「第２次情報セキュリティ基本計画（案）」に対する
提出意見の概要及び御意見に対する考え方

情報セキュリティ政策会議
２００９年２月３日

意見提出者一覧（五十音順）

(ISC)2　Japan
株式会社インフォセック
株式会社ラック
社団法人情報処理学会
社団法人日本経済団体連合会
情報セキュリティ教育事業者連絡会
日本ネットワークセキュリティ協会
日本弁護士連合会
日本ユニシス株式会社
富士通株式会社

その他個人２件

第1章　第1次情報セキュリティ基本計画下での取組みと2009年の状況

該当箇所		ご意見の概要	ご意見に対する考え方
第1章　第1次情報セキュリティ基本計画下での取組み　第1節	ページ5、第1章第1節(4)	利用者が安心を実感しながらITを利用・活用できる環境することを～ → 利用者が安心を実感しながらITを利用・活用できる環境を構築することを～ （日本ユニシス株式会社）	御意見ありがとうございます。 御指摘のとおり、修正いたします。
第2節　2009年の状況	(2)　6行目	「グランドチャレンジ」という用語説明はP59で記述されていますが、P16で記述していただきたい （日本ユニシス株式会社）	御意見ありがとうございます。 御指摘のとおり、修正いたします。
	ページ21　脚注23	「Meridian」の説明を追記していただきたい。 （日本ユニシス株式会社）	御意見ありがとうございます。 御指摘を踏まえ、以下のとおり修正いたします。 「その他、G8、ITU、重要情報インフラに関する国際会合(MERIDIAN)においても、」
	21ページ　第2節　③国際連携・協調の推進	国際連携・協調していくに当っての、日本国としての大きな貢献の一つに「優秀な人材の輩出」という事があるかと思うのですが、現実的には、国際的に貢献できる人材を育成し、輩出できているかについては課題として挙げられるのでないでしょうか。 ((ISC)2ジャパン）	御指摘の点は重要と認識しており、21－22ページに記載される課題を解決するための人材は不可欠であることに同意します。一方で、国際貢献に当たっては、どのような分野で貢献を行うかについての議論を待たずに、人材を育成することを目標にする場合、人材像が非常に曖昧になり効果的な施策とならない可能性があることも踏まえ、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。

第2章　第2次情報セキュリティ基本計画における基本的考え方と2012年の姿

該当箇所		ご意見の概要	ご意見に対する考え方
第1節　第1次情報セキュリティ基本計画からの移行	・事故前提社会を仮定した(p. 27)について	現状の観察や課題の抽出は的確だが，それに対する対策が不明確である. 具体的な対策案が望まれる. （社団法人情報処理学会）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。なお、御指摘を頂いた箇所は、課題の抽出及び必要な対応の方向性について述べたものであり、第3章において具体的な取組み（重点政策）について述べていますので、併せて御参照頂ければ幸いです。また、更に具体的な施策については、当該基本計画の下で毎年策定される年度計画に盛り込むこととなります。
	・「事故前提社会」への対応力強化（P27）	「万が一の事態においては，その影響範囲，影響の度合い，緊急度，原因などの事実関係を明らかにしつつ，迅速な対応・復旧を広く進めることで，事業継続性を確保する．」という記載がある. 「事故前提社会」への対応力のためには，対処方法の整備が必要であり，対処方法（技術面ならびに制度面）の整備についても言及して欲しいと考える. 例えば，ファイル共有ソフトの情報漏えいについては，情報漏えいのファイルを保有しているノードが特定できたとしても，そのファイルを削除するための仕組み（特に運用面）がない．また，意図的に，情報漏えいを助長する活動（Winnyで情報漏えいしたファイルをShareに再度流すなど）や，情報漏えいファイルの情報を元に誹謗中傷する活動など対処方法なども整備されないと， 「事故前提社会」への対応力強化という文字は，絵空事になってしまう. （社団法人情報処理学会）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。当方としましても「事故前提社会」への対応力を強化すべく、事故が発生した際の対処方法の整備が重要であるとの認識を持っております。具体的な対処ついては、行政がどの範囲まで関与するべきであるか、また、どの程度までコストを払うべきであるかなど、様々な場合を慎重に検討した上で取組みを考えていく必要があると考えております。
	(1)「事故前提社会」に向けて P27 「「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。」	現在も、日本の数多くのサイトで、サイト閲覧者がコンピュータウイルスを感染させるサイトに誘導されるような仕掛けの改ざんが多く発生している。改ざんを受けたサイトにて、適切にその危険性などを利用者に告知や啓発を行っているサイトは少数であり、風評被害などを恐れるあまり密かに対応を行いそのまま済ましていると見受けられるサイトも多い。 「事故前提社会」を適切に実現するためには、「事故」事実を隠蔽するのではなく、「事故」に関して過剰反応することなく粛々と対応できる社会を作ることが重要である。 その為には、発生組織レベルと事故の種類に応じた、適切な対外的な事故処理手順を明示し、適切な対応と情報共有できるフレームの再整備が重要と考える。また、風評被害などが発生しないように、或いは、万一発生した場合も適切に対応できるように、関係機関が強力にPR（社会とのコミュニケーション）出来る枠組みの準備も重要と考える。 （株式会社 ラック）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。当方としても、御指摘のとおり、『「事故前提社会」を適切に実現するためには、「事故」事実を隠蔽するのではなく、「事故」に関して過剰反応することなく粛々と対応できる社会を作ること』が重要であると認識しております。こうした目標に向けた具体的取組みについて、行政としてどのような取組みを進めることが適切であるか十分に検討を行ってまいりたいと考えております。
	ページ26　脚注30	（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。） →（ゆえに、適切な水準の対策であれば対策の徹底を行わなくても良い。） （日本ユニシス株式会社）	御意見ありがとうございます。 当該箇所は、「対策の徹底は難しいということを理由に開き直って、取り組むべき適切な水準の対策すら取り組まない（ということを認める訳ではない）」、という趣旨の文になりますので、原案のとおりとさせていただきます。
	P.27【③合理性に裏付けられたアプローチの実現】およびP.55【③企業（ア）情報セキュリティガバナンスの「経営の一環としての位置付け」の確立】	投資効率を測る手法としてROIの測定などが具体案として挙げられる。 従来のリスク分析手法では投資効果の観点が考慮されておらず、リスク対策に関して経営者は予算決定に苦慮していた。 リスク分析手法にROI等の投資効率を測る指標が導入された場合、この課題が緩和されると考える。 しかし、国内に留まらず諸外国を見渡しても情報セキュリティ投資に関する投資効率の測定データが不足している。 投資効率を測定するためのモデルを確立し、それらに関し実証実験をすることが必須と考える。 （株式会社インフォセック）	投資効率の測定データを増やすことをはじめ、情報セキュリティに係る投資効率を向上させることは、当方としても重要であると認識しており、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。当該論点について、様々な御意見や対応策等を十分に考慮しつつ、政策推進に努めてまいります。
	ページ27、第2章第1節(2)②	「事故前提社会」への対応力強化のため、万が一の事態に対する準備の一環として、実地訓練とまではいかなくてもシミュレーションなどによる机上訓練でもいいので、何らかの訓練を実施すべきことを記載していただきたい。 （日本ユニシス株式会社）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。 なお、重要インフラ分野については、第1次基本計画に引き続き、分野横断的演習に取り組んでいくこととしております。

