資料５参考

「「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）」に関する意見

08/02/06　神奈川県藤沢市

１．基本認識

○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。

＜意見＞

◇「個」の利用の拡大

情報伝達速度の高速化と伝達量の拡大があるが、官民等の組織的利用だけでなく「個」の利用拡大の流れがある。

特に、ブログや携帯メールなどＩＴのコミュニケーションの手段としての役割に注目する必要があり、旧来の衰退した地縁・血縁に替わり、急速に「電縁」（ネットワーク上の縁）が強まり、新しい価値観や文化の創造が図られてきている。

このため、情報セキュリティとして取り組むべき範囲については、「個」及び「個」が形成する地域社会といった地域コミュニティや、ネットワークコミュニティも考慮する必要がある。

○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次基本計画の期間中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。

＜意見＞

◇地方公共団体の立ち後れ

「情報セキュリティ基本計画」が策定されたことにより、政府機関の取組は進みつつある。地方公共団体においてもガイドライン（「地方公共団体における情報セキュリティポリシーに関するガイドライン」総務省）に基づく情報セキュリティポリシーの策定が進むなど、一定の進展が図られた。

しかし、地方公共団体における情報セキュリティレベルには非常に大きな格差が存在し、「情報セキュリティ基本計画」そのものもまだ浸透しているとは思えない。

このため、地方公共団体の実態を把握するとともに、この底上げに重点的に取り組む必要がある。

◇脅威の認識と不安の増幅

IT が国民全体、特に高齢者層に拡大し、かつ「個」の利用が急速に拡大しているが、IT 利用に関する脅威の認識が高まるにしたがい、逆に不安を増幅している面もある。

このため、IT 利用における利便性及びその脅威とともに、インシデント発生時の対応手段について、国民全体に浸透させる等の不安を除去することが重要である。

また、犯罪を犯している意識の欠如が見られ、ＩＴを利用した犯罪に対する法整備が急務と思われる。

※「インターネット上の安全確保に関する世論調査」（内閣府）より
ネット利用の不安を感じる４５．５％

◇各コメントに関して

１．について：

目標の観点に「インシデント対応の確立」を加えても良いのではないか。脅威への対応はあるが、実際に起こってしまった場合の対応までは無いため。

２．について：

地デジ、ワンセグ等の新たな手段・道具が増えた、ＳＮＳ等の普及も急速に進んでいる。

技術的な対策だけでは情報セキュリティは確保できず、ルール作りが必要。

３．について：

政府・民間企業等の供給側視点からだけでなく、個人や地域住民といった利用者からの視点が必要ではないか。

ＩＴ利用における情報の利便性及びその脅威、さらにはインシデント発生時の対応手段について、国民全体に浸透させることが重要である。

４．について：

Information Security の中に Cyber Security が包含される。

５．について：

重要インフラ中心に記述されているが、重要インフラ、官民に対してそれぞれ Preparedness、Response、Recovery を明確にする必要がある。

２．総論

○情報セキュリティ政策の理念について

～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。

＜意見＞

◇受動的から能動的な取組へ

情報セキュリティの対策は、ほとんどが受身の対策として実施されており、対症療法の域を出ていないが、自らがリスクを洗い出し、評価し、対策を立て、実施し、見直していくことが重要で、受動的な取組から能動的な取組への転換が必要である。

このため、情報セキュリティ対策を各主体の責務とするとともに、インセンティブの与え方や持ち方をどうしたら良いかの検討も必要である。

◇意識改革と社会風土

意識改革は必須であり、現在の社会風土を一新する必要がある。そのためには、事象、弱点、インシデント報告の重要性を強調し、さらに、問題発生時には人が悪いのではなく、組織が悪いという風土を定着させる必要がある。

しかし、日本の社会風土の中で、社会的な合意が形成され、定着するような改革は可能であろうか。

◇性善説と性悪説から環境説へ

セキュリティは必ず「性善説」か「性悪説」かの決定論的な議論となり、「どうすれば良いのか」の建設的・生産的な議論に結びつきにくい傾向がある。

このため、「どのような環境であれば情報セキュリティを守る気を起こさせることができるか」という観点が重要で、この「環境説」を採ることにより、具体的な政策をめぐる議論の土壌にあげやすくなる。

