「情報セキュリティ2012」(案)に対する意見募集の結果の概要

■ 実 施 方 法: 内閣官房情報セキュリティセンターのWebページ上に掲載して公募
■ 実 施 期 間: 2012年6月1日(金)～6月21日(木)
■ コメント総数: 63件【内訳:7企業・団体から延べ37件、13個人等から延べ26件】
■ コメント概要:

(1)修正意見: 47件

・ p59、7ウ(キ)のa)を「情報処理技術者試験について一層の周知と普及を図る」とし、b)を「民間の情報セキュリティに関する資格及び教育プログラムについて一層の周知と普及を図る」とすべきである。(→意見のとおり修正)

・ 司法、立法府においてもしかるべきセキュリティ対策を講じるべきであり、立法・司法と行政府との連携・協力体制を検討すべきと考える。(→情報セキュリティ対策会議等へのオブザーバ参加による協力体制を構築している旨を回答)

・ 我が国の将来を見据え、胸を張って、「情報セキュリティ先進国」と言えるような方針の策定及び具体的な取組を検討いただきたい。(→「国民を守る情報セキュリティ戦略」の策定等により具体的取組を推進している旨を回答)

(2)賛同意見: 10件

・ 大学入試センター試験において情報科を出題教科とするよう、大学入試センターに要請することに賛成する。

(3)無関係な意見: 6件

■ コメントを関係省庁と共有し、今後の政策の推進に当たっての参考とするなど、適切に活用。

受付番号	枝番号	提出者	該当箇所	概要	御意見に対する考え方
1	1	個人	体裁について	パブコメにおいては、専門家以外の意見をすくい上げるため、情報セキュリティとは何で、標的型攻撃等の各事例において情報セキュリティの何が侵害されているのかを説明してから議論した方がよい。	情報セキュリティの定義、標的型攻撃等の侵害事例等については、「国民を守る情報セキュリティサイト」や政府インターネットテレビ等を通じて、普及啓発に取り組んでおります。
	2		体裁について	パブコメにおいては、専門家以外の意見をすくい上げるため、プライバシーの定義を明確にしてから議論した方がよい。	プライバシーの定義については、個人情報を含む幅広い概念で捉えております。本文書では、改めて定義する必要はないと考えております。
	3		P22、3エ（ウ）	情報セキュリティを論ずる場合は、一般ユーザに関しては性善説で対応するのは間違いであり、教育してもその通りには行動しないことを前提に、いかなる対策を講じる必要があるのか考えないといけない。	ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
	4		P23、3エ（ケ）	DKIMやS/MIMEの導入促進とありますが、DKIMは、国家レベルで使うツールにはなりえていない。	DKIMにつきましては、総務省における電気通信事業者4社のデータの取りまとめ結果（http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/pdf/110302_3.pdf）によると、年々その導入が進んでいる状況です。政府機関においても、一部の府省庁では既にDKIMを導入・運用しております。このような状況であることから、「DKIMは、国家レベルで使うツールになりえていない」とのご指摘には当たらないものと考えております。
	5		P23、3エ（ケ）	送信ドメイン認証技術の中ではSPFは携帯会社などが既に運用しているため、技術の完成度は高いと思うが、全プロバイダのメールサーバに実装をするように期待しても今の制度下では無理で、何らかの法的強制力が必要と考える。	本取組は国民や民間事業者に対して送信ドメイン認証技術の採用を強制するものでありません。なお、本取組について、政府機関が率先して取り組むことにより、民間事業者においても、同技術が積極的に採用されることを期待しています。