	該当箇所	ご意見の概要	ご意見に対する考え方
第２節　２０１２年の姿	43ページ このニーズに対して、政府は企業が情報セキュリティ人材に係る環境整備・基盤整備をおこなうことで、企業における情報セキュリティ人材の育成・確保を推進している。	原文は、「企業が・・・・行うことで」「政府は・・・推進している」という構文になっており、意味不明になっていると思われます。したがい、「このニーズに対して、政府は、民間に出来る事は積極的に民間を活用する原則の下、民間における情報セキュリティ人材の教育育成、処遇、社会的評価、キャリアパスの形成等に係る環境整備・基盤整備をおこなうことで、企業における情報セキュリティ人材の育成・確保を推進し支援している。」というように記述することで整合を整えてはいかがかと考えます。 （ISEPA）	御意見ありがとうございます。 御指摘を踏まえ、以下のとおり修正いたします。 このニーズに対して、政府は情報セキュリティ人材に係る環境整備・基盤整備を行うことで、企業における情報セキュリティ人材の育成・確保を推進している。
	②情報セキュリティ人材の育成・確保	国として目指すセキュリティ人材像の大きな定義への言及がないように思われます。 育成していくという言葉は各所に出てきているのですが、理想として、また究極的に目指している人材とはどういう人達を指すのかについては定義をして頂きたい。もしそれが現在ないとすれば、どうやって定義を作っていくかについての提示が欲しいと思います。 （ISEPA）	御指摘の点について、情報セキュリティ人材における理想像を示す意義は大きいと考えております。その一方、情報セキュリティで必要とされる能力は分野ごとに多岐にわたることから、「国として目指すセキュリティ人材像」として、一様に定義することの実現可能性、そして、そもそも単一的に理想像を定義することの必要性を十分に見極めたいと考えております。 御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
	・「2012年の姿」－「対策実施4領域」－「企業」について	「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」を掲げている．その野心的な姿勢を評価したい． これを現実のものとするため，「世界トップクラスの水準」の定義を明確にする必要がある．現状では，リファレンスとする国・その状況，評価基準等が明らかになっていない． 「情報セキュリティガバナンスの経営の一環としての認識の定着」を掲げているが，現行の情勢を見るに，とくに昨今の世界的景気後退によって，セキュリティ対策が投資縮小の対象になりがちである．2012年までに「財務統制等と並ぶ経営上の重要な要素となっている」という状況を実現するには，政府が，これまで以上に，民間企業への適切な指導，投資喚起を行ってゆく必要を感じる． （社団法人情報処理学会）	御意見ありがとうございます。 御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。「世界トップクラスの水準」の実現には、情勢等の変化に応じ、適時適切な取組みが必要であると考えております。御指摘も踏まえつつ、実現のために必要かつ望ましい取組みについての検討を深めていきたいと考えております。
	・「2012年の姿」－「横断的な情報セキュリティ基盤」－「情報セキュリティ技術戦略の推進」について	「設計段階からセキュリティを作りこむ開発手法の普及と定義」が挙げられている．情報セキュリティについては，アドホックな対策，ピンポイントな対策が行われており，製品・システム全体を包括的に守る対策になっていない場合がある．何のための対策であるかを起点とするセキュリティ設計の重要性に着目した点を評価したい． 情報セキュリティ技術の発展は，これまで個別のテクノロジーの発展であった．しかしそれらを独立に採用しても，製品・システムを全体的に守る対策とはならない．それらを有機的に結びつけ総合的なモノづくりに反映しなければならないが，これを支えるセキュリティ『エンジニアリング』は未成熟であるといわざるを得ない．米国などでは，産学ともにこれを興そうとする動きが見られるが，わが国では不十分である． 「今後3年間に取り組む重点政策」には，「設計段階からセキュリティを作りこむ開発手法の普及と定義」を具現化する政策が盛込まれていない．今後の政策具体化に期待する． （社団法人情報処理学会）	御意見ありがとうございます。 「セキュリティを作りこむ開発手法の重要性」を御評価いただきありがとうございます。御指摘のとおり、当該の手法の普及のためには総合的な対策が必要であり、情報セキュリティ政策会議の技術戦略専門委員会を中心に議論を深め、実現に向けた戦略と具体的な施策、及びそれらの連携を図ることで、今後の政策運営に適切に反映してまいります。
	・「2012年の姿」－「横断的な情報セキュリティ基盤」－「情報セキュリティ人材の育成・確保」について	人材育成・確保の施策としてスキルフレームワークやキャリアパスの整備が進められているが，情報セキュリティ技術者の数・スキルは十分に向上していない． 情報セキュリティ分野がICT産業のなかで大きな利益を生む状況にないことなどから，必ずしも情報セキュリティ技術者は評価されにくい状況にあり，技術者はモチベーションの維持に苦心している． 国のセキュリティ政策を進める上で，実際の対策推進を支える人材が貧弱になってゆく状態を放置すると政策推進が根幹から立ち行かなくなる恐れがある．民間活力に委ねるだけではなく，政府自体が情報セキュリティ確保の主体事業者となり情報セキュリティ技術者の活躍の場を設ける施策をとることが望まれる． （社団法人情報処理学会）	情報セキュリティ分野から人材が離れていくと、国の政策推進にも支障をきたすという御指摘は、重要であると認識しております。御指摘の内容については、本計画にもあるように「優秀な人材が官民を問わず情報セキュリティ分野にすすんで集まること」を目指して、今後の政策の推進に当たっての参考とさせていただきます。
	（3）情報を預ける主体を念頭に置いたアプローチ P40 「第一に、『情報を預ける側の主体全体としての意識の向上』である。啓発活動やモデル契約書の提供などを通じて、当該情報を電子情報として預けることの必要性と万が一の場合のリスクの許容性について、個々の主体が無意識にある程度の注意を払うようになっている。 第二に、『対策知識が十分でなくとも情報を預ける際に安全が確保される技術的発展の実現』である。技術の発展により、意識的な対策をとらなくても預けた情報が保護されるようになっている。［参照：「（2）①情報セキュリティ技術戦略の推進」の2012年の姿］」	「事故前提社会」の推進を念頭に入れるならば、万一、情報流出が起きたときのリスクの許容だけではなく、サイバー社会で（ある程度の不利益は被るが）「生き返る」ような方策も根本的には重要かと考える。その上で初めて『（2）①情報セキュリティ技術戦略の推進」の2012年の姿』が活きるものと考える。 （株式会社 ラック）	発生した事故から回復するための方策も重要であるの視点は重要であると認識しており、今後、技術戦略専門委員会等の場において取り上げるなどして、御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。

	該当箇所	ご意見の概要	ご意見に対する考え方
	(5)情報セキュリティ人材の育成・確保 P42 「第2次基本計画の下で、社会全体のIT依存度の高まりを受けて情報セキュリティ人材の重要性が社会で十分に認識され、その業務が魅力的なものとして、優秀な人材が官民を問わず情報セキュリティ分野にすすんで集まることを目指して、政府をはじめ、各主体が種々の取組みを展開する。」	日本が向かう高度IT依存社会においては、高度な技術だけではなく、適切な倫理観・価値観を持った情報セキュリティ人材、並びにIT人材の育成は重要事項であり、このような方針で推進することを支持すると共に、当社においても積極的に取り組むこととする。 一方、倫理観・価値観を含めた人材の育成を図るためには、人材評価や資格などの枠組みにおいても、体系的に明示することが肝要かと考える。 (株式会社 ラック)	倫理観・価値観を含めた人材育成が重要であることは御指摘のとおりです。御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
	ページ33　第2章　第2節　4行目	のっとって述べる。 →則って述べる。 (日本ユニシス株式会社)	御意見ありがとうございます。 当方においては、公文書上、「のっとる」という語について平仮名で表記することを慣用としており、原案のとおりとさせていただきます。
	2-1 対策実施4領域	4領域に分けて考えられたことについては、責任を明確にするという点で今後も推進していただきたいと考えている。しかし、この4領域においては、小中学校などの教育機関においてどの省庁が主管となってセキュリティ対策を計画、実施しているのかが不明瞭である。国公立などは文科省など推測できるが、私立などはどうなっているのか。また、予算についても計画、実施の責任が文科省なのか、教育委員会なのか、自治体なのかなどわかりにくく対策が推進できていないのではないかと考える。対策実施4領域の中での教育機関の位置づけを明確にしていただきたい。 学校だけではなく、その他のすべての団体、企業などにおいて主管や責任を明確にする必要があるのではないか。 (日本ネットワークセキュリティ協会)	御意見ありがとうございます。 教育機関については、広い意味で、政府機関・地方公共団体の対策の一環として、対策を進めて頂いているところです。引き続き、基本計画で構築してきた枠組みを最大限活用しながらすべての主体における対策が進展するよう鋭意努力してまいりたいと考えております。
	42ページ　第2節　②情報セキュリティ人材の育成・確保	国として目指すセキュリティ人材像の大きな定義みたいな物への言及がないように思われます。育成していくという言葉は各所に出てきているのですが、理想として、また究極的に目指している人材とはどういう人達を指すのかについては定義をしていただきたい。もしそれが現在ないとすれば、どうやって定義を作っていくかについての提示が欲しいと思います。 ((ISC)2ジャパン)	御指摘の点について、情報セキュリティ人材における理想像を示す意義は大きいと考えております。その一方、情報セキュリティで必要とされる能力は分野ごとに多岐にわたることから、「国として目指すセキュリティ人材像」として、一様に定義することの実現可能性、そして、そもそも単一的に理想像を定義することの必要性を十分に見極めたいと考えております。 御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
	43ページ　第2節　③国際連携・協調の推進	前述でした国際的に通用する人材が不足しているとすると、そういった人材を育成していき、国際舞台で活躍できる人材が存在するのも2012年の姿として目指すべきなのではないしょうか。 ((ISC)2ジャパン)	国際連携・協調の推進に当たっては、その施策を実施するための国際的に通用する人材が存在することが重要であることは御指摘のとおりです。御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。

