「セキュア・ジャパン2009（案）」に対する
提出意見の概要及び御意見に対する考え方

2009年6月22日
情報セキュリティ政策会議

意見提出者一覧（五十音順）

株式会社ラック
クオリティ株式会社
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
日本セキュリティオペレーション事業者協議会
日本ユニシス株式会社
北陸無線データ通信協議会

その他個人５件

第１章　第一次情報セキュリティ基本計画（2006～2008年度）に基づく取組みと評価について			
該当箇所		ご意見の概要	ご意見に対する考え方
第２節　（１）施策の取組みによる社会的変化に関する評価・分析・課題	①政府機関・地方公共団体	「施策の取組みによる社会的変化に関する評価・分析・課題」に関し、政府機関・地方公共団体の評価は「概ね達成できている」とされているが、無線LANの運用を考える上で見識不足である。実際に４７都道府県及び市町村における無線LANの状況について調査を行ったが、多くの庁舎において問題のある無線LANが存在した。重要インフラ、企業においても無線LANの状況は地方公共団体と似た程度かそれ以下である。「政府・地方公共団体・各種団体・重要インフラ（病院・空港等）に免許不要の無線局の設置は原則として禁止する。」事（重要施設やそれに関わる職員の無線LAN使用の原則禁止）を強くお願いする。 （北陸無線データ通信協議会）	無線LANを含め情報システムの利用については、その利用主体が情報セキュリティポリシーに基づき、状況に応じて適切な管理を行うべきものと考えており、国において一律に禁止するものではないと考えております。なお、政府では、政府機関に対しては「情報システムの情報セキュリティ対策のための統一基準」を、重要インフラ事業者等に対しては「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」をそれぞれ策定し、所要の対策を講じるよう促しています。また、総務省では、「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」を策定し、無線LANの利用については、解読が困難な暗号化及び認証技術を使用するなど、適切な運用を行うこととしています。 なお、貴協議会の度重なるご意見もあり、地方公共団体における無線LANの利用については、適切な運用について周知を行ってきたところです。今後とも引き続き必要な普及啓発等に努めて参ります。
	③企業	国の政策として、政府や公共機関が率先してISMSを導入し、幅広い取引先に対してもISMSの導入を誘導する施策を実施し、その普及を国家として促進させるべきである。 （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。
	⑤情報セキュリティ技術戦略の推進	ASP、SaaS、クラウドコンピューティングといった最近のサービス技術においては、経路ハイジャック等の脅威の存在のしかたが、従来型のインターネット通信等とは異なると考えられる。そのため、対処方法については新たな研究が必要な場合と考えられる。また、小型の通信機器やストレージ機器が実現した今、発見しにくくなることは、管理者の知らない非許可のハードウェアの持込や接続を見過ごしやすくしているため、新たな脅威となるため、対処が必要と考えられる。 （個人）	新たなサービス・技術の実現により、新たな脅威が現れるということについては御指摘のとおりであり、当方としても問題意識をもっております。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。
	⑦国際連携・協調の推進	「情報セキュリティ関する」 →「情報セキュリティに関する」 （日本ユニシス株式会社）	御指摘のとおり、修正いたします。
	⑧犯罪の取締り及び権利・利益の保護	「一定範囲内に収」める →「一定範囲内」に収める （日本ユニシス株式会社）	誤表記との御指摘ですが、「第２次情報セキュリティ基本計画」から必要箇所を抜粋したものであるため、原案のとおりとさせていただきます。
		日本国内には推定で1200万台程度の無線LANアクセスポイントが存在し、暗号化無しの無線LANは約250万台であると推計できる。暗号化無しの無線LANは2005年頃と比較してほとんど変化していないという結果である。暗号化の無い無線LANが明確に減少傾向を示していない結果では何もしていないと変わらない。無線ＬＡＮの暗号化を進め、無線LANの安全を確保していただきたい。 (北陸無線データ通信協議会)	御指摘の内容については、今後の施策の推進に当たっての参考とさせていただきます。
第２節　（２）総評	「第一の課題については、…」	暗号化の無い無線LANを勝手に利用する事が問題化したことなどから、文部科学省は生徒児童に対する無線LANへの指導も追加しなければならない時になったと指摘する。また、不要不急の無線LANの設置利用は避け、国・地方公共団体・重要インフラは原則禁止すべきである。 （北陸無線データ通信協議会）	無線ＬＡＮの利用にあたっての情報セキュリティ対策に関しては、情報モラル教育の中で指導を行っております。 また、無線LANを含め情報システムの利用については、その利用主体が情報セキュリティポリシーに基づき、状況に応じて適切な管理を行うべきものと考えており、国において一律に禁止するものではないと考えております。なお、政府では、政府機関に対しては「情報システムの情報セキュリティ対策のための統一基準」を、重要インフラ事業者等に対しては「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」をそれぞれ策定し、所要の対策を講じるよう促しています。また、総務省では、「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」を策定し、無線LANの利用については、解読が困難な暗号化及び認証技術を使用するなど、適切な運用を行うこととしています。 なお、貴協議会の度重なるご意見もあり、地方公共団体における無線LANの利用については、適切な運用について周知を行ってきたところです。今後とも引き続き必要な普及啓発等に努めて参ります。
	「第二の課題については、…」	（本計画には「リソースの不足により情報セキュリティへの取組みが遅れている主体も観測されている。」との記述があるが、）リソース不足に陥った主体は、現行の経済状況悪化に伴い速やかに業務の停止を求める事ができる法律を制定すれば良い。一定基準に満たない主体はその主体が所属する業界・団体及び取引先全てに迷惑を掛けることになる。支援を行う事は必要であるが、支援しても明らかに手遅れな主体についても記述すべきである。 （北陸無線データ通信協議会）	リソースが不足している主体に対しての支援の在り方については、様々な観点からの検討が必要であると認識しております。
	「第三の課題については、…」	対策の社会的な効果のためには、各種調査・データの収集により可視化や専門外の人にも分かる様努力し、多くの人に継続して情報を出して行くことが重要です。自己目的化や硬直化は２の次、３の次に心がける事です。削除が適当かと考えます。 （北陸無線データ通信協議会）	各対策について継続的な情報発信を図ることにより、多くの方に御理解いただくことは対策の社会的効果のためには重要であると考えています。一方で、それと平行して自己目的化や硬直化を防ぐために情勢に合致した修正・変更を加えていくことも必要であると考えていることから、原文のままとさせていただきます。