	6		P23、3エ（ケ）	政府機関やプロバイダにメールを出す際はS/MIMEでないと受け付けないくらいの強い指導がない限り普及はしないと思う。	本取組は国民や民間事業者に対してS/MIMEの使用を強制するものでありません。なお、本取組の周知等により、国民や民間事業者においても、同技術が積極的に使用されることを期待しています。
	7		P28、3ケ	住基ネットの違憲問題が提示されるなど、社会保障・税番号制度に関しては先進各国に比較すると日本は結果的に周回遅れの状態だと思われる。2008年に最高裁が住基ネット合憲判決を出しているので、来年にも実施するくらいの時間感覚で作業する覚悟が必要と考える。	社会保障・税番号制度については、現在、関連法案を国会に提出中であり、制度の早期導入に向けて取り組んでいるところです。
	8		P32、4及びP40、5①イ（キ）	現在のクラウド技術のように、ネットワークに分散していた情報を少数のデータセンタに集約するのは、物理的な意味においても、地震等の自然災害に対してはまだまだ脆弱と考えられるため、一般の消費者が直感的に持っているクラウドのイメージに技術を近づけるべきと考える。	ご指摘に該当する取組として、総務省では広域に分散されたクラウドを連携することで、被災地のクラウドから遠隔地の安全なクラウドに重要データを退避させ、業務処理を継続する「広域災害対応型クラウド基盤構築に向けた研究開発」を実施しております。（P40、5①イ（カ））
	9		P38、5①ア（エ）	サービスとしてフィルタリングしている場合、ウォーターゲート事件の際に出されたHEW reportに記載されている事項を事業者が守るように持って行くべきではないか。	総務省及び経済産業省は従来青少年のインターネット環境整備の観点から、事業者におけるフィルタリングの改善を支援してきたところ、ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
	10		P55、7	人材育成に関しては、一過性ではなく、継続的に人材育成ができるように仕組みを変えないといけない。	ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
	11		P59、7ウ（カ）	「情報セキュリティに詳しい法律家育成」に関しては、情報技術者から選抜して法律家にするのか、法律家を教育して情報セキュリティに強くするのかの二通りが考えられる。これまでの経緯から、後者だけでは大きな期待できないと考えられるので、情報技術者から選抜してこの道専門の法律家にするような道を考えてもいいのではないか。	ご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。
2	1	個人	P19、3	情報セキュリティ緊急支援チーム（CYMAT）と記載があるが、脚注には「Cyber Incident Mobile Assistant Team の略」とある。従って情報セキュリティ緊急支援チームの略記はCIMATとすべきではないか。	CyberのCY、 MobileのM、AssistantのA、TeamのTを組み合わせて、CYMATとしております。
3	1	不明		最近自分のパソコンから検索した情報（検索内容）が他人に見られている気がして心配である。何かのスパイウイルスソフトか何かに侵入されているのだろうか。何か対策等はないか。	ご指摘の内容については、情報セキュリティ政策に関係する内容ではありませんので、回答を控えさせていただきます。 なお、インターネットに接続されているパソコンに実施すべき対策につきましては、「国民を守る情報セキュリティサイト」（http://www.nisc.go.jp/security-site/index.html）にも掲載しておりますので、ご参照ください。