第3章　今後3年間に取り組む重点政策

該当箇所		ご意見の概要	ご意見に対する考え方
3章全般		機密性、完全性、可用性についての取り組みは理解できるものが多く、引き続き推進していただきたい。ただし、もう少し具体的な内容として、権限における認証についても特化して記述することはできないか。政府だけではなく、民間においてもどのような認証システムを取り入れるかの方針などを示していただきたい。また、認証基盤の構築についても官民連携で実施していただきたい （日本ネットワークセキュリティ協会）	御意見ありがとうございます。 御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。 なお、民間の取り入れる認証システムについて、取り入れるべきものを行政としてどこまで示すべきかという論点については、十分かつ慎重な検討が必要であると考えております。
第1節　対策実施4領域における取組みの推進と政策目的の着実な現実	1）PDCAサイクルの各プロセスにおけるマネジメントの強化	最高情報セキュリティ責任者、PMOメンバー、最高情報セキュリティアドバイザー、そのスタッフについては、情報セキュリティに係る共通言語が必要不可欠である。 20ページに記載の「人材育成・資格制度体系化専門委員会報告書」図8情報セキュリティに係る人材に求められる能力と各種教育プログラムの体系図や民間の人材育成に関するフレームワークを参照し、政府機関における適切な責務に応じた教育の実施と、必要とされる（もしくは取得が望ましい）資格を明確にして頂きたい。 その際には、図8に示されるように、民間の各種教育資格試験及びそれらに対応した教育機会が既に充実していることにかんがみ、それらに資格並びに教育の活用を推進することとして頂きたい。上記を推進することが、人材育成の充実と効率性を目指す上で望ましいと考えます。また、そのような民間の蓄積を活用することで、政府機関と民間の情報セキュリティ対策における言語の共通化、経験の共有、対策レベルの一貫性・統一性が実現するものと考えます。すなわち、セキュアジャパンを官民上げて追求する上でも、必須の要件ではないかと考える次第です。 同盟国である米国の国防総省（NSA）では、情報保証の管理に係わる要員を対象とした、情報セキュリティ関連の「情報保証要員改善プログラム」Directiv8570.1においてANSI/ISO/IEC17024スタンダードにもとづいた、ANSIあるいは同等の認定機関によって認証された民間の情報セキュリティ認定資格の取得を、国防総省に勤務するすべてのスタッフに義務化し、資格取得後も、一定の継続教育を受けることを義務化しています。適用範囲としては情報システムにアクセスを許可された外国人スタッフを含む、すべてのスタッフに適応され、100,000人が対象となっています。（国防総省当局の試算） 更に2007年度に10パーセント、その後毎年30パーセントのスタッフに、認定資格を取得させることを計画すると共に国防連邦調達追加規則（DFARS）に新たな条項を加え、IT納入業者に対する入札条件として、Directive8570に準拠した従事者がいることを義務付けています。（情報提供(ISC)2 Japan） 米国では民間の教育や資格を政府内で積極的に活用しセキュリティレベルを高めると共に、納入業者にも義務付けることで民間での利活用に拍車をかけて両者の共通言語 としているのです。日本においても政策の参考とすべきと考えます。 （ISEPA）	政府機関の情報セキュリティに係る人材に求められる能力を明確にする必要があることは御指摘のとおりであり、第3章第1節（1）①（ア）2）において、「政府機関における情報セキュリティ関連業務を調査・検証し、これらの業務に携わる人材に必要とされるスキルをまとめる」としております。 御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
	2）政府機関における人材の育成・確保及び職員の意識啓発	第1次情報セキュリティ基本計画　第3章　今後3年間に取り組む重点政策ー「新しい官民連携モデル」の構築 ［5］政府機関における人材育成　には以下が記載されています。 「政府として情報セキュリティ対策を一体的に進めていくために、必要な知見や専門性を有する人材を育成・確保することが重要であることにかんがみ、政府機関における情報システム管理部門の担当職員の育成、情報セキュリティに関する専門性の高い人材の活用、教育機関と連携した人材育成の取組み、幹部職員・一般職員の意識の向上方策等を推進する。なお、政府機関の情報システム管理部門において、情報セキュリティ対策業務に携わる専門的職員については、全員が情報セキュリティに関する資格を保有することを目指す。」 しかしながら「政府機関の情報システム管理部門において、情報セキュリティ対策業務に携わる専門的職員については、全員が情報セキュリティに関する資格を保有することを目指す。」は達成されていないことから、第2次基本計画においても引続き推進すべき内容と考えますので、第2次基本計画の「2012年の姿」への再記載と施策の推進を頂きたい。また、推進にあたっては民間の各種教育、資格試験の積極的活用を推進して頂きたい。同盟国である米国の国防総省（NSA）では、情報保証の管理に係わる要員を対象とした、情報セキュリティ関連の「情報保証要員改善プログラム」Directiv8570.1においてANSI/ISO/IEC17024スタンダードにもとづいた、ANSIあるいは同等の認定機関によって認証された民間の情報セキュリティ認定資格の取得を、国防総省に勤務するすべてのスタッフに義務化し、資格取得後も、一定の継続教育を受けることを義務化しています。適用範囲としては情報システムにアクセスを許可された外国人スタッフを含む、すべてのスタッフに適応され、100,000人が対象となっています。（国防総省当局の試算）更に2007年度に10パーセント、その後毎年30パーセントのスタッフに、認定資格を取得させることを計画すると共に国防連邦調達追加規則（DFARS）に新たな条項を加え、IT納入業者に対する入札条件として、Directive8570に準拠した従事者がいることを義務付けています。（情報提供(ISC)2 Japan）米国では民間の教育や資格を政府内で積極的に活用しセキュリティレベルを高めると共に、納入業者にも義務付けることで民間での利活用に拍車をかけて両者の共通言語としているのです。日本においても政策の参考とすべきと考え （ISEPA）	政府機関における情報セキュリティ担当者については、資格の取得を画一的に促していくよりも、政府機関の特性を考慮した上で情報セキュリティに係る人材の能力を向上させるための教育プログラムを整備・実施していくことが効果的であることから、今回の基本計画においては、御指摘の「政府機関の情報システム管理部門において、情報セキュリティ対策業務に携わる専門的職員については、全員が情報セキュリティに関する資格を保有することを目指す」ことについて記載しておりません。 御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。

該当箇所	ご意見の概要	ご意見に対する考え方
2）政府機関における人材の育成・確保及び職員の意識啓発	「人材育成・資格制度体系化専門委員会報告書」で提言されているように、政府機関における人材の育成・確保及び職員の意識啓発の推進にあたっては、教育・研修など民間の企業や各社団体の提供する教育機会や知識・経験・ノウハウのの積極的な活用を推進して頂きたい。 （ISEPA）	政府機関における情報セキュリティに係る人材の育成は重要であると考えており、第3章第1節（1）①（ア）2）において、「各政府機関においては、官民人事交流制度の活用による人材育成の促進のほか、階層別研修に情報セキュリティに関する内容を盛り込むなど、幹部職員も含めた全職員の情報セキュリティに関する意識の向上方策を、人事担当部局と情報システム部門の密接な協力の下に推進する」と記載しております。 御指摘のとおり、教育・研修等の実施に当たっては民間の知識・経験・ノウハウ等を積極的に活用することも有効な手段であり、各政府機関において階層別研修等を実施する際には、必要に応じて民間を積極的に活用していくものと考えております。
2）政府機関における人材の育成・確保及び職員の意識啓発 また、各政府機関においては、セキュリティ対策に係る民間専門家の活用を促進するため、最高情報セキュリティアドバイザーやそのサポートスタッフの活用などの戦略的なアウトソーシングを進めるほか、任期付き採用制度などの積極的な活用を図る。	セキュリティ確保に係る民間専門家の積極的な活用、アウトソーシングについては米国など諸外国を見ても一般的になってきており、官民交流、民需拡大の観点からも賛同致します。 （ISEPA）	御意見ありがとうございます。
（オ）独立行政法人等の情報セキュリティ対策の推進	48ページ～49ページ 「2）政府機関における人材の育成・確保及び職員の意識啓発」同様の推進を行うと共に、その推進にあたっては、「人材育成・資格制度体系化専門委員会報告書」で提言されているように、教育・研修など民間の積極的な活用を推進して頂きたい。 （ISEPA）	独立行政法人等においても、政府機関における一連の対策を踏まえ、情報セキュリティに係る人材の育成に取り組むことは重要であると考えております。 御指摘のとおり、教育・研修等の実施に当たっては民間の知識・経験・ノウハウ等を積極的に活用することも有効な手段であり、各独立行政法人等において階層別研修等を実施する際には、必要に応じて民間を積極的に活用していくものと考えております。
（カ）地域の情報セキュリティ対策の担い手の育成支援	いわゆる情報セキュリティ人材は企業の情報システムが首都圏に集中していることもあり、人材も首都圏に集中し地域格差が認められます。地方においても情報セキュリティ人材育成に係る各種教育や試験開催等のニーズはあるものの、民間が実施する際の広報や費用面において実施が困難な状況にある為、実施に関わる広報・費用の一定額を助成するなどの対策を講じて頂きたい。 （ISEPA）	地方においても必要な情報セキュリティ人材が育成・確保されることの重要性は、御指摘のとおりです。一方、人材育成・確保に当たっての環境整備としてどのような方法がふさわしいかについては、様々な方法が考えられることも踏まえ、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
（ウ） 情報セキュリティ人材が保有するスキルの見える化の推進 情報セキュリティ分野に人材を集め、高い能力を有する人材に支えられた情報セキュリティを構築するためには、長期的な視点から、情報セキュリティ人材が自らの能力を高めることが業務に結びつく様にし、人材の側からキャリアパスを描くことができるようにすることが有効である。 このため、実際の業務において求められるスキルを明確にするとともに、人材が保有するスキルが外部からわかりやすくするための政策を実施する。	インターネットはボーダレスであることは周知の事実であり、第2次基本計画においても国際連携・協調の推進を図ることの重要性を記載されており、人材育成においても「国際的に通用する人材育成」が必須と考えます。本文を以下に修正頂きたい。 「情報セキュリティ分野に人材を集め、国際的に通用する高い能力を有する人材に支えられた情報セキュリティを構築するためには、長期的な視点から、情報セキュリティ人材が自らの能力を高めることが業務に結びつく様にし、人材の側からキャリアパスを描くことができるようにすることが有効である。 このため、実際の業務において求められるスキルを明確にするとともに、人材が保有するスキルが国際的基準・視点を含め外部からわかりやすくするための政策を実施する。」 （ISEPA）	国際的に通用する人材の育成が重要であることは御指摘のとおりです。一方で、すべての情報セキュリティ人材に対して「国際的に通用する」ことが必須であると言えるかについては、「国際的に通用する人材」の具体的な中身と併せて検討する必要があることも踏まえて、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
（ウ）企業における情報セキュリティ人材の育成・確保 官民の適切な役割分担のもと、客観的な人材評価メカニズムである各スキル標準の整合化を図った共通キャリア・スキルフレームワークとそれに準拠した情報処理技術者試験の活用、及び民間の人材育成に関するフレームワークや各種資格試験の活用を促進する。	未曾有の経済不況による危機が日本経済をとりまく現状を鑑み、積極的に民間を活用しつつ、人材の育成・確保を推進頂きたい。 （ISEPA）	経済不況によって、必要な情報セキュリティ人材の育成・確保が滞ってはならないことは御指摘のとおりです。 御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
（ウ）企業における情報セキュリティ人材の育成・確保 官民の適切な役割分担のもと、客観的な人材評価メカニズムである各スキル標準の整合化を図った共通キャリア・スキルフレームワークとそれに準拠した情報処理技術者試験の活用、及び民間の人材育成に関するフレームワークや各種資格試験の活用を促進する。	情報処理技術者試験については「人材育成・資格制度体系化専門委員会」においても「一定の役割を果たした」との意見も出ており、同資格のみ個別名称を出して基本計画で推進するのは反対である。 （ISEPA）	当方としては、情報処理技術者試験の名称が記載されていることをもって、官民の適切な役割分担のもと企業における情報セキュリティ人材の育成・確保を行うという趣旨に反するとは考えておらず、原案のとおりとさせていただきます。 なお、「人材育成・資格制度体系化専門委員会」報告書においては、情報処理技術者試験について「一定の役割を果たした」と結論づけるものではなく、情報処理技術者試験には「一定の意義がある」との意見や「商業ベースの民間試験とは自ずと役割が違う」との意見が記載されており、様々な見解があることが明確にされております。

