な推進体制が必要となることから、こうした点について、主体ごとの特性などを踏まえつつ、望ましい手法を検討する必要がある。

(2) 情報セキュリティ以外の他分野、他の関係機関との連携について

情報セキュリティ政策は、他の幅広い分野と密接に関連を有する。このため、施策効果を向上させるためには、必要に応じてこうした他分野や他の関係機関との連携を進めることが不可欠である。こうした点については、対策実施主体及び横断領域等の検討において個別に議論を行う必要がある。

結論は何ら予断しないものの、分野としては、例えば、科学技術、知的財産権保護、防災、製造物責任、消費者保護、違法有害情報対策、プライバシー、企業のリスクマネジメント等が挙げられる。

(3) 情報セキュリティ政策及び対策の柔軟かつ機動的な推進について

情報セキュリティ分野は、リスクの変化が非常に早い分野である。このため、

39 ここで述べるリスクアセスメント機能は、例えば、情報通信ネットワークにセンサーを置いて監視するような国家管理的な機能という趣旨ではない。

社会の変化や技術の進歩に合わせて柔軟かつ機動的な対応を進めることで、政策及び対策の効果を向上することが必要である。ＰＤＣＡサイクルの計画段階の想定からリスクが変化することは十分に有り得ることから、政策及び対策の評価においては、こうした変化も踏まえて、臆することなく客観的な評価を進めることが、取組みの実効性向上につながるという理解を関係者が深めるべきである。

第6章　実効性の確保のために今後の検討が必要な課題について

第１次提言のとりまとめ後は、基本計画検討委員会としては、対策実施主体や対策支援主体、情報提供主体、横断的セキュリティ基盤分野などの重点施策の方向性（各論）を中心に検討を進めることとなる。

なお、本章において盛込まれる検討課題は、あくまで今後の検討課題の例であり、これらを以って、網羅的に今後の検討課題を記述するものでは必ずしもない。また、ここで挙げた検討課題は、基本計画検討委員会及び個々の委員の議論・提案に基づくもののうち、特徴的なものを中心としている。個々の主体間などでの政策の分量のバランスなどについて、第２次基本計画における最終的な形態を予断するものでは必ずしもない。

⑴　対策実施主体に係る検討課題

●政府機関情報セキュリティ対策におけるＰＤＣＡサイクルの実効性強化

規範に基づく各府省庁の対策について、技術的な観点から見ても合理的な対策を確保するための方策や、統一的な視点に基づいて監査を進める機能（第１次基本計画で構築してきたＰＤＣＡサイクルの点検段階の実効性強化）、対策の改善に向けたアドバイスを行う機能の検討などを行う。

●行政情報システムの最適化の取組みとの関係に係る検討

行政情報システムの最適化の取組み（全体最適化よりも小さい各課単位の規模のシステムも含む）に、情報セキュリティの視点を加味するとともに、実効性を確保するための取組みについての検討を行う。

調達物品についてある程度の類型化とその基準化を行い、効率的かつ実効的な活用方法及び専門的・技術的観点からアドバイスを行う機能の検討を行う。

●政府機関における機密性の高い情報の保護及び事業継続性確保に係る検討

機密性の高い情報の保護のために必要な方策の検討を行う。

ＩＴ障害の発生時における緊急対応や復旧も含めて、政府機関の事業継続性

確保のための施策に関する検討を行う。

●政府機関の国民に対する説明責任に係る検討

事後対応時も含めて、国民に対して合理的に説明責任を果たす範囲や方法についての検討を行う。

●政府機関における人材の確保などに係る検討

人材の育成・確保、情報セキュリティ対応のための体制強化、柔軟な予算確保の方策、専門分野におけるアウトソーシングの戦略的な活用、共通的な取組みに係る集約化を通じた少ない人数でのセキュリティ確保などを含めて検討を行う。

●重要インフラに係る様々な検討

現在の重要インフラ１０分野[40]の分類や位置付けの適切性に係る検討を行う。

重要インフラとしての対策と企業としての対策の境界についての検討を行う。

重要インフラ対策に係る監査のあり方についての検討を行う。

重要インフラ関連の情報システムを含めて、事業過程の信頼性を高めるための機能に関する検討を行う。例えば、事業者の主体性を尊重した形での合理的な情報共有の推進などが挙げられる。

●企業に係る様々な検討

対策の最低水準を設定することの是非に係る検討を行う。

対策がコストとならないようにするための施策に係る検討を行う。この観点から、企業のセキュリティ対策に係る援助策が必要との意見もあった。

●個人に係る様々な検討

---

40 情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方自治体を含む）、医療、水道、物流が挙げられる。

児童・生徒への対応の要否に係る検討を行う。対応を行うべきとの結論が出た場合には、具体的な方策に係る検討を行う。

⑵　対策支援主体に係る検討課題

社会全体を視野に入れながら、情報セキュリティの観点からのリスクを的確に評価（アセスメント）する機能や、政府機関や社会全体として、どの程度の取組みを行えば最適な水準の対策を行っていると言えるかといった水準を示す機能、政策や対策の取組み状況や効果を測るとともに取組みの向上を支える機能などについて検討を行う。

情報システムに係る事故があった場合の調査や評価を行うとともにシステム自体の信頼性を高める機能に関する検討を行う。

対策支援主体としての情報関連事業者や地方自治体の役割に係る検討を行う。

⑶　情報提供主体に係る検討課題

情報提供主体としてのリスクの認識強化のための施策に係る検討を行う。

情報提供主体が、情報が保護されると合理的に期待できる範囲に関し、提供情報の保護が進む方策について検討を行う。例えば、一定の合理的な情報保護水準を保証するためのサービス責任（service liability）の概念や、情報保護を保証するための保険制度に係る検討などが挙げられる。

⑷　横断的な情報セキュリティ基盤に係る検討課題

●技術戦略の推進に係る様々な検討

技術戦略の推進に関して、暗号方式や認証基盤など技術的な先進性が重要な分野に係る国策としての取組みの検討を行う。

情報技術と情報セキュリティ技術の一体的な発展に係る検討を行う。

近年、活用が進む組込みソフトのセキュリティ確保のための方策に係る検討

を行う。

●人材の育成･確保に係る様々な検討

児童・生徒をはじめとする幅広い層を対象とした情報セキュリティ教育の要否に係る検討を行う。

●国際連携･協調に係る様々な検討

海外企業による日本企業の情報や日本国内の個人情報の保有に対して、セキュリティを確保するための施策の実現可能性を検討する。

情報セキュリティに係る国際標準の形成に対して、一定のイニシアティブを発揮するための方策について検討を行う。

安全保障の観点から、特別管理秘密などの情報管理や政府機関の事業継続性確保の取組みに関する国際連携の推進について検討を行う。

●犯罪取締り･権利利益保護に係る様々な検討

被害者の保護・救済のための法制度の整備の検討を行う。

情報セキュリティとの関係での情報の法的な評価方法に係る検討を行う。

サイバー攻撃によるテロへの対応について検討が必要との意見もあった。

別添1

情報セキュリティ政策会議
基本計画検討委員会
委員名簿

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
須藤　修	東京大学大学院情報学環・学際情報学府教授
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

（敬称略）

別添2

第１次提言までの検討の経緯
（基本計画検討委員会）

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