受付番号	枝番号	提出者	該当箇所	概要	御意見に対する考え方
4	1	不明		1)情報基盤における関所の構築 情報の一部閲覧を安全な場所で実施することで、ウイルスやサイバー攻撃、メール洪水などは削除可能と考える。重要なのは閲覧に際し攻撃性のあるものは排除するが、それ以外は素通しする技術である。 2)2バイト文字以外は跳ね除ける機能 1バイト国家とのやり取りでバイト変換をかける。これだけでも異常なメールは排除可能と考える。 3)情報網自体の暗号経路化 国家に関わる情報は、暗号経路を通るように特殊なフィルタを情報網にかけることで、平文のメールは通れないルートを構築すれば、漏洩も無ければスパムメールが入る余地を相当減少させられると考える。 この3つが実現すれば、攻撃されても防衛は可能と考えるが、ヒューマンエラーに対してセキュリティ上の防衛策が無いのが欠点と考える。我が国にとって本当に重要な情報はいつでも消去できるように紙に保管するのが一番良いのではないかと考える。	ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
5	1	個人	全般について	過去に被害を発生させた団体に対しては、抜き打ちによるパソコンの使用状況、内容開示を義務付ける等の対策と、個人被害や犯罪が発覚した場合、活動停止等の厳しい罰則を設けた法律を制定して欲しい（宗教団体等に対する規制強化を求める意見）。	ご指摘の内容については、情報セキュリティ政策に関係する内容ではありませんので、回答を控えさせていただきます。
	2			宗教団体等としての存在真意をネット投票等で国民に問う制度を構築して欲しい。	ご指摘の内容については、情報セキュリティ政策に関係する内容ではありませんので、回答を控えさせていただきます。
	3			人材の登用に当たっては、カルト教団信者等が採用されないように、事前に徹底調査して欲しい。	ご指摘の内容については、情報セキュリティ政策に関係する内容ではありませんので、回答を控えさせていただきます。
	4			私の被害状況から具体的な手口を調査し、それらを具体的な対策に利用して欲しい。	ご指摘の内容については、情報セキュリティ政策に関係する内容ではありませんので、回答を控えさせていただきます。
6	1	個人	全般について	内部からの情報漏洩やスパイ行為など、ICTを介さない手段での情報セキュリティに対する攻撃についても、「ICT面での対策を十全に施したとしても、それ以外の面からの攻撃によってセキュリティが危険に晒される可能性が残るので、安心してはいけない」というような趣旨で、注意喚起を盛り込んで欲しい。	ご指摘の内容については、政府統一基準群に必要な規定を盛り込み、対策を実施しております。
	1		全般について	昨年度、「情報セキュリティ2011」への意見として、「テロ（物理テロを含む）攻撃を想定した情報セキュリティ分野における対応」という項目を追加すべきと考えます、という意見を提出したところ、「御指摘の内容については、従前より継続的に実施してきているものであることから、最近の環境の変化に対する基本方針に新たに追加する必要はないと考えます。」という回答があった。しかしながら、物理テロへの対策に係るガイドライン的文書はどこにも公開されていない。 民間のクラウド・データセンター等に対し、郵便による炭疽菌の送り付けや爆発物持参による突入など比較的簡単に実行が可能なテロへの備えは、大規模災害対策と並んでやはり必要ではないか。	ご指摘の内容については、データセンター固有に求められる対策ではないことから、本文書に具体的な取組を掲げる必要はないと考えます。
	2		P24、3エ（ケ）a）	「…のように暗号技術を利用した対策の導入を積極的に検討する。」ではなく、「…のように暗号技術を利用した対策を導入する。」としてはいかがか。	政府機関から発信する電子メールに係るなりすましの防止策として、送信側SPF対策については、ほぼ対応済みとなっているところです。一方、DKIMやS/MIMEについては、現状各府省庁で使用しているメールシステムの構成により、その導入に係る技術的課題や実施コストが大きく異なるため、個別にその導入手段を検討しているところであることから、実体に即し原案のとおりとさせていただきます。