第２章　2009年度に我が国が情報セキュリティ問題に取り組む上での基本方針			
該当箇所		ご意見の概要	ご意見に対する考え方
第１節　２００９年度から２０１１年度までの３箇年を通じた方向性	全般	事故前提社会の前に事故だらけで被害者激増の危機に直面するのは明白である。中には情報システムの停止により飛行機や列車が止まり、携帯電話やネット利用が停止する事が日常茶飯事になる事をあらかじめ生活の常識として下さいと言っているものと解釈する。安全の崩壊と公共利用施設への信用低下を前提とする社会に情報セキュリティまでそうしなさいというのは納得できない。 （北陸無線データ通信協議会）	「『事故前提社会』への対応力強化」とは、事故が有り得るから諦めて予防のための対策を行わないという意味ではなく、万が一事故が顕在化しても各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を行うことを意味するものです。
	②「合理性に裏付けられたアプローチの実現」への取り組み開始	一般には、対策の実施には、コストとの衡量が求められるが、政府機関では、法令順守や公平性の確保は金額換算が難しく、コストとの比較の妥当性が量りにくい。まかりまちがえても、政権奪取とか、議席数増加といった政治的な目標に使われないこと、既得権益の確保と組織防衛といった行政的な目標に使われないことが大切である。したがって、セキュリティ目標が何か明確にする研究が必要であると考える。 （個人）	今後とも、情報セキュリティ対策に関し、何をどこまで実現すれば良いかということについて公正な観点から検討を行い、コストと効果のバランスのとれた対策実施に向けて取り組んで参りたいと考えております。
	全般	我が国において，民間を中心とした情報セキュリティ対策のベストプラクティスの表彰，あるいはベストプラクティス集（「××100選」など）の発行などを推進・強化いただきたい。 （日本ユニシス株式会社）	民間を中心とした取組みを促進することは重要であると考えており、御指摘の内容については、今後の施策の推進に当たっての参考とさせていただきます。
第２節　３箇年の取組みの流れ	P12、P13	P12 真にＩＴを使いこなすことのできる「力強い「個」と「社会」の確立」を目指し・・・・・ P13 第２次基本計画の目指す「ＩＴ時代の力強い「個」と「社会」の確立」のため →「」で囲まれた表現を、どちらかに統一していただきたい。 （日本ユニシス株式会社）	御指摘の点につきましては、第２次基本計画からの抜粋箇所が異なるためであり、原文のとおりとさせていただきます。

第３章　対策実施４領域における情報セキュリティ対策の強化			
該当箇所		ご意見の概要	ご意見に対する考え方
第１節（１）①政府機関・地方公共団体	〔政府機関〕 （ア）全ての政府機関において能動的に情報セキュリティ対策に取り組む体制の確立 ア）情報セキュリティガバナンスの確立に向けた取組 （全府省庁）	情報セキュリティアドバイザーおよびスタッフの制度については、情報化統括責任者（ＣＩＯ）補佐官（※情報セキュリティに関しても外部専門家の位置づけである）制度との関連の整理が必要である。制度自体も、似通っているため、運営状況の長所・短所（うまくいっている点、そうでない点）をよく見極めて導入すべきと考える。 （参考） 電子政府構築計画　P21（2003年7月17日、各府省情報化統括責任者連絡会議） CIO 補佐官には、業務分析手法、情報システム技術及び情報セキュリティに関する専門的な知識・経験を有し、独立性・中立性を有する外部専門家を充てることとし、高度な国家安全保障、治安に係る分野においては内部人材の活用を図ることとする。 （http://www.kantei.go.jp/jp/singi/it2/cio/dai4/4siryou2.pdf） （個人）	最高情報セキュリティアドバイザーと情報化統括責任者（ＣＩＯ）補佐官は兼務することも想定しており、各府省庁の実情に応じて設置されるものですが、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。
	〔政府機関〕 （イ）政府全体を通じて情報システムに情報セキュリティ対策が適切に組み込まれる仕組みの構築	今回のSJ2009においては、政府機関における取組の一環として、「政府全体を通じて情報システムに情報セキュリティ対策が適切に組み込まれる仕組の構築」が示されています。 「情報システムの構築や運用段階のみならず、企画・設計段階からの情報セキュリティ（略）」の記述には、「企画→設計→構築→運用」の包括的な視野を見据えた情報セキュリティ対策の検討の重要性が弱まる印象があります。セキュリティオペレーションのサービスを提供する立場からは、「情報システムの構築や運用までを視野に入れた、企画・設計段階からの（略）」に変更していただけるよう、ご検討をお願い申し上げます。また、あわせまして、【具体的施策】ア）の表題につきましても、「情報システムの構築や運用までを視野に入れた、企画・設計段階からの情報セキュリティ対策の組み込みについても意識するための方策の検討」への変更につき、ご検討いただくようお願いいたします。 （日本セキュリティオペレーション事業者協議会）	「企画→設計→構築→運用」を包括的に見据えた情報セキュリティ対策の重要性については当方も認識を同じくしています。しかし、ここでは企画・設計段階からの情報セキュリティ対策の組込みを取り上げさせていただいています。御指摘の内容については、今後の政策の推進にあたって参考とさせていただきます。
	〔政府機関〕 （ウ）電子政府の利便性･セキュリティレベルの向上	「電子行政のセキュリティ確保」 日本経団連では電子行政の実現に向けた積極的な活動を行っている。今後電子行政推進の大前提となる国民・企業ＩＤの早期導入に向けた検討が活発化すると思われるが、広く国民の理解を得るためにはセキュリティの確保が不可欠である。社会保障番号、納税者番号制度、国民電子私書箱などの検討の段階からNISCが参画し、安心なシステム構築に貢献すべきである。 （(社)日本経済団体連合会）	ＮＩＳＣにおいては、「電子政府ガイドライン作成検討委員会　セキュリティ分科会」の事務局として運営に参加するなど、今後も電子行政のセキュリティ確保に検討段階から参画してまいります。
	〔地方公共団体〕	「地方自治体における情報セキュリティ対策の促進」 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み、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。 予算や人員の限られている地方公共団体の対策を推進するために、例えば、地方自治体が標準的に保有する情報資産類（例：住民基本台帳、固定資産課税台帳等）を列挙し、それごとに、セキュリティ上望ましい媒体形態・保有場所を例示して、容易にリスク管理できるような方法・書式等を開発・提供することなども考えられる。 （(社)日本経済団体連合会）	本年３月に、「地方公共団体における情報資産のリスク分析・評価に関する手引き」を作成し、提供しています。 この手引きでは、情報資産を把握し、リスク分析を行い、情報セキュリティ上適切な取扱いをすることとしています。 今後は、地方公共団体におけるこの手引きの活用を推進していくこととしています。 御指摘を踏まえ、本計画第３章 第１節（１）①〔地方公共団体〕（ア）ア）地方公共団体の情報セキュリティ対策水準向上のための普及・啓発 にも施策の内容が明確に表れるよう、下記のとおり修正いたします。 地方公共団体における情報システム部門の業務継続計画の策定、情報資産台帳の作成及びリスク分析の実施等の促進を図るため、全国数か所において、情報セキュリティに関するセミナーを開催するとともに、「地方公共団体における情報資産のリスク分析・評価に関する手引き」の活用を推進する。
重要インフラ　第１節（１）②	（イ）情報共有体制の強化	セプターの注記を最初に現れるP4へ移動していただきたい。 （日本ユニシス株式会社）	御指摘のとおり、修正いたします。