◇各コメントに関して

１．について：

コスト把握が容易なものと、何か指針を出さなければ把握できないものがある。

２．について：

ＩＳＭＳの概念を用いて、利便性とセキュリティ対策の均衡を取ることは可能であり、第１次基本計画でも提唱されているが、均衡を取るためのさじ加減が組織ごとに異なるため、ある程度の指針は必要である。

３．について：

意識改革は必須であり、現在の社会風土を一新しなければならない。

しかし、日本の文化・風土を考慮した新たな推進手法を考える必要がある。

４．について：

１００％事前防止は組織の建前で、実態は不可能であるとの認識は広まっている。

上記「３.」にも関連するが、組織の中でＰＤＣＡサイクルが活用され、その仕組みがスパイラルアップしていくようにしなければならない。

５．について：

責任限界点は時とともに変化すると考えるが、これが無いと明確な目標や、責任の認識が曖昧になってしまう。

ＩＳＭＳで提唱しているリスクマネジメントの考え方を広く普及していくことで、ある程度の対応ができる。

６．について：

可能な部分と、それを必要としない部分との境界に対する適用が課題である。

情報セキュリティ対策による財の価値向上はあるとしても、情報セキュリティ対策だけを見れば、公共財に近いものになる。

７．について：

ある程度の影響は回避できない。また、親子関係の組織であれば、親組織がそれを負担する、若しくは、わが国のセキュリティ対策を推進していくためにファンドを設けることも視野に入れて検討していかなければならない。

８．について：

情報セキュリティ事件事故の８０％以上は人的な原因。

教育研修を階層別等工夫を凝らして数多く実施したり、小集団活動の採用、表彰制度の導入、訓練の実施、クリアデスク等日常的の取組が実用。

９．について

外部委託のメリット（工数削減、技術レベルの確保等）とデメリット（組織内技術の枯渇化、管理の複雑さ等）について明確にすべきである。

ＩＴゼネコンのロックインや再委託は、大変大きな問題となっている。

１０．について：

重要インフラの安全性確保、インシデント発生時のバックアップ体制の確立が重要である。また、国防に関わるセキュリティは国家が主体とならなければならない。

１１．について：

諸外国の最善事例を参考にする前に、国内の政策を体系化（例：セキュリティで言えば、ＩＳＭＳ、情報セキュリティ管理基準）し、その後、有効と判断した場合に、国内の風土に合わせて取り入れるべきである。

１２．について：

中期及び長期計画を国民に提示し、それに合わせた予算を確保し、実践的、計画的に対応していくべきである。

○第２次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。

＜意見＞

◇対策実施領域としての地方公共団体の位置づけと扱い

大中小、規模も環境も異なる約１８００の地方公共団体は住民や地域に密着して様々な業務を行い、１億２７００万人超の個人情報等の情報を預かり、管理している。そして、これらの情報資産価値や脅威はほぼ同様であるが、脆弱性が大きく異なっており、情報セキュリティレベルに非常に大きな格差が存在する。

このため、各地方公共団体の情報セキュリティ対策に「差」があってはならず、取り扱いも含め全国均一な対応が必要で、独立して取り扱うべき重要な領域ではないだろうか。

◇コミュニティや NPO の視点

IT の利活用には、コミュニティや文化に関する視点を加えるべきであり、地域コミュニティや NPO 等を情報セキュリティの普及啓発等の担い手と考える発想、支援される対象から推進する主体と捉える発想も必要である。