該当箇所	ご意見の概要	ご意見に対する考え方
(ウ)企業における情報セキュリティ人材の育成・確保 官民の適切な役割分担のもと、客観的な人材評価メカニズムである各スキル標準の整合化を図った共通キャリア・スキルフレームワークとそれに準拠した情報処理技術者試験の活用、及び民間の人材育成に関するフレームワークや各種資格試験の活用を促進する。	「官民の適切な役割分担」とあるが、これは「人材育成・資格制度体系化専門委員会」において検討された内容と考えます。「適切な役割分担」については、時代背景によって変化するものと考えられることから、継続的な検討が必要と考えます。本文に「官民の適切な役割分担という観点から、国家資格と民間資格の適切な役割分担及び経済的な視点からの国家資格の在り方の見直しについて、引き続き検討を行う」ことを追記して頂きたい。 (ISEPA)	当該箇所は、企業における人材の育成・確保について官民の適切な役割分担のもと政策を推進する旨が書かれた箇所となります。「人材評価・資格制度体系化専門委員会」と異なり、個々の資格制度のあり方について論じることを目的とするものではないため、個々の制度の見直しについて言及することが必ずしも適切ではないと考えており、原案のとおりとさせていただきます。
(カ)日系企業のグローバルな事業展開を支える情報セキュリティ政策の推進	グローバルな事業展開を支える上で、人材育成は欠かせません。例えば本社のセキュリティ責任者と諸外国支社のセキュリティ担当者が共通言語で会話出来なければ、セキュリティレベルは確保出来ないと考えます。取組みを推進するにあたり「セキュリティ人材の国際交流・協調プラットフォームの構築の推進」を追記頂きたい。 (ISEPA)	日系企業の海外における事業活動を支えるべく、高い水準の情報セキュリティ対策を実現するためには、経営者層における情報セキュリティ対策の認識の向上、社内のセキュリティ人材を含めた、「人材の育成」が必要な事項の一つであることは御指摘のとおりであり、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
②重要インフラ	重要インフラにおける人材の必要性に対しての記述が見当たらない。政府や企業同様、種々の対策を講じていくにあたっては、優秀な人材の確保は必須と思われます。 自社内育成及びアウトソースの両面での取り組みが可能かと思われますが、両方もしくは選択した1つのモデルでの育成・確保についての記述の追加を御願いしたいと思います。 (ISEPA)	重要インフラ事業者は、政府・企業としての側面も有するため、人材育成については、政府・企業それぞれの記述が該当します。 また、第2次行動計画(案)において、「人材育成については、演習・訓練及びセミナー等を通じて、高度なITスキルを有する人材の育成を図る」とされています。 御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
1. 地方自治体における情報セキュリティ対策の促進(P.52)	小規模な地方自治体も含め全ての地方自治体を対象として情報セキュリティ対策の促進に向けた具体的な施策を盛り込んでおり、特にベストプラクティスの共有や人的支援、人材育成を促進する支援を盛り込んだ点を高く評価する。 企業・個人にとっての行政の窓口は主に地方自治体であることに鑑み、地方自治体における情報セキュリティ水準を着実に底上げするとともに、今後は各地方自治体が自主的に情報セキュリティ対策の取組み状況を開示するなど、情報セキュリティ水準の「見える化」の促進に向けた仕組みづくりを推進すべきである。 ((社)日本経済団体連合会)	御意見ありがとうございます。 御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。国としてできることを十分に見極めつつ、検討を行いたいと考えております。
情報セキュリティガバナンスの「経営の一環としての位置付け」の確立(P.55)	情報セキュリティは今やIT統制、内部統制の観点から健全な経営に不可欠な要素の一つとなっていることに鑑み、経営層に対する啓発活動の推進等により経営者の意識向上ならびにISMSをはじめとする認証制度の普及を図るとした上で、政府自らが情報システム等の政府調達の競争参加者に対し、情報セキュリティ対策レベルの評価を入札条件等の一つとすることを明記した点は重要である。政府自らがこのような方針を示すことは、インセンティブの導入とともに、企業経営者の意識改革を促す効果があり、ひいては日本全体の情報セキュリティ水準の向上に繋がる。是非とも、中央省庁のみならず地方自治体も含めた全ての行政機関で同様の取組みを実践していただきたい。 ((社)日本経済団体連合会)	御意見ありがとうございます。 御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。国としてできることを十分に見極めつつ、検討を行いたいと考えております。
情報セキュリティ対策の定量的評価(P.55)	本計画で述べられている「情報セキュリティガバナンスのための取組みが企業にとって過度の負担とならないよう、投資効果を測る手法を実際に活用可能にするための検討を促進」すること、並びに「企業の情報セキュリティ関連リスクに対する定量的評価手法の実用化を目指した研究を促進」することに賛同する。本計画の柱の一つである「事故前提社会」への対応力強化を図るうえでも、何らかの定量的評価水準に関するコンセンサスは不可欠であり、喫緊の課題としてスピード感をもって取組んでいただきたい。 ((社)日本経済団体連合会)	御意見ありがとうございます。 御指摘のような取り組みは効果的・効率的な対策推進に役立つものと考えております。御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
標準化を含む戦略的国際貢献(P.64)	わが国はISMS認証取得数で世界一を誇るなど、取組みや経験を積極的に国際社会へ発信するべき立場にある。また、国際貢献を通じて標準化に寄与することは、国際競争力向上の観点から見ても重要である。標準化を図るためには、途上国においては情報通信インフラの拡充が不可欠であり、財政面のみならず人材面、技術面での支援も必要である。その際には、政府が先鞭をつけ、民間の投資を呼び込むようなフレームワークが必要となろう。したがい、国と企業が連携しながら戦略的に国際貢献できる体制の整備には、より具体的な施策・工程表を検討いただきたい。 ((社)日本経済団体連合会)	国際貢献を戦略的に実施するにあたっては、現地の状況、我が国の強み、その他に貢献を行う国の支援状況を踏まえた具体的な施策の検討が必要であり、検討に当たっては官民の連携が重要となる点は重要と認識しており、御指摘の内容については、今後の政策運営に適切に反映してまいります。
その他	・「IPV6化(p. 51)」は政府に言われなくても勝手に進むと思われる. V6にしてもセキュリティはなくならないのでは. (社団法人情報処理学会)	政府機関の情報システムのIPv6対応化については、「重点計画2008」(2008年8月20日IT戦略本部決定)においても記述されているところであり、今回は特に、IPv4からIPv6への移行期におけるセキュリティ上の課題に適切に対応することを記載しております。 御指摘のとおり、IPv6対応後においてもセキュリティの確保は重要であると考えており、今後の政策運営に適切に反映してまいります。
・「政府機関への成りすまし(p. 51)」について	GPKIの話題が出ていないのが不十分である. フィッシングがあれだけ進んでいる中で証明書を用いたメールの交換もそれほど進んでいないし, e-TaxなどのGPKIの証明書が現状の商用のものとあまりにかけ離れていて普及が進んでいないことにも触れるべきかと思う. (社団法人情報処理学会)	政府機関への成りすまし対策については、GPKIの活用も当然含まれております。御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。