該当箇所		ご意見の概要	ご意見に対する考え方
第１節（１）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	情報セキュリティマネジメントシステム（ＩＳＭＳ）適合性評価や「情報セキュリティ監査」、ＩＴセキュリティ評価及び認証制度 →　「情報セキュリティ監査制度」と「制度」を付加していただきたい。 （日本ユニシス株式会社）	御指摘の箇所については、第２次情報セキュリティ基本計画から抜粋しているところであるため、原案のとおりとさせていただきます。
		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、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。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すべきである。 （(社)日本経済団体連合会）	御指摘の内容については、今後の施策の推進にあたって参考とさせていただきます。
	(イ)企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進 エ）組込みソフトウェアの安全性向上のための取組み（経済産業省）	「情報家電の組込みソフトウェアのセキュリティ問題の今後、情報公開方法、指導面などを集中的に検討する組織を立ち上げる」などの問題対処方策を追記していただきたい。 （日本ユニシス株式会社）	御指摘の本項については、今後の政策運営において検討してまいります。
	(イ)企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進	ク）信頼性を評価するための共通の評価指標の確立 ク）「SaaS向けSLAガイドライン」の活用・普及 →タイトル記号ク）の重複を修正していただきたい。 （日本ユニシス株式会社）	御指摘のとおり、修正いたします。
	(イ)企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進 ツ)非機能要求の合意手法の確立（経済産業省）	「非機能要求」という言葉の注記を追加していただきたい。 （日本ユニシス株式会社）	御指摘を踏まえ、以下のとおり修正いたします。 ※「非機能要求」の注記として、次の説明を追加いたします。 レスポンスタイム、バッチ処理の制限時間、あるいはユーザビリティといった情報システム・ソフトウェアの性能や品質に関する要求事項を非機能要求という。
	(イ）企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進に向けたより効果的な普及・啓発活動の実現 ウ)企業の運営するWebサイトの安全性向上（経済産業省）	webにおいてのセキュアコーディング技術が普及していないことからこれを向上する必要があると考える。 なお、企業のみならず、政府、日系企業のグローバルな事業展開に関しても同様である。 （個人）	御指摘いただきました点につきましてはＩＰＡ、ＪＰＣＥＲＴ／ＣＣ等を通じ実施に努めてきたところであり、今後も引き続き推進してまいります。
	(ウ)企業における情報セキュリティ人材の育成・確保 カ)民間のセキュリティ資格の周知（内閣官房、総務省及び経済産業省）	カ）・・・・・民間における情報セキュリティ「専門家の充実の観点」から、民間の情報セキュリティに関する資格の周知を図る。 →「専門家や監査人の充実の観点」と「や監査人」を追加していただきたい。 （日本ユニシス株式会社）	監査人が情報セキュリティにおいて重要な役割を占めることは御指摘の通りです。 しかし、情報セキュリティの専門家には様々な役割が存在し、資格も多様な専門家を対象にしたものが存在します。そうした中で、各種「専門家」から「監査人」だけをあえて強調することは妥当でないと考えるため、原案通りといたします。
	(ウ)　企業における情報セキュリティ人材の育成・確保 エ）情報セキュリティ・サポーターの育成（総務省）	情報セキュリティに関する教材作成や講習会・認定試験の開催を支援することにより、・・・（情報セキュリティ・サポーター）を育成 →　「教材作成や講習会・認定試験の開催を支援する」ことの他に、実務経験等が必要と思われ、「等」の追記または具体的な施策の追記をしていただきたい。 （日本ユニシス株式会社）	原文のとおりとさせていただきます。 実務経験を有する者がサポーターとなることは想定されますが、実務経験の取得支援を施策として実施することは予定しておりません。サポートを行うにあたっての技術の取得については講習会の中で取り入れていきたいと考えております。
	(ウ)　企業における情報セキュリティ人材の育成・確保 コ）モデルキャリア開発計画策定事業（経済産業省）	「・・・・専門家によるコミュニティを活用した情報セキュリティ人材を含めた高度IT 人材の育成の職種ごとにモデルキャリア開発計画を策定し、これらを広報・普及する。・・・・・」 →　書き方の変更をしていただきたい。 （日本ユニシス株式会社）	御指摘を踏まえ、以下のとおり修正いたします。 情報セキュリティ人材を含めた高度ＩＴ人材育成のためには、学生や若手技術者が将来のキャリアパスをイメージできるようにすることが重要であるが、ＩＴ産業におけるキャリアパスのイメージは他産業に比べて明確ではない。このため、専門家のコミュニティを活用することにより、職種ごとにモデルキャリア開発計画を策定し、これらを広報・普及する。