また、官や市場原理、技術だけでは解決できない課題を、コミュニティで解決するような発想も必要であり、公助、自助に加え、共助の考え方も必要である。

◇各コメントに関して

１．について：

技術、人材においては中期目標を立案し、その中で技術革新、人材スキルレベルを提唱するのも１つの手段である。

２．について：

地方公共団体を独立して取り扱う必要がある。

３．について：

今の段階では現状のままで良いと考える。第１次基本計画で提唱されているとおり、各事業者の監督官庁ごとの統制では、全体最適が図れない。

４．について：

例示のとおり、企業を分類する方が望ましい。

５．について：

IT 利用者の観点からすれば、年齢（未成年、高齢者）を区別することには疑問があるが、それをサポートする体制を整えるべきである。

６．について：

特に委託先のリスク管理は大きな課題である。

７．について：

情報インフラの整備を行うことにより、距離的ビハインドを情報伝達の無格差化でカバーすることが重要ではないか。

８．について：

リサイクル時の情報漏えい指針、防災における事業継続（BC)、機密性の観点での個人情報保護が考えられるので、明確の部分から整合を取るべきである。

９．について：

事業継続の概念。

３．各論

○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

～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、今後どのような対策が必要か。

＜意見＞

◇地方公共団体の実態把握

現行の基本計画は政府機関により重点が置かれているが、次期基本計画では地方公共団体の実態をより捉え、進化した計画とする必要がある。

このため、各地方公共団体の情報セキュリティレベルをできるだけ客観的に把握できるように工夫するとともに、情報セキュリティ対策に決定的な影響のあるトップや職員の意識レベルを把握する等、具体的な阻害要因の調査が必要である。（なぜ進まないか）

また、ほとんどの地方公共団体は、既に情報セキュリティポリシーの基本方針や対策基準は策定したことになっているが、PDCA サイクルを毎年確実に実施している団体は、非常に少ないと推測される。さらに、総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン（平成１８年９月版）」でも実施手順までは定めていないことから、実施手順は未整備となっていると推測される。

このため、情報資産台帳やリスク分析、規程類の見直しをしているか、教育研修や訓練の実態、セキュリティ監査の内容、監査結果の改善結果などを定期的に調査し実態を把握する必要がある。（どこまで進んでいるのか）

◇個人情報保護条例・情報ｾｷｭﾘﾃｨ対策の実施

都道府県　n=47	H15	H16	H17	H18
個人情報保護条例制定率	100.0%	100.0%	100.0%	100.0%
情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定率	80.9%	97.9%	100.0%	100.0%
情報ｾｷｭﾘﾃｨ研修実施率	61.7%	87.2%	95.7%	100.0%
情報ｾｷｭﾘﾃｨ監査実施率	23.4%	36.2%	55.3%	78.7%

市町村　n=1843	H15	H16	H17	H18
個人情報保護条例制定率	73.6%	82.1%	98.0%	100.0%
情報ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定率	29.5%	74.4%	92.5%	96.2%
情報ｾｷｭﾘﾃｨ研修実施率	21.9%	40.5%	51.5%	61.2%
情報ｾｷｭﾘﾃｨ監査実施率	8.9%	11.8%	20.8%	29.1%

◇情報ｾｷｭﾘﾃｨ監査の実施内容

	都道府県	率%	市町村	率%
内部監査の実施	12	25.5	294	16.0
外部監査の実施	10	21.3	171	9.3
内部・外部監査をあわせて実施	15	31.9	72	3.9
計	37	78.7	537	29.1

平成18年度　地方自治コンピュータ総覧より

◇地方公共団体の成熟度による目標管理

各地方公共団体の情報セキュリティレベルは大きな格差があるが、レベルアップに対するポテンシャルも阻害要因も一律ではない。このため、現状（成熟度）を把握するとともに、段階的な目標を定めて段階的にレベルアップすることが有効と考えられる。

現状把握や目標設定、段階的レベルアップの計画や実施が求められるが、成熟度の判定基準とそれにあわせた目標設定方法のガイドライン作りが必要である。。

◇地方公共団体の情報セキュリティ推進要件

情報セキュリティの推進要件は、地方公共団体の規模や地理的環境だけでなく、トップの意識に大きく依存する。また、情報セキュリティ部門の意欲も大きな要素となる。

このため、トップの意識啓発をどのように図っていくかが重要な課題で、全国知事会、市長会、町村会等組織の役割が期待される。

また、組織的に明確な責任体制の構築も必要で、CISO を設置するのもその１つであり、情報セキュリティ部門の明確な権限と位置づけが必要となる。

さらに、首長の責任を明確にするため、情報セキュリティポリシーの条例化も有効ではないか。

◇地方公共団体の課題と解決手法

情報セキュリティポリシーはＰＤＣＡサイクルを毎年確実に実施するかや、組織への浸透度が問題となる。

このため、情報資産台帳、リスク分析、規程類の見直し、教育研修の実施、情報セキュリティ監査や緊急時訓練の実施、監査結果等の改善への反映等を計画的に実施することや、実施手順を豊富にそろえること、職員啓発の工夫が必要である。