受付番号	枝番号	提出者	該当箇所	概要	御意見に対する考え方
7	3	日本ユニシス株式会社	P24、3エ（ケ）b）	「･･･（SPF30、DKIM等）等の導入を促進する。」ではなく、「･･･（SPF30、DKIM等）等を導入する。」としてはいかがか。	民間等における送信ドメイン認証技術の導入については自主的な取組とし、政府はその促進を図るべきであると考えます。
	4		P24、3エ（サ）	「･･･電子ファイルの正当性・安全性を担保するための取組を推進する。」ではなく、「･･･電子ファイルの正当性・安全性を担保するための仕組みを導入する。」としてはいかがか。	「･･･取組を推進する。」という表現には、御指摘のような仕組みの導入のほか、利用者に対する教育・啓発活動等の関連取組も含めていることから、原案のとおりとさせていただきます。
	5		P29、3コ（ア）e）	「･･･SPF等の送信ドメイン認証技術の採用等を推進する。」ではなく、「･･･SPF等の送信ドメイン認証技術を採用する。」としてはいかがか。	実際にSPF等の送信ドメイン認証技術を採用するかどうかの判断は、個々の地方公共団体が主体的に行っていただくものです。国としては、地方公共団体に対し、送信ドメイン認証技術のメリット等を説明し、その導入を促す立場にありますので、原案の表現が適切と考えます。
	6		P30、3コ（エ）c）	「･･･SPF、DKIM等の送信ドメイン認証技術の採用等を推進する。」ではなく、「･･･SPF、DKIM等の送信ドメイン認証技術を採用する。」としてはいかがか。	独立行政法人から発信する電子メールに係るなりすましの防止策として、送信側SPF対策については、ほぼ対応済みとなっているところです（但し、.go.jpドメインを利用している独立行政法人に限ります）。一方、DKIMやS/MIMEについては、現状独立行政法人で使用しているメールシステムの構成により、その導入に係る技術的課題や実施コストが大きく異なるため、個別にその導入手段を検討しているところであることから、実体に即し原案のとおりとさせていただきます。
	7		P38、5①ア（エ）	「スマートフォン等におけるフィルタリングの在り方を検討する。」のフィルタリングの意味が不明である。	スマートフォン等については、無線LANによるインターネット接続が可能であり、電気通信事業者による従前のフィルタリングが機能しない場合があることから、その在り方を検討するものです。
	8		P41、5①ウ（エ）	「･･･SNSの利用に係る情報セキュリティの確保について検討を行うとともに･･･」は、「･･･SNSの利用に係る情報セキュリティの確保についてガイドライン等を策定するとともに･･･」としてはいかがか。	ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
	9		P48、5③ウ（ア）	「･･･企業における電子署名の利活用の普及促進策について、検討を行う。」ではなく、「･･･企業における電子署名の利活用の実現に向けた取組みを実施する。」としてはいかがか。	電子署名の利活用の普及促進策については、実施も視野に入れた検討を行っていく予定であり、原案のままとさせて頂きます。
	10		P49、5③オ（ア）b）	「･･･送信ドメイン認証技術（SPF、DKIM等）等の導入を促進する。」ではなく、「･･･送信ドメイン認証技術（SPF、DKIM等）等を着実に導入する。」としてはいかがか。	民間等における送信ドメイン認証技術等の導入については自主的な取り組みとし、政府はその促進を図るべきであると考えます。
	11		P50、5③オ（ア）e）	「･･･のように暗号技術を利用した対策の導入を積極的に検討する。」ではなく、「･･･のように暗号技術を利用した対策を導入する。」としてはいかがか。	政府ドメイン（.go.jp）を利用する電子メールのなりすまし対策として、送信ドメイン認証技術SPFの送信側対策がほぼ完了したところで、現在は受信側SPF対策の一層の推進を諮っているところです。なお、この取組にあわせ、関連技術であるDKIMやS/MIMEのように、電子メールの改ざんや盗聴の対策を行う技術についても、その導入に係る技術的課題や実施コストを鑑みながら、あわせて導入を推進しているところです。
8	1	株式会社サーティファイ	P58、7ウ（イ）	大学入試センター試験において情報科を出題教科とするよう、大学入試センターに要請することに賛成する。	大学入試センター試験にどのような教科科目を出題するかについては、いただいたご意見も参考としつつ、大学入試センターにおいて大学及び高等学校関係者のニーズを踏まえながら検討を行うこととしています。
9	1	日本セキュリティマネジメント学会電子的本人認証の検討会	P11、Ⅳ	利用者の本人認証に関して以下のような記述を加えることを提言する。 『標準的な利用者本人認証として使用されているパスワードについては破られにくいという機密性に加えて、利用者が容易に使いこなせるかどうかという現実的な可用性/利便性についても十分に考慮した運用を図ること』	ご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。
10	1	個人	P58、7ウ(イ)及びP61、8ア(カ)	全面的に賛成する。	大学入試センター試験にどのような教科科目を出題するかについては、いただいたご意見も参考としつつ、大学入試センターにおいて大学及び高等学校関係者のニーズを踏まえながら検討を行うこととしています。
11	1	個人		私の携帯電話の契約が他人に勝手に書き換えられてしまいましたが、関係機関において親身に対応してもらえない。	ご指摘の内容については、情報セキュリティ政策に関係する内容ではありませんので、回答を控えさせていただきます。
12	1	個人	P58	情報を是非大学入試に入れて欲しい。	大学入試センター試験にどのような教科科目を出題するかについては、いただいたご意見も参考としつつ、大学入試センターにおいて大学及び高等学校関係者のニーズを踏まえながら検討を行うこととしています。