該当箇所		ご意見の概要	ご意見に対する考え方
第１節（１）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」 キ）入札条件等の見直し （内閣官房、総務省、財務省、経済産業省及び全府省庁）	政府調達におけるセキュリティ確保の一環として、競争参加者の評価を指標として挙げられております。入札の際の評価は大切ですが、公募全体を通して見た場合、安全性の確保の点から若干の補足が必要であると考えます。 公募で業者の選定終了後、一般的には業者との協議の上で細部を詰め、発注仕様書をもって正式な開発契約となります。この時、発注仕様書の内容についてセキュリティ的な観点からの評価は行われず、次に評価が行われるのは契約が完了し、実際に開発が開始されてからの設計フェイズとなります。　発注仕様書の作成において、府省庁の担当者が必ずしもセキュリティに長けているわけではありません。そのため、元の発注仕様にセキュリティ上の問題が内包されていた場合、契約上の問題により修正が困難となったり、やむをえずセキュリティレベルを下げる等という事態になる可能性があります。　発注仕様書の作成において、入札条件においてセキュリティ要件を備えていると判断された業者がセキュリティレビューを行うことで、誤った発注仕様を防止することができます。なお、入札時の選定が行われなかった場合など、セキュリティレビューを行うのは落札業者ではなく、第三者でも問題はありませんが、一般にその状態でのレビューは実行し難いと想像します。入札時の選定を前提として、契約前にあらかじめ落札業者等が適切に「発注仕様書のセキュリティレビューを行う」ことを入札手続きの一環として加えて頂くようお願いします。 （株式会社ラック）	御指摘の内容については、情報システムに係る政府調達案件の入札において情報セキュリティ対策を適切に考慮する方法の一環であると認識しており、今後の政策の推進にあたっての参考とさせていただきます。
第１節（１）④個人	（ア）情報セキュリティ教育の強化・推進 （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 （ウ）対策が困難な個人も含めた情報セキュリティ水準向上に向けた取組み	「ＩＴの利用・活用には積極的であるものの、リスクの認識や情報セキュリティ対策の重要性の認識が必ずしも十分ではない児童・生徒や保護者への教育・啓発を推進する。こうした観点も踏まえつつ、学校や地域における情報モラル等の教育を推進する。」とあります。それに応じて、具体的施策として様々な施策が挙げられておりますが、対象者についての分類が年齢や団体といった区分になっており、対象者の技術レベルが多岐に渡る項目がいくつも見受けられます。啓発と教育は必ずしも同じ対象者に行えるわけではありません。児童・生徒などに関しては啓発でまずは知ってもらうことが必要ですが、Webサイト運営者や製品開発者については、啓発がまず必要な層と、安全のための専門的な教育が必要な層が混在しております。混在したまま啓発・教育を行ったとしても中途半端な情報伝達となってしまう可能性は否めません。実施する対象者について、可能であれば目標となる技術程度を決定した上で「対象者の技術程度を明示し、施策ごとのレベル分けを明確化」した施策となるよう付記をお願いします。 （株式会社ラック）	情報セキュリティ教育を対象者の技術レベルを考慮しつつ実施する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、国として一様に技術レベルを定義することの実現可能性を十分に見極めたいと考えております。 よって、原文のままとさせていただきます。
	（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 イ）ランドマーク的イベントの実施	イ）ランドマーク的イベントの実施 a）・・・・・情報セキュリティに関する国民の意識の醸成を促進すべく、毎年２月２日の「情報セキュリティの日」の趣旨を踏まえ、これに伴う広報啓発的行事を全国的規模で開催する。 →ランドマークは、建物や空間が想像されるので、他の語彙の方がよいと思われます （日本ユニシス株式会社）	「ランドマーク」という言葉は「建造物等の陸上の目印」という意味に加え、「画期的な出来事」という意味も持っており、後者のニュアンスを出す趣旨で用いていることから、原文のままとさせていただきます。
	（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 ア)全国規模での広報啓発・情報発信の継続的実施 f)無線LANのセキュリティ対策（総務省及び経済産業省）	周知啓発だけでは暗号化の無い無線LANは絶滅はおろか減少すらしない。WEPのみしか暗号対策を行わない地方公共団体行政庁舎の無線LANは全体の7%以上と調査結果は出ており、早急な対策を国（内閣官房・総務省）に求めなければならない。総務省の指示により無線LANの利用状況について報告し改善を求めること程度であれば可能であるはず。 また、総務省は無線LAN機器を無線機とは扱わず、違法な海外無線LANについては啓発活動を「していない。」。これは総務省の組織的なサボタージュと市場拡大優先施策だと考えその間違いを指摘し大きな反動を招くと警告する。 最後に、WEP暗号化の解読手法の進歩により、無線LANセキュリティ問題は数多くのデータ流出を招くことになる。 （北陸無線データ通信協議会）	無線LANを含め情報システムの利用については、その利用主体が情報セキュリティポリシーに基づき、状況に応じて適切な管理を行うべきものと考えており、国において一律に禁止するものではないと考えております。なお、政府では、政府機関に対しては「情報システムの情報セキュリティ対策のための統一基準」を、重要インフラ事業者等に対しては「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」をそれぞれ策定し、所要の対策を講じるよう促しています。また、総務省では、「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」を策定し、無線LANの利用については、解読が困難な暗号化及び認証技術を使用するなど、適切な運用を行うこととしています。 なお、貴協議会の度重なるご意見もあり、地方公共団体における無線LANの利用については、適切な運用について周知を行ってきたところです。今後とも引き続き必要な普及啓発等に努めて参ります。 御指摘の内容については、今後の施策の推進に当たっての参考とさせていただきます。
第１１節（１１）③①企業　政府機関・地方公共団体	①（イ）政府全体を通じて情報システムに情報セキュリティ対策が適切に組込まれる仕組みの構築 ③（イ）企業の情報セキュリティ向上に資する製品やサービスの提供促進と活動の推進	「事故前提社会」における安全性の品質保証のため、重要度に応じて適切な「継続的な検証による品質の維持」を行うべきである。 （株式会社ラック）	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。また、脆弱性対策の重要性については、ＩＰＡ、ＪＰＣＥＲＴ等を通じ普及に向けた働きかけを実施しているところであり、こうした施策を今後も引き続き推進して参ります。