特に、情報セキュリティポリシーの根幹となるのはリスク分析で、様々なレベルにある地方公共団体には、分かり易いガイドラインや、マニュアルが必要となる。

また、近年の中越沖地震等災害の発生を考えると、大災害発生等に対応する業務継続計画についても、実効性のあるガイドラインやマニュアルが不可欠である。

◇地方公共団体の責任範囲

地方公共団体は様々な情報セキュリティ対策を実施するだけでなく、新たな脅威にも対応する必要があり、さらに、住民や組織内にリスク受容の理解を求める必要がある。

このため、ＩＳＭＳはリスクをコントロールする１つの手法であるが、どこまで対策を実施すれば良いのか、免責となるかは不明確であり、何らかの指標が必要である。

また、保証型の情報セキュリティ監査、情報セキュリティ保険の創設なども検討する必要がある。

◇地方公共団体の外部委託と地元企業育成

地方公共団体の外部委託は増加しており、委託先からの情報漏えいは大きな問題で、この防止対策が必要である。このため、外部委託事業者の情報セキュリティ対策実施状況の確認や、リスクアセスメント実施後に契約し、契約後に実地検査等による確認を行

うことが必要となが、このような取組は多くの地方公共団体にとって大きな負担で実現性が薄い。また、ＩＴゼネコン等の再委託問題や地元ベンダー育成という大きな課題もあり、これらの点も考慮した委託管理のガイドラインが必要である。

◇小規模な地方公共団体の対策

首長の意識や担当部門の意欲が不可欠であるが、まずは人材の育成が必要である。

（財）地方自治情報センターの講師派遣事業やネットワーク機器等の遠隔診断を利用するなど、外部支援機関の利用も有効である。

また、情報システムの共同化やＡＳＰ、ＳａａＳなどとともに、人材の共同利用、相互利用も検討の必要がある。

◇地域住民の情報セキュリティ対策

地方公共団体は住民の情報セキュリティ対策にも取り組む必要がある。この際ＮＰＯやボランティアグループとの協働が有効である。

◇各コメントに関して

１．について：

詳細化を各省庁に振るのであれば、それは現在の各省庁毎に提示されているセキュリティガイドラインのように統一性がとれなくなる。この領域は政府（例えば、内閣官房情報セキュリティの部門）が統制を取るべきである。

２．について：

上記「１.」と同じ。

３．について：

上記「１.」と同じであるが、自己チェック（監査）できる仕組みを統一的に提示した上で、各省庁でチェックを実施し、さらに政府がチェックする仕組みを構築すべきである。

現状は出来ていないと思われても仕方が無い、若しくは国民に伝わっていない。

４．について：

ＩＳＭＳや、情報セキュリティ監査（保証型）を用いるべきではないか。

５．について：

ＩＳＭＳで提唱されている通り、情報セキュリティの責任者、資産の責任者等を明確に定め、あるインシデントが発生したら、組織の責任者として当該幹部が謝罪すること等を認識させるべきである。

６．について：

上記「１.」と同じ。

７．について：

人員の育成を図った上で予算を検討すべきである。

セキュリティ対策（事前、事後）の指揮命令権の委譲を行い、迅速に対応できる仕組みを構築すべきである。

８．について：

上記「７.」と同じ。

９．について：

対応部門を特定し、さらに中央においては、それらを統括する部署が必要である。

１０．について：

均一的に展開するためには、有効な手段と言える。

１１．について：

政府がガイドライン（そのまま使えるもの）を提示し、順守してもらう。また、必要に応じてファンドを設けることも検討する。

○重要インフラにおける情報セキュリティ対策について

～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。

＜意見＞

◇各コメントに関して

１．について：

ＢＣの観点から、災害、事故、故意等を個々に具体的に想定して計画すべきであり、ここまでの被害であればどの程度影響が出て、復旧にどれくらいかかるかを提示すべきである。(最重要課題)

２．について：

現状、ＯＥＣＤの概念に従い、わが国独自の内容があれば盛り込むべきである。

３．について：

「共通課題」については、エスかレーション、管理体制、報告フォーマット等共通部分を規定すること。

「個別課題」については、災害（地震、風水害、火災等)、事故、故意等の個々に、具体的は対応策（マニュアルとして使用できるもの）を規定すること。

４．について：

「部分最適」と「全体最適」の差異はあるものの、セキュリティに関する考え方、対応の仕方等は同じである。

「個々の利用者」は、あくまでも利用の立場でのセキュリティ対策となり、「社会全体」としては、特に組織としての責任を考慮したものでなければならない。

５．について：

民間の取り組みを参照し、国家としてのポリシーを確立し、官民を含めて全てそれに順守する体制を構築すること。

６．について：

重要インフラに寄与している民間においては、インシデント発生時に優先的に対応する仕組みを構築させると。また、その際には、その対応のために生じた損失を国が担保する体制を整えること。