該当箇所	ご意見の概要	ご意見に対する考え方
（2）国際連携・協力の推進 P57 「我が国企業がグローバルな事業展開を行うにあたり、日本国外のビジネス拠点において情報セキュリティを確保するための取組みを推進する。例えば、アジアなど我が国企業の事業活動に関係の深い国や地域を念頭に、円滑なアウトソーシングを行える環境づくりや、セキュアなネットワーク環境の構築へ向けた国際連携・協力を推進する。」	グローバル展開においては、各国の法律・文化・風習等を意識したマネジメントが必要で、海外現地従業員への教育や監督、IT運用、万一の場合の対応方法などは、日本式だけでは通用しないことも多い。個別の企業で全てを実施するのは非効率であり我が国の競争力低下を招く危険性もある。よって、国による国際連携・協力の推進は重要な課題であり、大いに賛同するものである。 ただ、推進にあたっては「事故前提社会」を念頭に入れ、予防策に対するだけではなく、事件発生時の対応に関する連携や協力も政府レベルで一層の強化を図っていただきたい。また、国外政府機関拠点におけるセキュリティ対策を率先して実施し、情報共有や枠組みの検証などを行い、海外進出企業への対策指針となるようにお願いしたい。 また、国際連携・協力は、多くの日本企業が進出するアジア地域だけではなく、アジア地域の犯罪者が拠り所としていると考えられる、犯罪モデルや犯罪手法を開発などする地域との連携も重要である。 （株式会社 ラック）	御意見ありがとうございます。 事件発生後の対応に関する連携や協力について、政府レベルで強化を図っていく必要があることについては御指摘のとおりです。 また、国外政府機関拠点におけるセキュリティ対策についても、国内の対策同様に、積極的に推進することを目指しており、さらに、アジア地域との連携については、企業の事業展開支援という観点に加えて、脅威への対応という視点が不可欠であるため、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
（4）中小企業の情報セキュリティ対策の推進 P57	中小企業といっても、ITが事業基盤でない（従来の）中小企業と、ネット事業者などに代表されるITを事業基盤とした企業とでは、セキュリティ対策の推進は異なると考える。 前者の場合はセキュリティよりまずはIT活用によるコスト削減や経営効率の改善を図ることが先決である。一方、サプライチェーンの関係で様々な発注元から様々なレベルの要求を突きつけられ効率を落とすようでは本末転倒であり、「事故前提」の元での統一的な指針を明確にすることが重要と考える。 後者の場合は、黎明期の企業や事業においては十分な予防的セキュリティ対策を実施することが事実上難しい時期が発生することも多い。 とはいえ、対策がなされていないため犯罪者が標的にしてくる危険性も高い。そこで、個人情報保護法等の適切な運用を行うと共に、「事故前提社会」を鑑みて、被害拡大防止・二次被害防止の観点で、処理できるフレームも重要と考える。 具体的には、個人情報取扱事業者でない、若しくは、ある水準以下のネット事業者に対する、事故処理手順を明示することが重要と考える。 （株式会社 ラック）	当方としても、事業形態、事業内容、保有する情報資産などに応じて、適切な対策がとられることが重要であると考えております。 なお、第２次基本計画の下では、自社の情報セキュリティレベルを客観的評価として提示するためのチェックリストの開発、普及を図るとともに、情報セキュリティ上の問題が発生した場合に必要な緊急時対応体制の強化を推進することとしており、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
（6）重要インフラ 分野横断演習に関して p.54 「第１次行動計画において得られた分野横断的な演習手法に関する知見を踏まえ、各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野のセプター等の協力を得て、IT障害の発生を想定した、重要インフラ分野横断的な演習を実施する。」	未曾有の経済環境悪化並びに今後の高度IT依存となることを鑑みると、従来の外部からの要因によるIT障害や事件・事故に留まらず、内部関係者或いは（退職者や受託者などの）元内部関係者による事件も視野に入れた演習も肝要と考える。 （株式会社 ラック）	具体的な演習の内容は、関係者や参加者の御意見を聞きながら検討していくこととしております。 御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
3-2-2 情報セキュリティ人材の育成・確保	政府機関の情報セキュリティ対策のための統一基準では、高情報セキュリティアドバイザーの設置といった具体的な役職名などが出ているが、その他にも情報セキュリティにかかわる様々な人材が必要になると考えられる。どのような人材がどの程度必要になってくるのかといった調査を行っていただき、必要な人材の育成に関する助言をいただきたいと考えている。また、情報セキュリティにかかわる業務における許認可など、資格制度についても検討していただきたい。 また、この分野においては特に専門家の職業倫理などを求められることもあり、それ担保する仕組みについても検討していただきたい。 （日本ネットワークセキュリティ協会）	情報セキュリティ人材について、必要となる人材を明確にすることが有益であることは御指摘のとおりです。一方、人材育成・確保のための環境整備については様々な方法が考えられるため、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
3-1-1　対策実施4領域	政府統一基準などによれば、各省庁からの報告書が一か所に集まり、情報共有をする機会があるように見受けられるが、これらを4領域までに広げるような施策はとることはできないだろうか。 企業においては様々なセキュリティ脅威を自社内だけの情報としていることが多いが、これらを共有することで事前対策がより効果的にできるのではないかと考える。 民間主導でこれらの情報共有を行うことは難しいと考えるため、政府主導での推進（情報セキュリティ報告書の提出など）を行ってはどうか。また、情報セキュリティ白書のようなサマリー文書が公開されるとよいと考える。 （日本ネットワークセキュリティ協会）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。当方としても、情報共有による各主体相互の水準向上効果については期待を有するところです。他方、行政が民間主体にどの範囲まで情報共有を要請するべきかといった論点は、十分かつ慎重な検討を行うべきものと認識しております。 なお、情報セキュリティ政策の取組みの結果について、社会状況等の変化も含めて、年度ごとの評価等を文書として取りまとめた上で公表しておりますので、御参照下さい。
47ページ　1）PDCAサイクルの各プロセスにおけるマネジメントの強化	最高情報セキュリティ責任者、PMOメンバー、最高情報セキュリティアドバイザー、そのスタッフについては、国際的に通用する情報セキュリティに係る共通言語の理解や素養が必要不可欠であり20ページに記載の「人材育成・資格制度体系化専門委員会報告書」図8情報セキュリティに係る人材に求められる能力と各種教育プログラムの体系図や民間の人材育成に関するフレームワークを参照し適切な責務に応じた教育の実施と資格取得を目指していただきたい。 ((ISC)2ジャパン)	各政府機関において、民間専門家を活用する際には、当該業務に求められる能力等が適切に判断されるものと考えております。御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。