該当箇所		ご意見の概要	ご意見に対する考え方
第１１節（１１）③①企業	①（イ）政府全体を通じて情報システムに情報セキュリティ対策が適切に組込まれる仕組みの構築 ③（エ）「事故前提社会」への対応力強化に向けた事業継続性確保・緊急対応体制等の強化	「事故前提社会」におけるすみやかな発見と対応のため、ネットワークやコンピュータに対し、重要度に応じて適切な「日常的な監視による事故防止」を導入するべきである。 （株式会社ラック）	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。
第１１節（１１）③①政府機関・地方公共団体	・①(カ)1)政府機関の情報システムのＩＰｖ６対応化 ア)電子政府システムのＩＰｖ６対応化（内閣官房、総務省及び全府省庁） ・③(イ)企業の情報セキュリティ向上に資する製品やサービスの提供推進と活動の推進	SJ2009の、①政府機関・地方公共団体の「(カ) その他個別の情報セキュリティ対策の推進」「１）政府機関の情報システムの IPv6 対応化」及び③企業の「(イ) 企業の情報セキュリティ向上に資する製品 やサービスの提供推進と活動の推進」において述べられている IPv6環境移行に向けての検討に、セキュリティの運用面からの考慮も含めることも検討していただくようお願いいたします。 （日本セキュリティオペレーション事業者協議会）	情報システムの IPv6 対応化におけるセキュリティ面からの検討は重要であることから、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。
第１１節（２１）②③企業 テイ人材の育成・情報セキュリ確保	④企業 (ウ) 企業における情報セキュリティ人材の育成・確保 (オ) 中小企業の情報セキュリティ対策の推進	以下の施策を加えていただきたい。（３箇所） 「情報セキュリティに詳しいITコーディネータや中小企業診断士など、中小企業経営に関わる専門家による支援活動とその利用促進」 （日本ユニシス株式会社）	企業における情報セキュリティについては、様々な観点からの対策が必要と考えており、御指摘の内容については、今後の参考とさせていただきます。
	②情報セキュリティ人材の育成・確保 (イ) 企業における情報セキュリティ人材の育成・確保（再掲）		
第１１節（１１）④①政府機関・地方公共団体 利益の保護犯罪の取締り及び権利・	P.17、P.77	「情報セキュリティ報告書」の作成が、政府の施策（P.17）、および企業の施策(P.77)として、言及されている。いずれの施策も、情報セキュリティに関する取り組みを他者からわかりやすくするように開示するものであるが、NISCが各府省庁での情報セキュリティ関連の取り組みを把握するための施策である政府機関の「報告書」と、企業がステイクホルダーへの情報開示の一環として自発的に発行する「報告書」では、その記載すべき内容も、主体にとっての意義・位置づけも異なってくる。本施策の実施にあたっては政府各府省庁向け、企業向けの性格、位置づけの違いに留意したうえで取り組むべきである。 （(社)日本経済団体連合会）	政府機関における情報セキュリティ報告書に係る取組みについては、情報セキュリティ政策会議に情報セキュリティ報告書専門委員会を設置し、行政に対する国民の信頼の確保に向けて情報セキュリティ対策に係る説明責任を明らかにする観点から、その作成のためのガイドラインを現在検討しているところです。他方、企業における情報セキュリティ報告書に係る取組みについては、経済産業省において取りまとめた情報セキュリティ報告書モデルに基づき、施策を推進しているところです。このように、政府機関及び企業に対してそれぞれ対策を進めているところであり、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。
第１１節（２１）③①重要インフラの推進国際連携・協調	全般	国際的枠組みを活用したサイバー演習への参加を通じて、政府各府省庁や重要インフラ防護事業者の緊急時における対応能力を高め、そこで獲得した知見を、国内外の組織内CSIRT連携などを通じて、段階的に民間企業に対しても活用できるよう、NISCは環境整備と演習に対する理解を促進するような文化の醸成、普及・啓発活動を行うべきである。 （(社)日本経済団体連合会）	御指摘の内容については、今後の政策運営に適切に反映することを検討させていただきます。ＮＩＳＣにおいても、国際会合で得られた知見を国内に還元することは大変重要であると考えております。具体的には第３章 第１章(2)④(イ)の施策「ア）国内関係機関との連携強化（内閣官房）」にも記載しておりますので、併せて御覧いただけると幸いです。
第１節（２）②情報セキュリティ人材の育成・確保	(ア) 政府機関における人材の育成・確保及び職員の意識啓発 ア）政府職員向け教育プログラムの充実(内閣官房及び総務省)	教育プログラムについては、民間の各種情報セキュリティ教育プログラムを積極的に活用頂きたい。 （情報セキュリティ教育事業者連絡会）	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。
	(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 オ）民間のセキュリティ資格の周知（内閣官房、総務省及び経済産業省）	各種民間情報セキュリティ資格は情報処理技術者試験とも補完関係が築けると考えており。是非、積極的に民間のセキュリティ資格の周知拡大をお願い致します。 （情報セキュリティ教育事業者連絡会）	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。
	全般	「セキュリティアドバイザー資格の創設」 明確に資格化することにより、セキュリティアドバイザーの認知を促進できる。また、資格の取得に関してはISMS取得に関する知識・ノウハウを持つことを最低条件とするとともに、一定期間での更新制とするべきである。 （個人）	情報セキュリティ資格につきましては、現状においても官民の様々な資格が存在しております。こうした現状において、各種存在する資格に加えて「セキュリティアドバイザー」をあえて資格化することは、情報セキュリティ人材育成・確保の観点から必須ではないと考えております。
	全般	「個人の情報セキュリティ意識に関する全国的なテストの施行と結果の公表」 現在までに行われた政府主導の個人向けセキュリティ教室の成果が不明確である。どの程度の効果が表れているか国民が知ることのできる制度が必要である。 （個人）	個人向けの広報・啓発の成果を測定することが重要であるは御指摘のとおりです。しかし、その手段として全国一斉のテスト施行をすることが適切であるかどうか、実現可能性を含めて検討が必要と考えております。