７．について：

脅威に対するセキュリティ対策（ウィルス対応等）は、共有データベースを構築して情報共有すべきである。

８．について：

難しい領域ではあるが、匿名制にて公開できる仕組みを国等が提供すること。

９．について：

個々の文化の違い。機密性の確保（どこまで信頼してもらえるかも含めて）

１０．について：

機能別にマトリックス化を行うことにより、関連部分の可視化を用意にさせる。

また、それらの情報共有、公開が連鎖を止める。

１１．について：
　第三者の視点で調査委員会等を設けることは、公平性、中立をたもつためにも必須となる。
１２．について：
　徐々に関心を持ってきつつあるが、まだまだ自分のところには関係が無いといった風潮が感じられる。

○一般企業における情報セキュリティ対策について
～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。

＜意見＞
◇各コメントに関して
１．について：
　部分的には基本計画の影響のもと、対応しつつあるが、そもそも基本計画そのものが浸透しているとは思えない。（アピール不足）
２．について：
　メリットは、各組織、個人のセキュリティ意識の向上。
　デメリットは、利便性を考慮しないことによる生産性の悪化。
３．について：
　国家としてのスタンダードを確立し、企業に順守させる仕組みを構築させること。
４．について：
　重要情報の特定と管理方法の確立を義務付ける。
　重要情報の取り扱いに関するガイドライン（具体的）を提示すること。
５．について：
　国が意図している方向に、必ずしも企業が向かっているとは思えず、現状は、各企業が独自に取り組んでいるように思える。
６．について：
　日本が不得意とする「契約」に、いかに具体的に盛り込めるかに依存する。
　具体的な、ガイドラインが必要であり、場合によっては義務化も検討すべきである。
７．について：
　まず、人では無く、組織に責任があることに注力すべきである。その上で個人の責任に及ぶ場合に、そこではじめて言及すべきである。（故意の場合はそのかぎりではない）
８．について：
　目先の対策にとらわれて施行したものであれば、コスト、生産性を危惧することもあるが、体系的（ＩＳＭＳの仕組みを利用）に実施すれば、その様な意識も軽減されると思う。

○中小企業における情報セキュリティ対策について

～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。

＜意見＞

◇各コメントに関して

１．について：

負担を軽減させるために、ガイドライン（具体的）の提示が必要。

２．について

その通り。

３．について：

金銭的に負担のかからない人材育成（教育）から着手し、費用に関しては、関連親企業がサポートもしくは、ファンドを用いることになると思う。

４．について：

支援のためのファンド等のバックアップ体制が必要となる。

５．について：

責任分担を明確にし、ある程度大企業及び国がサポート（費用面）すべきである。

６．について：

情報資産のコスト化（可視化）の課題がクリアできれば対応可能となる。

７．について：

SaaS 等への活用に注力していくことになると考えるが、SaaSにおける情報セキュリティレベルの向上が必要。

○ＩＴ企業の情報セキュリティ対策における役割について

～我が国のＩＴ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。

＜意見＞

◇各コメントに関して

１．について：

一つの事象に対し、統一的な対策をとることが困難な場合がある。（個別対応を余儀なくされる）

２．について：

セキュリティ基準、順守事項、要求事項等の明確な提示及び順守。

３．について：

品質基準を設けることは必須。

４．について：

その通り。可視化、明確化のためのガイドラインを提供すべきである。

５．について：

委託先管理（監査を含む）の徹底。

６．について：
単一製品：情報公開とパッチ等の配布の徹底。構築されたアプリケーション（システム）の可視化。
７．について：
コンサル等その他においても十分可能と考える。
８．について：
例えばＩＳＰにおけるセキュリティ対策の一環として、セキュアでない端末からの接続を制限（この中でパッチ適用等を実施）し、対応後、通常のサービスを利用できる仕組みを提供する。
Ｐ２Ｐ関連のソフトウェアの利用又はその中で流通可能なファイル形式の制限等を行うことにより、不用意な流出を防ぐ等。
９．について：
授受した情報（個人情報等）の管理に対するガイドラインの提示が必要。
通信過程における情報の保護（暗号化等）の適用。
１０．について：
現在のサービス説明中心のサイト（文書等も含む）から、もっと分かりやすい危険性に関する記載の工夫が要求される。
ガイドラインを提示し、ＩＳＰ等はそれに準拠しなければならない仕組みにする。