受付番号	枝番号	提出者	該当箇所	概要	御意見に対する考え方
13	1	個人	P58	情報セキュリティ教育を充実させるにあたっては、初等中等教育において、情報科学・数学と情報技術の理解を促すようにするべきであり、さらに、倫理学（モラルジレンマ）に関わる技術者倫理教育の導入も望ましい。	初等中等教育段階における情報セキュリティを含む情報モラルに関する教育については、学習指導要領の改訂等を踏まえ、発達段階に応じて積極的に推進してまいります。
14	1	個人	P61、8ア(オ)及び8ア(カ)	全面的に強く賛成する。	今後とも、初等中等教育段階における、情報セキュリティを含む情報モラルに関する教育を積極的に推進してまいります。また、大学入試センター試験にどのような教科科目を出題するかについては、いただいたご意見も参考としつつ、大学入試センターにおいて大学及び高等学校関係者のニーズを踏まえながら検討を行うこととしています。
15	1	データベース・セキュリティ・コンソーシアム	全般	昨年から発生している大型情報漏えい事件・標的型攻撃等の事案を考慮した場合、情報の「入れ物」であるデータベース（RDBMS）に対する対策の重要性が増していると考えられる。一方現在、我が国政府・関係機関等において策定されている基準・ガイドライン等には、その旨の記述はほとんどなく、システムの実装においても十分な対策が実施されているとは言いがたいのが現実である。 この状況を鑑み、今後政府機関、および関連独立行政法人等においてデータベース（ここではリレーショナル・データベース：RDBMS）に関わるセキュリティ対策についての調査・研究を行い、それを適切な政策・ガイドラインに反映させて頂くことを要望する。また実際に検討を行う場合には、当コンソーシアムでは専門的な見地から、協力する用意がある。	統一基準群の対象にはデータベースに関する対策も含まれており、各府省庁において必要な対策を実施していますが、当該分野における技術動向の変化も踏まえ、必要な検討を行ってまいります。
	2		P25、3オ(イ)	該当の定義を以下のように明言することが望ましいと考える。 安全性の高い暗号モジュールを利用するため、IPAの運用する暗号モジュール試験及び認証制度（JCMVP）およびCMVP共同認定制度を受けたセキュリティレベル2以上の暗号モジュール等を取り扱う。	御指摘の共同認定制度については本年3月からその運用が始まったものであり、認定製品も限られていることから、現時点で、調達で一律にこれのみを扱うことは困難と考えます。なお、今後当該制度が着実に普及することを期待しており、その際には御指摘のような調達方針とすることが可能になると考えております。
16	1	個人	P58、7ウ(イ)	賛成である。是非推進して欲しい。	大学入試センター試験にどのような教科科目を出題するかについては、いただいたご意見も参考としつつ、大学入試センターにおいて大学及び高等学校関係者のニーズを踏まえながら検討を行うこととしています。
17	1	個人	P56、7ア(ケ)	賛成する。	今後とも情報セキュリティ人材の育成に取り組んまいります。
	2		P56、7ア(キ)	賛成する。専門教育だけでなく、一般情報教育に対しても同様の施策を組み入れて欲しい。	ご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。
	3		P57、7イ(オ)	情報セキュリティ関連素養の確認を行うことに賛成する。より明確に、「国家公務員採用試験」に「情報・情報セキュリティ」を必答科目として追加することを要請する。	国家公務員の採用試験については、中立・公正性を担保するため，国家公務員法の規定により、中立・第三者機関としての人事院が実施しているものであり、その出題内容を含めた実施に関する事項については、いかなる機関からも指示を受けずに、人事院が判断すること（国家公務員法第3条）とされていることから、国家公務員採用試験に言及する要請
	4		P58、7ウ(ア)a)	賛成する。しかし、ことを「情報モラル」教育に矮小化してはならないと考えます。	情報セキュリティに関する教育の推進は重要であり、今後とも初等中等教育段階における情報教育の中で、情報セキュリティに関する教育を積極的に推進してまいります。
	5		P58、7ウ(ア)b)	賛成する。加えて、初中等教育の教員養成における情報教育・情報セキュリティ教育に対する施策を設けるべきだと考える。	グローバル化や情報化など社会が急速に変化し、学校教育において求められる人材育成像が変化する中、教員には複雑かつ多様な課題に対応することが求められており、現在、教員養成の修士レベル化、教員免許制度について中央教育審議会で議論しているところです。したがって、原案のままとさせていただきます。
	6		P58、7ウ(イ)	賛成する。	大学入試センター試験にどのような教科科目を出題するかについては、いただいたご意見も参考としつつ、大学入試センターにおいて大学及び高等学校関係者のニーズを踏まえながら検討を行うこととしています。
	7		P58、7ウ(ウ)及びP58、7ウ(エ)	大学での人材類型を跨がっての情報セキュリティ教育の推進を図る施策に賛成する。しかし、「一般教育（専門によらない教養）」としての「情報セキュリティ教育」及びその前提となる「情報教育」という観点を明確に打ち出すべきだと考える。	ご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。