該当箇所		ご意見の概要	ご意見に対する考え方
第1章第1節（2）③国際連携・協調の推進	(オ)標準化を含んだ我が国の戦略的貢献の実現	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る。したがって、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のために、より具体的な施策・工程表を検討すべきである。 （(社)日本経済団体連合会）	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。NISCは、総務省、経済産業省と協力してASEAN諸国との間で情報セキュリティ政策会合を開催し、我が国の強みを生かせる分野についての貢献を積極的に推進する等、国際貢献に向けた取組を行っているところです。今後も、機会を捉えて、官民が連携しながら、貢献の具体化に向けた検討を行っていく予定です。

第４章　横断的な情報セキュリティ基盤の形成			
該当箇所		ご意見の概要	ご意見に対する考え方
第１節（１）内閣官房情報セキュリティセンター（ＮＩＳＣ）の強化と役割	ア）ＮＩＳＣの強化（内閣官房）	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が不可欠である。そのためには、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すべきである。 （(社)日本経済団体連合会）	ＮＩＳＣがセキュリティ対策において果たす役割を評価いただきまして、ありがとうございます。今後とも、現在の施策の効果を踏まえつつ、今後のＮＩＳＣの在り方についても検討して参ります。また、政府全体の情報セキュリティ対策の推進体制の中核となるべく、ＮＩＳＣの人員体制を継続的に確保し、官民を問わず優れた人材を積極的に活用して参ります。

第５章　2009年度に喫緊に取り組むべき課題		
該当箇所	ご意見の概要	ご意見に対する考え方
前文	「合理性に裏付けられたアプローチ」等の新しい要素を加えたものに進化させることを意図したものである。 →「合理性に裏付けられたアプローチ」の具体的な説明を追記していただきたい。 （日本ユニシス株式会社）	御指摘の内容につきましては、第２章 第１節②「合理性に裏付けられたアプローチの実現」への取組みの開始　において記載しております。