	該当箇所	ご意見の概要	ご意見に対する考え方
	48~49ページ　2）政府機関における人材の育成・確保及び職員の意識啓発	第1次情報セキュリティ基本計画において「政府機関の情報システム管理部門において、情報セキュリティ対策業務に携わる専門的職員については、全員が情報セキュリティに関する資格を保有することを目指す。」という記述がありましたが、これにていてはまだ実現できるとは言えず、本基本計画においても継続すべき内容と考えますので、再記載と推進を頂きたい。 ((ISC)2ジャパン)	政府機関における情報セキュリティ担当者については、資格の取得を画一的に促していくよりも、政府機関の特性を考慮した上で情報セキュリティに係る人材の能力を向上させるための教育プログラムを整備・実施していくことが効果的であることから、今回の基本計画においては、御指摘の「政府機関の情報システム管理部門において、情報セキュリティ対策業務に携わる専門的職員については、全員が情報セキュリティに関する資格を保有することを目指す」ことについて記載しておりません。 御指摘の趣旨については、今後の政策の推進に当たっての参考とさせていただきます。
	48~49ページ　2）政府機関における人材の育成・確保及び職員の意識啓発	人材の育成・確保及び職員の意識啓発の推進にあたっては、議論を重ねた「人材育成・資格制度体系化専門委員会報告書」の意見を取り入れると共に、教育・研修など民間に出来る事は積極的に民間を活用する原則の下推進をして頂きたい。 ((ISC)2ジャパン)	御指摘のとおり、教育・研修等の実施に当たっては民間の知識・経験・ノウハウ等を積極的に活用することも有効な手段であり、各政府機関において階層別研修等を実施する際には、必要に応じて民間を積極的に活用していくものと考えております。
	49ページ前半　2）政府機関における人材の育成・確保及び職員の意識啓発 また、各政府機関においては、セキュリティ対策に係る民間専門家の活用を促進するため、最高情報セキュリティアドバイザーやそのサポートスタッフの活用などの戦略的なアウトソーシングを進めるほか、任期付き採用制度などの積極的な活用を図る。	セキュリティ確保に係る民間専門家の積極的な活用、アウトソーシングについては米国など諸外国を見ても一般的になってきており、官民交流、民需拡大の観点からも賛同致します。その際、活用に当っての基準においては、業務遂行に必要とされる知識の証明としての教育や資格保持を含んでいただきたい。 ((ISC)2ジャパン)	御意見ありがとうございます。 御指摘のとおり、最高情報セキュリティアドバイザー等に民間専門家を活用する際には、当該業務の遂行に必要とされるスキルの証明が重要な要素となります。各政府機関において、民間専門家を活用する際には、当該業務に求められる能力等が適切に判断されるものと考えております。御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
	53ページ後半　（カ）地域の情報セキュリティ対策の担い手の育成支援	いわゆる情報セキュリティ人材は企業の情報システムが首都圏に集中していることもあり、人材も首都圏に集中し地域格差が認められます。民間が地方において情報セキュリティ人材育成に係る各種教育や試験開催等を行う際にニーズはあるものの、広報や費用面において実施が困難な状況にある為、実施に関わる広報・費用の一定額を助成するなどの対策を講じて頂きたい。 ((ISC)2ジャパン)	地方においても必要な情報セキュリティ人材が育成・確保されることの重要性は、御指摘のとおりです。一方、人材育成・確保に当たっての環境整備としてどのような方法がふさわしいかについては、様々な方法が考えられることも踏まえ、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
	54~55ページ　②重要インフラ	重要インフラにおける人材の必要性に対しての記述が見当たらない。政府や企業同様、種々の対策を講じていくにあたっては、優秀な人材の確保は必須と思われます。自社内育成及びアウトソースの両面での取り組みが可能かと思われますが、両方もしくは選択した1つのモデルでの育成・確保についての記述の追加を御願いしたいと思います。 ((ISC)2ジャパン)	重要インフラ事業者は、政府・企業としての側面も有するため、人材育成については、政府・企業それぞれの記述が該当します。 また、第2次行動計画(案)において、「人材育成については、演習・訓練及びセミナー等を通じて、高度なITスキルを有する人材の育成を図る」とされています。 御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。
	56ページ（ウ）企業における情報セキュリティ人材の育成・確保 経営層の情報セキュリティ対策への理解増進とともに、企業の情報セキュリティ対策の推進を担う人材の育成・確保が必要不可欠である	インターネットはボーダレスであることは周知の事実であり、第2次基本計画においても国際連携・協調の推進を図ること人材育成においても「国際的に通用する人材育成」が必須であり、本文を以下に修正頂きたい。 「経営層の情報セキュリティ対策への理解増進とともに、企業の情報セキュリティ対策の推進を担う国際的に通用する人材の育成・確保が必要不可欠である」 ((ISC)2ジャパン)	国際的に通用する人材の育成が重要であることは御指摘のとおりです。一方で、すべての情報セキュリティ人材に対して「国際的に通用する」ことが必須であると言えるかについては、「国際的に通用する人材」の具体的な中身と併せて検討する必要があることも踏まえて、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
	56ページ（ウ）企業における情報セキュリティ人材の育成・確保 官民の適切な役割分担のもと、客観的な人材評価メカニズムである各スキル標準の整合化を図った共通キャリア・スキルフレームワークとそれに準拠した情報処理技術者試験の活用、及び民間の人材育成に関するフレームワークや各種資格試験の活用を促進する。	未曾有の経済不況による危機が日本経済をとりまく現状を鑑み、民間に出来る事は積極的に民間を活用する原則の下、人材の育成・確保を推進頂きたい。 ((ISC)2ジャパン)	経済不況によって、必要な情報セキュリティ人材の育成・確保が滞ってはならないことは御指摘のとおりです。 御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
	57ページ（カ）日系企業のグローバルな事業展開を支える情報セキュリティ政策の 推進	グローバルな事業展開を支える上で、人材育成は欠かせません。例えば本社のセキュリティ責任者と諸外国支社のセキュリティ担当者が共通言語で会話出来なければ、セキュリティレベルは確保出来ないと考えます。取組みを推進するにあたり「セキュリティ人材の育成に係るプラットフォームの構築の推進」を追記頂きたい。 ((ISC)2ジャパン)	日系企業の海外における事業活動を支えるべく、高い水準の情報セキュリティ対策を実現するためには、経営者層における情報セキュリティ対策の認識の向上、社内のセキュリティ人材を含めた、「人材の育成」が必要な事項の一つであることは御指摘のとおりであり、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
	62ページ　③国際連携・協調の推進	文中に「効率的・効果的な国際連携活動の推進」とう表現がありますが、この実施に必要な大きな要素として人材での貢献があるかと思います。「国際的な人材の育成により、より効率的・効果的な推進」が図れる事は間違いないかと思われますので、3つの観点からの取り組みに一つ「3つの取り組みを達成する為に、国際的に通用する人材の育成・確保を積極的に推進していく」追加していただきたい。 ((ISC)2ジャパン)	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。

第4章　政策の推進体制と持続的改善の構造について			
該当箇所		ご意見の概要	ご意見に対する考え方
第1節　政策の推進体制	67ページ　内閣官房情報セキュリティセンター（NISC）の強化と役割	政府全体の推進機能の有効に機能させるための中核として、国際POCであるNISC自らが人材育成の模範となるべきではないでしょうか。同時に民間人材の活用に当っての採用基準にはぜひ教育・資格の有無を含めていただける事を御願いしたいと思います。 （ISEPA）、（(ISC)2ジャパン）	NISCにおいては、情報セキュリティに関する技術的・専門的な知識・技能に優れた人材のみならず、そうした知識・技能に裏付けられた対策について、政府機関を始め社会全体として浸透させるための政策推進を果たせる人材を確保することが重要であり、採用基準に教育・資格の要件を含めることは必ずしも適当でないと考えております。
	NISCの権限強化（P.67）	日本経団連が予ねて主張しているように、NISCが政府全体の情報セキュリティ対策において果たす役割が極めて重要であることを鑑みると、省庁横断的に、より強力に情報セキュリティ対策を推進するための権限強化は不可欠である。そのためには、米FISMAと同様に、省庁横断的なガバナンスが有効に機能するような法制度の整備が必要である。また、引き続き民間の人材活用等を通じ情報セキュリティ推進体制の強化に努め、NISCの重要性を内外にアピールしていただきたい。 （(社)日本経済団体連合会）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。御指摘を踏まえつつ、情報セキリティ推進体制の強化に向けて、鋭意努力してまいります。

その他

該当箇所	ご意見の概要	ご意見に対する考え方
全般	冒頭に「第2次情報セキュリティ基本計画」（案）の取りまとめに尽力された、委員の皆様、NISC基本戦略策定チームの皆様、関係各省の皆様に敬意を表します。 今回の重要なキーワードである「事故前提社会」への対応強化は、インターネットが普及し国境が無い以上、大変重要な考え方であり賛同申し上げます。 （ISEPA）	御意見ありがとうございます。 御意見を踏まえつつ、「事故前提社会」への対応力強化が進むよう、このような方向性で政策推進に鋭意努力してまいります。
	要にある第1次計画の総括では、「関係者の気付きを高めた」「事前対策の取り組みはある程度進展」という記述があります。しかし、本当に効果はあがったのか？2008年、SQLの大規模攻撃があった際、世界で50万を越えるWebサイトが被害にあっています。その原因はソフトウェアの脆弱性です。これだけ脆弱性が露見してしまうのはなぜか？という点を、上記のような総括の前に考慮する必要があるのではないかと考えます。 （富士通株式会社）	当方としては、第1次計画の実施によって取組みはある程度進んだものの、リスクも日々変容していることから、常にリスクを把握しながら取組みを進めていく必要があるものと認識しております。また、ソフトウェアをに係るものをはじめ、脆弱性については社会全体として適切に対処が進むような取組みに向けて鋭意努力したいと考えております。御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
	政府統一基準では「新規ソフトウェアの開発」のみに注目しているが、開発済みのレガシーなソフトウェアでは、脆弱性が放置されている例が散見されます。これらの既存システムについても、点検、安全性確保の取り組みが必要になってくるのではないでしょうか。 （富士通株式会社）	過去に構築したシステムであっても、対策を行うことが必要であると認識しており、対策が現在未導入である場合は、各省庁において例外措置の適用を行うことにより代替策を含め検討することとしております。
	・必要性に疑問がある。 民間の情報まで、情報を共有化する「必要性」はない。 今の案では、むしろ「民間の情報すら国家が管理する」ことに繋がる可能性がある「ザル法案」です。 見直すべきです。 （個人）	御指摘は、主としてセプター、セプターカウンシルの取組みに係るものと理解いたしますが、これらにおいて情報共有するのは、個人情報のような情報ではなく、脆弱性に係る情報やIT障害の発生時の対応から得た知見といったものになります。こうした情報が適時適切に関係者に共有されることで、重要インフラサービス利用者である国民にとっても大きなメリットが生じるものと認識しております。また、情報の共有はあくまで各主体の自主的な御判断に基づくものであり、「国家」が情報管理するための取組みではないと考えております。引き続きの御理解をよろしくお願いいたします。
・POC(Point of Contact) について	どの分野で，どのような立場で振舞うことを意図しているのかが明確にされていない． 例えば，情報セキュリティ政策に関するPOC機能（P62）のPOCとは何を意図しているのだろうか． 先導者という意図なのか，諸外国の対応窓口になることを意図しているのか． 用語に振り回されることなく，役割について明記すべきであると考える． （社団法人情報処理学会）	POCは、国際連携を強化するにあたり、情報セキュリティ政策を横断的に取り扱うための窓口機能を指しております。様々な機関によって実施される情報セキュリティ政策について、我が国としての統一的なPOC機能が存在することが明らかであれば、国際連携強化の端緒となり得ると考えられます。POCの必要性については、最初に記載された第１次情報セキュリティ基本計画から変わるものではないため、引き続きその必要性について記載されております。
・POCについて	サービス主体者だけではなく，大学や個人的なサイトや小さな企業においてはそのPOCが徹底していないところが多くあるように思う． それらに対しての指導の役割は必要でないだろうか． （社団法人情報処理学会）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。当該論点は、行政が民間主体に対してどの範囲まで要請できるかということも含め、十分な検討を行うことが前提となると認識しております。
・CERTの表現について	国家レベルのCERT（P62）とあるが，CERTは，cert.orgの登録商標である．国家であろうが，企業であろうが，情報セキュリティのインデント対応という意図であるならば，CSIRTという表記を利用すべきである． （社団法人情報処理学会）	御意見ありがとうございます。 御指摘を踏まえ、以下のとおり修正いたします。 国家レベルのCERT→国家レベルのCSIRT
・個人への情報セキュリティ教育の強化・推進	児童・生徒の居ない家庭や高齢者などに対しても，学校の枠にとらわれない教育・啓発を推進することも必要ではないか． 携帯持ち込み禁止といったリスクをすべて排除するのではなく，リスクを認識し適切に対処できるスキルを養うための教育を推進してもらいたい． （社団法人情報処理学会）	第2次基本計画の下では、児童・生徒や保護者のみならず、幅広い層を対象とするセミナーや教室を通じた普及・啓発を、第１次基本計画に引き続いて進めてまいります。また、サービス等の利用において生じえるリスクを認識し、リスクを被害に変えない環境を整備することとしており、個人に対する啓発活動とともに、サービス提供事業者や対策支援主体によるリスク情報、対策情報の適切な提供、事故発生時の対応等の取り組みを進めてまいりたいと考えております。