○個人に対する情報セキュリティ対策について
～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。

＜意見＞
◇各コメントに関して
１．について：
学校教育（小中高等）に至るまで、そのレベルに合わせたセキュリティ教育を義務付けることが必要。
高齢者等を含む学校教育に参加できない国民に対しても、例えば、地方公共団体等を活用できる仕組みも必要である。
２．について：
上記「１.」と同じ。
３．について：
現状は、消費者保護というよりも利益優先であると感じられる。
政府として、事業者に対する「消費者保護に関するガイドライン」を作成し、準拠させるべきである。
４．について：
違法行為に対する対策は必須であり、対策を広く明示することにより抑止効果も上がる。
何をもって有害と定義するかが、大きな課題となる。（言論の自由の観点も考慮）

５．について：
　考え方は良いが、国民をランク（差別）化してしまう恐れに対して十分検討しなければならない。
６．について：
　鍵管理の徹底をいかに確実にするか、暗号化を徹底できるか等の問題を考慮した上で、ガイドラインを提示すべきである。
７．について：
　どの様な場合に国家が国民の個人情報を収集でき、どの様に活用する場合があるのかといった具体的な情報を開示すべきと考える。
８．について：
　どのレベルであったら公開可能か、匿名による事件との因果関係を十分調査した上で、開示及び匿名におけるガイドラインを設ける必要がある。
９．について：
　障害者、（受刑者？）等に対する対策。
　国内に居住する外国人についての対策。
　長期海外渡航者についての対策。
　これらは、どこまで考慮するのかというところか検討しなければならない。

○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
～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、どのように評価するのか。

＜意見＞
◇各コメントに関して
１．について：
　政府の技術開発戦略の先進的な取り組みは十分評価できるが、実践という観点では対応の遅れが懸念される。（例：ＩＰ－ｖ６対応、他国開発ＯＳへの依存等）
　我が国の情報セキュリティにおいても、対策面では体系的構築されつつあることを評価できるが、セキュリティ関連製品の国産化（暗号技術、ＮＷ製品）には諸外国に遅れをとっている。
２．について：
　具体的な実践がなかなか表面に出てこないため、一般論的に言えば、投資効果があり評価されているとは言えない。（水面下ではそのようなことは無いのかもしれないが）
３．について：
　大いに推奨していくべきことと考えるが、やはり、実践あっての開発ということになる。
４．について：
　利便性だけを追及するＩＴではなく、セキュリティを意識した提供が今後の展開すべき方向ではないかと思う。
５．について：
　第１次で提唱していることを積極的に展開してほしい。

６．について：
第１次で提唱していることを積極的に展開してほしい。
７．について：
まずは、方個性を明確にした上で、何に投資するのかを判断すべきであり、ここにもＩＳＭＳ的な思考要素を組み込む必要がある。
８．について：
民間に対し、国家プロジェクトの一環であることを明確にした上で、必要に応じて投資を行わなければならい。（費用の配分に十分注意すること）
９．について：
現在のセキュリティ対策の一環からは、今の段階では少し距離を置くことも検討されたい。ただし、新規領域への取り組みに対する全体の体力があればその限りではない。
１０．について：
研究成果は、広く公開すべきであり、国民に後押しされるようでなければならない。
また、有効な技術は、それを導入することを推奨し、迅速に実践（市場）に展開すべきである。

○情報セキュリティ分野における人材育成について
～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。

＜意見＞
◇各コメントに関して
１．について：
徐々に人材育成がなされてきたと評価できるが、まだまだ発展途上であるとともに、カテゴリ別の人材育成像が明確になっているのか、それらに対する育成カリキュラムは構築されているのか等が課題である。
２．について：
まずは、段階を踏みながら推進していくべきであることと、ターゲットの具体化も併せて明確にしていかなければならない。（官民等の一般社会人、学生、をまずは先行させていくのか？）
３．について：
現在のところ、一応セキュリティ教育を実施しているといった状況であり、それらで教育された内容が理解され、行動に定着しているかどうかは今後の課題である。
４．について：
製品に関するセキュリティ知識、開発者、管理者としてのセキュリティ知識、利用者としてのセキュリティ知識をいったカテゴリを明確して、それぞれの教育カリキュラムを構築、活用していかなければならない。
５．について：
まだまだ表面的であり、十分とは言いがたい。組織の長の意識をもっと高め、これらのことを実施していくことの重要性をもっと認識すべきである。