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	サイバー犯罪の追跡ではログの相関分析が重要と考えられますが、漏れのないログ採取のガイドライン、たとえば採取するログの種類、保管、監視など重要度に応じてのガイドラインを示していただきたい。 （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。
第３章、４章	・以下のような段落番号の振り方に対しての説明を記載していただき たい。 「(1)①(ア)１)ア)ａ）」 ・□(四角)で囲んである部分が、同じセクション内に２つの段落レベルであるため、構成がわかりにくい。1)レベルの□(四角)囲みははずしていただきたい。 ・目次の記載レベルを（ア）または１）レベルまで下げていただきたい。 （日本ユニシス株式会社）	・段落番号の振り方については、第2次基本計画の段落番号に対応しております。 ・１）レベルの□（四角）囲みについては、第2次基本計画の抜粋記述であり、それが明確に確認可能なよう、原文とさせていただきます。 ・目次に関しては細かくすることで、目的の箇所が見つかりづらくなるため、原文のままとさせていただきます。
全般	（再掲施策について） どこに記載された内容の再掲なのかを記載していただきたい。例えば、「Ｐ３７参照。①政府機関・地方公共団体、（オ）環境変化への対応、イ）リスクコミュニケーションの充実のｂ)と同様」といったような記載をしていただきたい。 （日本ユニシス株式会社）	再掲施策については、前掲された箇所を明示いたします。
全般	セキュア・ジャパンすなわち安全な日本を標榜するならば、ぜひとも自衛隊における取り組みについて盛り込んでいただきたい。 （個人）	セキュア・ジャパンの実現のためには、防衛省のみならず、すべての政府機関の情報セキュリティ対策が重要であると考えております。防衛省を含めた政府機関の様々な取り組みについては第３章 第１節 (1) ①政府機関・地方公共団体の項目において具体的に記述しておりますので、御参照いただけると幸いです。
全般	計画をみると、どういう政策を対象に対して国家がリーダシップをになうべきなのか、あるいは民間にまかせるのはどういう技術施策なのか、その考え方が見えてこない（記述されていない）。本計画は情報セキュリティに関わる施策をただ網羅的に国家が介入しているだけに過ぎない。その具体的成果（目標に対する）も不明確である。 （個人）	本計画は情報セキュリティに関する政府の施策について記載したものです。官民の適切な役割分担についての検討は引き続き行って参りたいと考えています。
全般	クラウドコンピューティングやSaaSなどに対しても、本計画で取り上げようとしているが、先進企業（米国を中心としたグローバル企業）は既に数年まえから取り組んでおり、いまさら日本の政府だけが取り上げるべき課題なのか、はなはだ疑問である。もし、取り上げるのなら、どのような具体的成果・目標をもって取り組むのか明らかにして取り組むべきである。 （個人）	クラウド・コンピューティングの発展は、利用者のコスト面の利点はもちろん、膨大な情報の適切な利活用による企業経営の高度化や生活の質の向上といったメリットをもたらし、経済活動や社会・文化を革新する可能性を秘めています。 一方、世界では、御指摘のとおり、個人向けサービスを中心にクラウドコンピューティングが始まっており、日本がIT活用における世界のリーダーを目指す上で、全て海外のデーターセンタによるクラウドコンピューティングに依存することは、機微な情報漏えいやアクセスのためのネットワークにトラブルがあった場合の事業継続性の懸念が生じるなどの問題が指摘されています。 こうしたことから、政府としては、クラウドコンピューティング等の問題について精緻に検討した上で、クラウドコンピューティングの発展に向けて施策を行ってまいります。
全般	本計画の目標は具体的にどこにあるのか、その指標がない。 （個人）	本計画は、第２次情報セキュリティ基本計画が目指す「「ＩＴを安心して利用できる環境」の構築」を推進するため、同基本計画が描く「2012年の姿」を実現すべく、初年度である今年は、「すべての主体に事故前提の自覚を」との思想を中核に据えて各種対策の立案と実施に努めることとしているものです。
・第２章 第１節2009年度から2011年度までの３箇年を通じた方向性 ・第３章 第１節 (1) 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	情報セキュリティ対策として何をどこまで実施すればよいかという社会的合意が形成されていない現在、「合理性に裏付けられたアプローチの実現」により、コストと効果のバランスのとれた情報セキュリティ対策を実施する方針を示したことは評価できる。 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や、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について早急に検討し、実際に活用できるようにすべきである。 例えば、各種リスクに関する発生頻度統計、損害額統計を整備・整理して、公表すれば、情報セキュリティに関するコストパフォーマンスの定量的な算出が容易になると考えられる。 （(社)日本経済団体連合会）	ご指摘の点については、６月１０日に経済産業省において「情報セキュリティ導入ガイダンス」等を取りまとめたところです。今後、この普及に努めてまいりたいと考えております。
全般	「人間の存在を考慮したセキュリティ施策を」 関係する者が意図的に情報の横領を行い事故発生に至る場合があるのは、先日の証券会社の社員の情報漏えい等の例を見ても明らかである。 セキュリティを守るも脅かすも関係者の心がけ次第である。 今後も技術論に偏らない、人間の存在を考慮したセキュリティ施策を期待するものである。 （個人）	御指摘のとおり、人間の存在を考慮したセキュリティ施策が必要であると考えており、第２次情報セキュリティ基本計画においては、第２章 第1節(3)④に、「情報セキュリティ対策の推進には、対策に係る技術的な側面に加えて、制度面や対策を実施する人的な側面からの総合的な対策が必要である。」との記述がありますので、併せて御覧ください。