該当箇所	ご意見の概要	ご意見に対する考え方
全般	・『個人分野では，第1次基本計画の下，「政府は，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」し，取組みを進めてきた．しかし，例えば，インターネット利用に不安があるとする個人は4割を越えている（図6参照）．』(p. 14)『（イ） 個人の底上げに向けたより効果的な普及・啓発活動の実現個人の底上げに向け，周知・啓発活動を，関係府省庁が更に連携し，より効果的に実施できるような取組みを進めていく．また，ITに関して必ずしも詳しくない個人を含めた一般利用者のセキュリティレベルを効果的に上げるために，質問への適切なアドバイスや訪問対応を行えるサポータの育成，地域団体ネットワークの実現を促進する．』ITに関して必ずしも詳しくない個人を含めた一般利用者のセキュリティレベルを上げなければいけないということは，「IT利用に不安を感じる」をゼロにつなげることはできないのではないか． ITに関して必ずしも詳しくない個人を含めた一般利用者のセキュリティレベルをあげなくてもよい，技術面や制度面の仕組みを整備することを考えることが必要に思われる． （社団法人情報処理学会）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。当方としては、技術面や制度面の仕組みの重要性も認識しており、例えば技術戦略の分野でこういった観点も踏まえた検討を進めていくこととしております。
・「重要インフラ」について	基本計画書の中では定義が明確でなく，行動計画書まで読まないと何を指すのか不明確．国や状況によって違うのだろうが，政策として重点を置くのはどこなのか絞れないものだろうか． （社団法人情報処理学会）	基本計画及び行動計画策定過程では、関係委員会等での議論も経て、大きな方向性については基本計画、具体的な内容については、行動計画にまとめるという形としております。こうした観点から、定義についても第２次行動計画にまとめる形としている点について御理解頂ければ幸いです。なお、第２次行動計画では、第１次行動計画に引き続き、「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む。）」、「医療」、「水道」及び「物流」の10分野の重要インフラを防護対象とすることとしております。 政策としての重点については、重要インフラサービスの維持、IT障害発生時の迅速な復旧等の確保に重点を置くこととしており、第２次基本計画に盛り込みましたように、（ア）「安全基準等」の整備及び浸透、（イ）情報共有体制の強化、（ウ）共通脅威分析、（エ）分野横断的演習、（オ）環境変化への対応の５つを取組みの具体的な柱としております。
・「政府機関への成りすまし防止」	発送する電子メールに電子署名を付与したとしても，政府機関を騙ったメールを無くすことはできない．受け取る側の不注意と責任を転嫁するように感じる． 根本的な解決策を検討する必要があるのではないか． （社団法人情報処理学会）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
・情報セキュリティ人材の育成・確保	情報セキュリティのスキルは，問題が起きなくてあたりまえ，起きたら責めを問われるというように，プラス的な評価を受けにくいところがある． モチベーションを高める取り組み，（育成側と被育成側双方に対する）インセンティブ制度といった，関係者がプラス思考になるような施策を推進してもらいたい． （社団法人情報処理学会）	情報セキュリティに携わる人材に対するインセンティブの重要性については、御指摘のとおりです。 御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
その他	・情報セキュリティセンター等で収集した障害情報/事例分析結果は，その成果の検証/評価と周知徹底ならびに広く再発防止を図るために，情報の公開と共有が必要と考える． （社団法人情報処理学会）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。情報を提供して頂く主体を含め、関係者と十分に検討を深めていくべき論点と理解しております。
・個人情報漏洩について	P2Pをはじめとする情報漏えいは一向に減少しないし，一度漏洩した情報の失効が出来ない状況は変わっていない．政府として，この状況に対する具体的な対策を図る必要はないだろうか． （社団法人情報処理学会）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
・主体識別コードについて	韓国の様に個人識別のためのフレームワークを国家レベルで推進している試みがある． 匿名性も重要だが，識別のための統一された識別子の必要性もある． 住民基本台帳ネットワークの普及度が低い日本では，その代用を検討する必要がないだろうか． （社団法人情報処理学会）	情報セキュリティの観点から有効に取り組むべきことがあるかを十分に見極めたいと考えております。

該当箇所	ご意見の概要	ご意見に対する考え方
第一次計画よりさらに「事故前提社会」への対応力を強化することに関して	従来の「事故ゼロを目指す」というアリバイ対策的な方針が強かった第一次計画から、万一を前提とし、より現実的なアプローチを狙う今回の第二次計画は、今後一層重要度が増すサイバー社会をリードする日本を作ろうとする気概の表れで、情報セキュリティ事業に携わる当社としても、大いに賛同する。 それは、100年に一度という経済危機の中、日本の今後10年を鑑み、社会コスト削減が大命題であると考えられる現在において、多くのサービスへの重要な役割を担うITは、単に「事故ゼロ」をスローガンにアリバイ対策的に予防策を叫ぶだけの政策は、社会コスト増の危険性も高く、現実を見据えた上で、対応力や生命力を身に付けていくことが、有効かつ経済的な政策であると考えるからである。 （株式会社 ラック）	当方としても、『単に「事故ゼロ」をスローガンにアリバイ対策的に予防策を叫ぶだけの政策』では、『社会コスト増の危険性も高』いことから、決して十分であるとは言えないと考えております。このような方向性で政策推進に鋭意努力してまいります。
その他	セプターカウンシルの創設及び独立性を保つ方策を早急に定めるべきである。いつまでに、どのようにカウンシルを立ち上げ、どのように運営するかをまず定めておく必要がある。そののちパブリックコメントを求めるのが筋ではないか。 （個人）	カウンシルの運営に関する事項はセプターカウンシル創設に際してセプターカウンシル自身が定めるものであり、政府の決定文書において定めるのは適当ではないと考えております。 御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。
	セプターカウンシルの事務局を政府が担うことは絶対に避けるべきである。民間の情報の管理を政府が行うことになり、戦前のように言論の検閲が行われる暗黒の時代を迎えることになりかねない。 （個人）	セプターカウンシルの事務局は当分の間内閣官房が担うこととされていますが、これはカウンシルの体制が充実するまでの間、事務的な支援を行うことが想定されたためです。セプターカウンシルは自らの決定により内閣官房以外に自由に事務局を置くことができ、またそのようになることが望ましいものと考えております。
	情報セキュリティ推進において、組織のマネージメントシステム導入は非常に重要な役割をもつと考えます。基本計画案では例としてISMS導入事業者の増加を例示してますが、QMSやEMSと比較するとまだまだその普及は不十分です。 これを打開するためには何らかのインテンシブを与えるとか、政府機関が率先してマネージメントシステム（第三者認証の）を導入するなどの対策が必要と考えます。 （個人）	御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。政府として当該論点についてどのように考えるべきか、検討を深めてまいりたいと考えております。
「第2次情報セキュリティ基本計画」（案）の基本的な考え方について	1 「第2次情報セキュリティ基本計画」（案）の概要 「第2次情報セキュリティ基本計画」（案）（以下「基本計画案」という。）は，「第2次基本計画における重要なメッセージの一つは，『事故前提社会』への対応力強化（第2章第1節を参照）である。これは，第1次基本計画の下での取組みが，事前対策に重点を置くような形で進められたことを受けて，万が一の事態における広い範囲での対応や復旧の準備にも注力することを意味する。もちろん，引き続き，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事前対策について最大限の努力を行う必要があることは言うまでもない。第2次基本計画を受けて，あらゆる主体は事前から事後まで，一貫した情報セキュリティ対策を進めることが期待される。」（基本計画案3頁）としている。 2 当連合会の基本的立場 このような基本的な考え方自体については，当連合会は賛成である。当連合会はトラブルは起きるという前提で対応を考えなければならないという意見を述べてきた。個人情報の漏洩などのトラブルが起きた際のことを考え，そのための予算，人員の確実な手当がなされる必要がある。 （日本弁護士連合会）	当方としても、「トラブル」の発生も踏まえた対応を考えなければならない」と考えている状況です。御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。情報セキュリティの観点から有効に取り組むべきことがあるかを十分に見極めたいと考えております。