受付番号	枝番号	提出者	該当箇所	概要	御意見に対する考え方
18	1	インテル株式会社	P8、Ⅲ②及びP26、3カ（エ）並びにP38、5ア（ア）	スマートフォンを安全に利活用するための環境整備、セキュリティ対策は、可搬型計算機器（スマートフォン、タブレット型PC、ノートPC、その他）全般を対象に行うべきであり、社会に対して利用促進のための指針を示すことで、日本において遅れているモバイルコンピューティングの活用を加速化し、社会活動、国民生活の効率化、安心の向上、国際競争力強化に寄与するようにすべきと考えます。	政府としてはこれまでも可搬型計算機器の情報セキュリティ対策に取り組んできたところですが、本項目では、近年急速に普及が進むスマートフォンやタブレット型PC等について、新たな脅威も想定されることから、特に情報セキュリティ対策について検討を行っていくこととしているものです。
19	1	特定非営利活動法人 日本ネットワークセキュリティ協会 社会活動部会	全般	司法、立法府においてもしかるべきセキュリティ対策を講じるべきであり、立法・司法と行政府との連携・協力体制を検討すべきと考える。	立法府、司法府などの政府機関以外の機関についても、情報セキュリティ対策推進会議等におけるオブザーバー参加により協力体制を構築しており、行政府が実施するセキュリティ対策を共有しています。
	2		全般	日本政府として、情報セキュリティに対する規模やコストなどの具体的な目標を設定すべきと考える。	政府機関においては、統一基準群において情報セキュリティ対策に関する統一的な基準を定めておりますが、政府一律で規模やコスト等を定めることは難しく、各省庁の実情に応じて適切に実施されるべきものと考えております。
	3		P8、Ⅲ①	「守るべき情報」を明確に定義すべきと考える。	ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
	4		P8、Ⅲ③	安全保障の観点から第 5の戦略空間としてのサイバー戦略を決定すべきと考える。	ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
	5		P27、3ク	システムに適切な情報セキュリティ対策が組み込まれるための実効性の担保をNISC主導で検討いただきたい。	システムに適切な情報セキュリティ対策を組み込む最終的な責任は、その調達主体である各省庁が負うべきものと考えています。なお、各省庁でセキュリティを確保した調達を円滑に行うため、NISCにおいて、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を策定し、統一基準群への反映を行うとともに、各省庁への普及活動に取り組んでいます。
	6		P27、3ク	各府省庁が保有する情報システムについて、情報セキュリティの有効性を評価する適切な監査体制の整備も必須と考える。例えば、政府機関統一基準群への準拠性確認については、現状の自己診断に基づく報告制度に加え、会計検査院などのような厳密な監査体制の構築を検討すべきと考える。 また、適切な監査体制の確保のためには民間活力を導入することが適切であると考えられる。例えば経済産業省が策定し推進する情報セキュリティ監査制度の活用なども考えられる。そのような具体策が盛り込まれることを期待する。	情報セキュリティ監査の実施については、統一管理基準1.2.3.2 において定めており、各府省庁において毎年度、情報セキュリティ監査を実施しております。各府省庁の特性に応じて、内部の監査を実施したり、民間の知見を活用した外部監査を導入するなどの取組を行っています。
	7		P28、3ク（エ）	政府機関が情報セキュリティ対策を支援するツールを作るということは、その内容や方法如何によっては民業圧迫となる可能性があり、情報セキュリティ対策促進による、我が国経済振興という根本的な方針に逆行する恐れがあるものと考える。	ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
	8		P39、5①イ	クラウドコンピューティングの活用に向けて、サービス提供者からの情報開示と、第三者による評価の仕組みを整える必要があると考える。	経済産業省では「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（平成23年4月1日）を公表し、「クラウド事業者の実施が望まれる事項」として、クラウド利用者がクラウドサービスを導入・利用するために必要な情報の提供等を挙げています。また、第三者評価の仕組みについては、クラウドセキュリティに係る国際標準化動向（ISO/IEC SC27）を踏まえ、今後検討してまいります。 総務省ではクラウドサービスの比較・評価・選択等を容易にするため「クラウドサービスの安全・信頼性に係る情報開示指針」（平成23年12月16日）を公表しています。また、一般財団法人マルチメディア振興センター（FMMC）において、「ASP・SaaS 安全・信頼性に係る情報開示認定制度」が運用されています。
	9		P49、5③エ	中小企業における情報セキュリティ対策の推進策の一環としてクラウドコンピューティングの活用等を盛り込み、より低コストで、高セキュリティな事業環境の整備が必要と考える。	中小企業におけるクラウドコンピューティングの利活用を促進するため、独立行政法人情報処理推進機構（IPA）において「中小企業のためのクラウドサービス安全利用の手引き」（2011年4月25日公表）を提供しています。
	10		P50、5③カ	知的財産権保護の推進だけでなく、インターネット上のプライバシー問題について、我が国として責任を持って方針を示せる組織を作り、国際競争力の確保を検討すべきと考える。	ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
	11		P54、6イ	情報セキュリティ産業の振興策として、（ア）、（イ）だけでは不十分であり、より広範で具体的な産業振興策を検討いただきたい。	ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
	12		P55、7ア	情報セキュリティ人材の育成には、政府として、より具体的・直接的施策を施す必要がある。人材育成・開発の具体的手段として、補助金政策を明示されるよう提案する。また、最終的には、育成した人材が社会で活躍する場としての労働環境の整備を検討いただきたい。	ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。