該当箇所	ご意見の概要	ご意見に対する考え方
全般	「公正な競争環境の確保」 IT産業の業者間の競争が激しくなると、コスト削減のために約束事を守らない、粗悪な業者が出てきて、セキュリティ被害を発生しやすいサービスを意に反して受けてしまう場合が危惧される。 たとえば、適正な構成管理をおこなわず、ハウジング契約に係わらず共用サーバを利用する。セキュリティを口実に利用者の監査を拒否し隠蔽するなどがおこりうる。 違約金などで解決する場合もあるが、ブランドイメージや取引先との信頼関係など金額換算できないものの被害を受けることの原因となる。 このようなメカニズムができないように、公正な競争環境をととのえ、悪質な業者の排除ができることが重要であると考える。 （個人）	当方としては市場における公正な競争の中で悪質な業者の淘汰が行われると考えておりますので、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。
全般	国家機関・地方公共団体・企業・個人における無線ＬＡＮ及び総務省の認可を必要とする無線機の実態調査を強く求める。また、HPCを始めとする暗号解読技術の進歩については、情報セキュリティを考える上で特に注意を払って情報の収集と安全対策について考えなければならない基本的情報であることから、政府及び識者の見解を求め明確にSJ2009に記述するべきである。 （北陸無線データ通信協議会）	御指摘の内容については、今後の施策の推進に当たっての参考とさせていただきます。 なお、暗号技術の安全性については、第３章第１節（１）①(カ)３）アにあるように政府機関における安全な暗号利用の推進の一環として、電子政府推奨暗号の監視や安全性等の確保のための調査、研究等を行う旨、明記されているところであり、これを踏まえ施策を鋭意推進してまいります。
全般	OSの脆弱性を防御する意味でのセキュアVMプロジェクトでしたが、結局、脆弱性を調査してデータベース化するという事業自身がウィルス対策ソフトベンダの商品にもなっています。このデータベースを管理・運営維持するための費用を考慮すると、ボックスタイプのファイアウォール装置にこれらの攻撃手法の対策モジュールを搭載したUTMを設置する形がセキュリティ保持のより堅牢な形になると考えます。これは、全てのOSをVM上に載せる形ではなく、単独で動くOSも含めてのサーバ環境・クライアント環境に適用する次のステップになると考えます。 尚、VMについては別の用途で複数のプロバイダやベンダが ・テスト環境構築のための仮想化環境 ・機器コスト削減のための仮想化環境 （人的コストは削減出来ず大きくなる） という形での利用を行う事も考えられますのでOSS化してそれらの今後を行政として見守るという事も付け加えておきます。 （個人）	セキュアVMは、ストレージやネットワークの管理などのセキュリティ機能を、利用者環境のOSやアプリケーションからは独立した形で実現することを目的としています。 当方としては、OS等の脆弱性への対応としては、ウィルス対策ソフトの導入や、ご指摘のようにファイアウォール等での対策導入というアプローチも有効と思われますが、安全な利用者環境の実現には、OS等の脆弱性への対応にとどまらず、ストレージやネットワークの適切な管理も必要と認識しており、今後、第3章 第１節(1)①(イ)に記載しているように、プロトタイプ版の評価及び性能向上に向けた取組みを進めて参ります。ご指摘の内容は、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。 また、セキュアVMは、テスト環境構築・機器削減を目的として開発されたものではありませんが、オープンソースで公開されており（http://www.securevm.org/からダウンロード可能）、プロバイダ、ベンダ等がそれぞれの目的に応じて利用することは可能になっています。
全般	近年ではハッキング・クラッキング技術が金銭を狙うという事で　セキュリティ事故1件当たり27億円の被害額平均となっています。プロバイダは中国IPを抑止する等の対策を行い対応していますが、DDoS攻撃を防ぐという形に至っていません。（実際、DDoS攻撃でIPセントレックス（IP電話）化したIPへの攻撃による電話の停止が有り、ISDNを残しておいて良かったという実例も有ります） インターネット自身が学術研究前提の無法地帯であるため、国内の企業・学校等は少なからずこれらのインフラに対するセキュリティの費用を捻出するという状況が散見されます。 そこで、インターネットの接続を国内のイントラネット全体で受け、更にその下に各プロバイダを設けるという形での【新しいインターネット利用】は如何でしょうか？国内通信を堅牢に守ると共に、何か有った場合にはコネクティビティを物理的に断線する等を行えば、ハッキング・クラッキングの対策になると考えます。また、内部のIPについても必要なリバースプロキシやロードバランサを経由した形でのサービスを行う事で、Webサーバに対する直接のDDoS攻撃も防げると考えます。 （個人）	御指摘の内容については、今後の施策の推進に当たっての参考とさせていただきます。
全般	以前のシステム構築技術とITILは、部分的には似通った箇所が有ります。然しながら【現場で汗を流していない人間達の紙の上だけの論議】に見えているのも事実です。例えば、システム設計の前段のシステム計画フェーズが完全に抜け落ち ・顧客の求める要件が国内の法律に合わない場合の対応。（例えば、社内の内線電話が公道を挟む場合等） ・顧客の業界の動向からの予想されるシステム変更に対する調整。 ・顧客自身が意図しない事故の発生の予見とその対策のための整備。 これらが完全に汲む事無くシステム設計に移っています。 （１）システム計画段階で人・物・時代への配慮が欠ける。 （２）システム設計段階で必要なインフラ自身に対する費用が欠ける。 （３）システム構築段階で言われた事のみを行うインフラのみに注力する。 このデフレスパイラルに似た構造の結果、セキュリティ事故についても「表面だけ対応していればエンドユーザの信頼を得られる」という事で対応する企業が後を絶ちません。必要な法整備とこれらの実現に向けたシステム構築技法の整備を行う事が行政が監督官庁を用いて情報技術を国内に広めるための第一歩ではないかと考えます。（建築基準法で耐震強度等はどうやって基準化されましたか？何も無い空間に容積を持つ建物を建築するものを法整備により画一化する事で国民の安全を求めたのではないですか？今、情報化社会でサイバーテロを未然に防ぐという事が容易ではない状況です。ならば、あぜ道を舗装するのは行政側の仕事と考える次第です） （個人）	政府機関については、内閣官房を中心に、情報システムの企画・設計段階からの情報セキュリティ対策の組込みについても意識するための方策（Security by Design）について検討を行っております。 またソフトウェアエンジニアリング手法の開発・普及などのシステム構築技法については、独立行政法人情報処理推進機構のソフトウェア・エンジニアリング・センター（ＳＥＣ）で取り組んでおり、引き続き、手法の開発・高度化に努めてまいります。 御指摘の内容については、今後の施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
全般	緊急経済対策も加味した国家政策には『ソフトウェア革新による技術立国日本』の確立が必要と考えています。 第二次基本計画は『事故前提社会』に対応する社会を目指しているにもかかわらず、今回、公開された17件の技術戦略施策には、これに相当する施策が見受けられません。 今こそ、『事故前提社会』を旗印に、これに対応するソフトウェア開発を日本のソフトウェア産業界に求め、その開発を支援することによりソフトウェアの技術革新を行わせ、世界に誇れるソフトウェア産業を国家として育成する事を目指していただきたいと思っております。『事故』を前提とした場合、やらなければならない項目には １）サーバ環境を如何にするか？ ２）情報流通環境を如何にするか？ ３）PC環境を如何にするか？ の3つの視点から考える必要があると思っております。 １）サーバ環境を如何にするか？では、 ①事故を前提としたサーバのバックアップ方法は現在のままで良いのか？ ②事故を前提としたサーバOS環境は現在のままで良いのか？ の視点があり、これには、「CDP（Continuos Data Protection）常時バックアップソフトウェアの開発普及」（サーバに起こった変更をトラキングし、変更された情報だけを常時バックアップする手法）及び「OSカーネルとアプリケーション領域を分離した新OSの開発普及」を提案したい。 また、２）情報流通環境を如何にするか？ということについては、「『事故前提社会』に対応した新メールシステムの標準化と開発普及 」（国として情報につける『情報タグ』を標準化し、また、これを検知して動くソフトの開発普及）を提案したい。 最後に、３）PC環境を如何にするか？ということについては、「情報セキュリティプロファイル方式によるPCのセキュリティ対策ソフトウェアの開発推進」（国家として①OSのパッチ情報やウィルスソフトの最新情報を定義するものと②禁止ソフトウェアを定義するものの2種類情報セキュリティプロファイルを提供する体制を構築すると共に、これを使ったソフトウェアの開発普及）を提案したい。 （クオリティ株式会社）	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、３）につきましては、民間サービスとして提供されているものもありますので、その必要性等について十分に見極めて参りたいと考えております。
全般	セキュリティ運用技術の開発とセキュリティ運用サービスの共通指標化情報セキュリティ対策の組み込み」における適切な調達のため、「セキュリティ運用技術の開発と運用サービスの共通指標化を行う」ことの追加を進言致します。 （日本セキュリティオペレーション事業者協議会）	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。