該当箇所	ご意見の概要	ご意見に対する考え方
国の政府機関間，国と地方の機関間，官民間の情報の共有の範囲を明確にする必要がある。	1　政府機関・地方公共団体の重要インフラについて 　政府機関・地方公共団体の重要インフラについて、基本計画案では次のように記述している（基本計画案54－55頁。なお，「重要インフラの情報セキュリティ対策に係る第2次行動計画」（案）（以下「行動計画案」という。）15－20頁は、基本計画案を敷衍してやや具体的な記述がなされている。）。 「② 重要インフラ 　重要インフラの情報セキュリティ対策に関する関係主体は，第2次行動計画に基づいて，各々重要インフラサービスの維持に努め，またIT障害発生時の迅速な復旧等を確保することに努めることとする。また，情報セキュリティ対策の実施状況について指標を用いた検証を毎年実施するとともに，行動計画の評価を実施し，各々の取組みの継続的改善を図ることとする。これらについての具体的な取組みは第2次行動計画に詳述しているが，以下にその概要を示す。 （ア）「安全基準等」の整備及び浸透 　第1次行動計画で策定された指針について，事業継続の観点からの具体的内容の補充を含め，指針の位置づけや記載内容の具体性のレベルの見直しを行う。また，重要インフラ事業者等のPDCAサイクルとの整合性を踏まえた安全基準等の整備の推進などの底上げに資する取組みのみならず，3年毎に個別の先進的な対策を伸ばしその浸透を図る観点からの取組みも推進する。 （イ）情報共有体制の強化 　第1次行動計画で構築されたセプター，セプターカウンシルを含む関係主体間で共有する情報についての整理を行い，情報提供，情報連絡等に必要な環境整備等を推進するとともに，各セプター，セプターカウンシルの自主的な活動の充実強化を推進する。 （ウ）共通脅威分析 　第1次行動計画で実施してきた，ある重要インフラ分野にIT障害が発生した場合に他のどの重要インフラ分野に影響が波及するか，という相互依存性解析を継続するとともに，重要インフラ分野共通に起こりうる脅威が何であるかを把握するための検討を行う。 （エ）分野横断的演習 　第1次行動計画において得られた分野横断的な演習手法に関する知見を踏まえ，各重要インフラ所管省庁，各重要インフラ事業者等，各重要インフラ分野のセプター等の協力を得て，IT障害の発生を想定した，重要インフラ分野横断的な演習を実施する。 （オ）環境変化への対応 　社会環境や技術環境等の状況の変化に合わせて情報セキュリティ対策を機敏に対応させていくために，第2次行動計画策定時に想定しなかった環境の変化を察知する能力の向上に努める。また，こうした環境の変化に対して第2次行動計画の枠組みだけでは十分に対応できない場合は，内閣官房は必要な対応が可能となるような体制の検討を行う。」 2　国家機関内における情報共有についての懸念 　この基本計画案及び行動計画案で議論されていることは情報セキュリティの強化についてであり，ここで議論されている「情報共有」や「共通脅威」，「分野横断的演習」などもあくまで，情報セキュリティに関する技術的なものであると理解される。 　しかしながら，当連合会は国や地方公共団体に蓄積されている情報が横断的に共有されることについては，一貫して個人のプライバシーの権利への大きな侵害となる可能性を指摘し，警鐘を述べてきた。	第2次行動計画（案）は、「IT障害が国民生活や社会経済活動に重大な影響を及ぼさないようにすること」を目標として、「重要インフラ事業者等のサービスの維持」と「IT障害発生時の迅速な復旧等の確保」のために必要となる情報セキュリティ対策を具体化したものであり、情報共有についてもこの目標の範囲で行うことを想定しております。 　共有すべき情報としては、脆弱性に係る情報やIT障害の発生時の対応から得た知見といったものを各主体の自主性にのっとって共有することを想定しており、直接的に個人情報を扱うことは想定しておりません。 　御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。

該当箇所	ご意見の概要	ご意見に対する考え方
	例えば，第50回人権擁護大会（2007年11月2日）における「人権保障を通じて自由で安全な社会の実現を求める宣言」の本文においては，「国や地方自治体が，住民基本台帳ネットワークシステムや外国人の入国・在留管理などを通じて，また，国家間の情報の共有によって，あるいは市民や事業主からの報告を義務付けることにより個人情報を取得する制度が創設されつつあり，その情報を統合し，利用することが模索されている。憲法13条の個人の尊厳，幸福追求権の保障に含まれる自己情報コントロール権尊重の見地から，『改正』入管法などの制度の見直しを行うとともに，このような個人情報の統合，利用を厳格に規制し，特に警察などが市民の生活や思想を監視するために情報を利用することを防止すること。 また，国及び地方自治体などによる個人情報の取得，保管，利用に対する調査，是正命令などを行う権限を持つ，政府から独立した機関を設立すること。」を求め，決議理由においては，「警察は，通行する車両の移動をテレビカメラとコンピューターによって監視・記録・保存するNシステムによって，車両の位置情報を全国規模で入手することができる。また，国や地方自治体は，住民基本台帳ネットワーク（以下「住基ネット」という。）によって様々な個人情報を統合して利用することが可能となっている。 テロや犯罪を防止する社会体制を構築するためとして，『改正』入管法によって国が取得した外国人の指紋情報，顔情報と在留関係の様々な情報が，統合されて利用されることが可能となっている。さらに，銀行などが取得した個人の金融取引情報，監視カメラなどで取得した人の顔貌や所在などの情報，外国人の就労，就学情報などが国に集積され，市民の生活状況が国によって詳細に把握される可能性が高まっている。これらの情報は『改正』入管法の国際的な情報提供の規定などを通じて，国際的にも統合される可能性が生じている。このように，市民の生活情報，思想傾向などのデリケートな自己情報が，知らないうちに警察などの国の機関に集積され，名寄せされて，市民の行動や思想などが容易に把握されるという監視社会化が進む可能性が生じている。 これに対して，行政機関の保有する個人情報の保護に関する法律は，行政機関の取得した個人情報について法律の規定さえあれば，その実質的な理由の有無や相当性などにかかわらず他の行政機関に提供することを可能としており（同法8条），取得した情報の保有期間やデータの個人ごとの集約による生活状況の分析に対する規制も何ら規定していない。 この結果，市民は，一方で政治過程へ民主的に参加する上で必要不可欠な公益的情報から閉ざされながら，他方で個人のプライバシー権ないし自己情報コントロール権が侵害されるおそれが強まっている。」としている。 3　基本計画案及び行動計画案についての当連合会の疑問と見解 上記のような当連合会の基本的な立場から検討すると，基本計画案及び行動計画案には次のような疑問と懸念があると言わざるを得ない。 基本計画案及び行動計画案においては，国家機関間，国家機関と地方公共団体の間，官民間の情報共有の方法やそのためのルールについての考え方を述べたものとは理解されない。 しかしながら，基本計画案及び行動計画案の前記の部分を注意深く読めば，背後に何らかのデータベース結合の計画ないし実体が既に存在し，これらが現実に運用されるような状況の下で，このような統合されたネットワーク全体の情報セキュリティの向上を図ることを念頭に置いた計画となっているのではないかとの疑問を表明せざるを得ない。なぜならば，国家機関間，国家機関と地方公共団体の間，官民間の情報共有がなされていなければ，「情報共有」や「共通脅威」，「分野横断的演習」を議論する実益もないのである。	

該当箇所	ご意見の概要	ご意見に対する考え方
	少なくとも，当連合会としては，国家機関間，国家機関と地方公共団体の間，官民間の情報共有の方法については，その考え方やそのルールを明確にする必要があり，共有される情報がどのような性格を持った情報を含有し，どのような情報は含まれないのかを明らかにすべきであると考える。 また，「共通脅威」や「分野横断的演習」を問題とするのであれば，なぜ一つの脅威が共通の脅威となるのか，「各重要インフラ所管省庁，各重要インフラ事業者等，各重要インフラ分野のセプター等の協力を得て」行われるとされる「重要インフラ分野横断的な演習」が必要である技術的な背景として，各重要インフラ所管省庁，各重要インフラ事業者等，各重要インフラ分野のセプターがネットワークを通じてどのような結合・相互連携の状況にあるのかを明確にすることが必要であると考える。 そして，情報セキュリティの向上を図るだけでなく，このような活動を通じてプライバシー権ないし自己情報コントロール権に対する侵害が発生しないように，当連合会は前記の宣言において以下のとおり独立の第三者機関の設立を求めている。 「これに対して，EUでは，加盟各国に対して政府から独立した，情報保護に関する第三者機関の設置を指示し，各国においてデータ保護監察官（ドイツ連邦共和国）などが設置されている。多岐にわたるプライバシー権ないし自己情報コントロール権に対する侵害の問題については，その専門性，人権保障という準司法的性格に鑑み，日本においても，プライバシー権ないし自己情報コントロール権を保護する観点から，国及び地方自治体などによる個人情報の取得，保管，利用に対する調査，是正命令などを行う権限を持つ，政府から独立した第三者機関を設立するべきである。」 よって，このような情報セキュリティについての基本計画を立案する際には，この問題と密接に関連する自己情報コントロール権を保護する観点から，国及び地方自治体などによる個人情報の取得，保管，利用に対する調査，是正命令などを行う権限を持つ，政府から独立した第三者機関の設立を前向きに検討するべきである。 （日本弁護士連合会）	