受付番号	枝番号	提出者	該当箇所	概要	御意見に対する考え方
	13		P58、7ウ（ア）	初等中等教育における情報セキュリティの推進にあたっては、教員の指導力の向上が必須であり、記載されている取組みだけでは不十分と考える。	地方公務員である公立学校の教員の採用及び研修は、任命権者である教育委員会が実施すべきものですが、国として各地域における取組を促進するため、各地域で情報教育を推進する中核的な役割を担う指導主事、教員等を対象とした研修等に取り組んでまいります。
	14		P73、10エ	我が国の将来を見据え、胸を張って、「情報セキュリティ先進国」と言えるような方針の策定および具体的な取り組みを検討いただきたい。	政府におきましては、「国民を守る情報セキュリティ戦略」を策定し、その年度計画により具体的な取組を推進してきたところですが、ご指摘の内容を踏まえ、引き続き情報セキュリティ政策を推進してまいります。
20	1	情報セキュリティ教育事業者連絡会（ISEPA）	P59、7ウ（キ）	下記の項目について「」内を追記すべきである。 a) 情報セキュリティ人材を含めた高度 IT 人材の育成強化のため、情報セキュリティ分野を含めた各種情報分野の人材スキルを測る情報処理技術者試験について一層の「周知と」普及を図る。 b) 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「及び教育プログラムについて一層」の周知「と普及」を図る。	ご指摘を踏まえ、修正いたします。