６．について：
　少人数でも対応でき、費用負担を軽減させるために、ガイドラインや教育カリキュラムの提供を検討すべきである。

○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。

＜意見＞
◇各コメントに関して
１．について：
　今後も推進していかなければならないことであり、さらに発言力も高めていかなければならない。
２．について：
　ＩＴ先進国ではあるが、情報発信に関しては後手にまわっていると思われがちである。内外の研究機関、機構等への情報発信も積極的に行わなければならない。
３．について：
　我が国の政策が評価されることにより、政策そのものが実体化し、最終的には利益（国益も含めて）に繋がると思われる。
４．について：
　まだまだ、標準化の主導はＥＵ（特にセキュリティにおいてはＢＳ）がもっており、我が国は、それを翻訳（多少、異見も上げているが）する程度に留まっている。
５．について：
　十分評価できるが、まだまだ先進的とは言えない、若しくは広く国民に理解されていない。

○情報セキュリティ分野における犯罪取締り、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。

＜意見＞
◇各コメントに関して
１．について：
　今後も国際協力を推進していくとともに、国際法的な視点またはそのものを確立し実行していかなければ、全世界同じ尺度で裁けない。
　サイバー空間がグローバルである現状で、それを裁く法律もグローバルでなければならない。
２．について：

例示されている内容はもちろん重要であるが、さらに、例えば、ログの保存を要求するのであれば、その手法、内容も含めさらには、ＩＴ製品の中に、利用者の負荷のかからない仕組みを組み込むことを提唱し制度化していくことで、確実かつ安全に取得できることを推進していかなければならない。

３．について：

各々の法律等に対する矛盾（例：個人情報保護、プライバシー保護と情報セキュリティ権等における開示権）をいかに埋めることができるかが課題となり、法令等の条文では表現しきれない部分は、範例をもって対応していかなければならない。

４．について：

上記「３.」と同様。

○その他の検討の視点

～その他として、どのようなものの検討が必要か。

＜意見＞

◇各コメントに関して

１．について：

「情報セキュリティ基本法」は必要と考えます。また、「ＩＴ基本法」への組み込みと考えるにあたって、本当にセキュリティに関する範囲を網羅できるか（ＩＴだけが情報セキュリティではないということ）が疑問です。

２．について：

各種法律の整合がなされているとは思えません。各法律はその分野に特化した内容で構成されているため、多様化した情報セキュリティ分野を裁ききれないと判断します。むしろ、関連法の統廃合を行う段階にきているのではないかと思います。

３．について：

外部委託に関する一般法は必要と考えます。さらに、その対象は、全ての組織とすべきであると考えます。

４．について：

その通りである。

５．について：

上記「２.」と同様。

６．について：

前にも述べたが、学校教育、企業教育、それ以外の人々に対する教育を充実させることが重要であり、さらに、政府発行のガイドライン（ハンドブック的な簡略化された冊子）の配布も有効かと思います。

７．について：

現状、米国依存であることは仕方が無いが、国産ものを考慮するか、若しくは、どこの国のもでも構わないので、国防と切り離された中立的な仕組みで提供されるものを利用すべきである（プライバシー保護）。

８．について：

資産に対する価値評価（金銭的）のガイドラインを提示し、事例等を用いて広くそれを提示していくことで認識を高める。

９．について：

一般的通例（各国際規格の更新タイミング）と併せて概ね３年が妥当であるが、常にそれを評価する組織が必要であり、必要に応じて適宜更新する仕組みも必要である。

１０．について

現状の推進体制の中で、特に「内閣官房情報セキュリティセンター」の権限を強化し、全体統制を取るべきと考えます。

各府省は、それに準拠するかたちを継承し、省庁別に似通ったガイドラインを発行することの無いように統制すべきです。（必要に応じて、個々に特化した内容であればそれは歓迎します）