セキュア・ジャパン2006（案）に対する意見及びそれらについての考え方

情報セキュリティ政策会議

2006年6月15日

意見提出者一覧（五十音順）

株式会社 CSK システムズ
(ISC)2 Japan
KNC
株式会社 Qript
株式会社 SRA
(株)イマオコーポレーション
インテリジェントディスク株式会社
オリエント測器コンピュータ株式会社
神奈川県立産業技術短期大学校
グローバルセキュリティエキスパート(株)
セイコーインスツル(株)
セキュリティ・エデュケーション・アライアンス・ジャパン（SEA/J 事務局）
(社)日本経済団体連合会
日本セキュアテック研究所
第六感の港有限会社
有限会社デジタルインフラ
テッドインパクト株式会社
ドコモ・システムズ(株)
株式会社ニーモニックセキュリティ
株式会社ニューオータニ
有限会社日本ネット技術研究所
NPO 日本ネットワークセキュリティ協会
株式会社日立製作所
富士通株式会社
北陸無線データ通信協議会
(株)まりも
三重大学

その他個人１２件

第１章　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			
分野	該当箇所	ご意見の概要	ご意見に対する考え方
	本文１２行目	「政府機関のWebサーバへのサイバー攻撃」は毎年発生しており2005年に急増したということもない（と思われるため）、これを削除する。 （個人）	ご指摘の政府機関のWebサーバへのサイバー攻撃は、情報セキュリティ問題としてはＩＴ利用・活用自体に対する不安を増大させる原因の一つとなっていることから記載しているものです。
	（１）官民各主体の共通認識の形成	２行目「自立的な取組みが重要」とある。この記述には全く異論はないのだが、「動機付け」を明確に打ち出す必要があるのではないか。 具体的には、例えば、以下のようなものが考えられる。 「先端技術追求」→ＩＴ業界のビジネスチャンス（民）オンリーワン商品 情報セキュリティの「ジャパンモデル」提示→日本の世界貢献（官）、それに伴うビジネスチャンス（民） 上記ビジネスチャンス及びジャパンブランドイメージの向上による、より広い経済効果→日本の国際競争力強化（官、民） （グローバルセキュリティエキスパート（株））	ご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の一つとさせていただきます。
	（２）先進的技術の追求	人的問題も併記してほしい （個人）	人的問題については重要と認識しており、（１）「官民各主体の共通認識の形成」の中で各主体の自律的な取組みが重要である旨述べているところですが、ご指摘の点については、今後の政策運営に適切に反映してまいります。

第２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			
分野	該当箇所	ご意見の概要	ご意見に対する考え方
第１節ア　政府機関	①イ）ａ）各政府機関でのＰＤＣＡサイクルの確立	２行目「具体的な実施手順の整備」について、消去した記録媒体を撮影して証明書が発行できる消去装置を使い、資産管理ソフトと組み合わせて、資産管理から消去、更には廃棄やリサイクルにいたるまでの一連の管理を行う方法を確立したガイドラインを策定致しましたのでご参照下さい。 （オリエント測器コンピュータ株式会社）	ご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の一つとさせていただきます。
	同上	ハードディスクを含めて、パソコンに使われる各種電子記録媒体を、包括した具体的かつ安全確実な消去方法の提案を行いますのでご参照下さい。 弊社が提案しますガイドラインでは、ＣＤやＤＶＤ等はデータ消去後にリサイクル処理した利活用が可能になります。 （オリエント測器コンピュータ株式会社）	ご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の一つとさせていただきます。
	同上	「情報セキュリティ対策の実施状況の自己点検及び監査」につきまして、具体的な方法を明示することが望ましいと考えます。 （株式会社日立製作所）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	①イ）ｂ）政府全体でのＰＤＣＡサイクルの確立	検査・評価の対象について基準等を明示することが望ましいと考えます。 （株式会社日立製作所）	内閣官房は、各府省庁の情報セキュリティ対策の実施状況を、政府機関統一基準に基づき、検査を行い、評価を行うこととしております。
	①エ）コンピュータウイルスなどに起因する情報流出への対応	情報の外部持ち出し・私物パソコンの使用などを根絶するには、その理由となっている「利用者の不満」を解消する以外に方法はないはずです。 （個人）	ご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の一つとさせていただきます
	①オ）外部委託先等の情報セキュリティ対策の水準の確保	オ）a)情報セキュリティマネージメントシステム適合性評価制度の活用、及びb)情報セキュリティ監査制度の活用の主旨には賛同するものですが、これらの基準は各府省庁で個別に設定するのではなく、政府機関で統一的なものとなるよう記述することが望ましい、と考えます。 （株式会社日立製作所）	外部委託先等の情報セキュリティ対策について、各府省庁は、政府機関統一基準を踏まえた省庁基準に基づき、その対策を実施することとしています。
	①オ）ａ）情報セキュリティマネジメントシステム適合性評価制度等の活用	３行目から４行目「情報セキュリティ対策ベンチマークを活用する。」を、「情報セキュリティ対策ベンチマークを活用すると共に人材評価基準を策定し活用する。」と修正すべき。 （(ISC)2 Japan）	ご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の一つとさせていただきます。
	①オ）ｃ）「情報システムの信頼性向上に関するガイドライン」の活用・普及他に 第２節①ア） 第３節①ア）ａ）	個々の主体（政府機関、重要インフラ、企業）において、ガイドラインの利活用の度合いにレベル差がある。各主体は信頼性・安全性向上にむけて、ガイドラインを参照のうえ、適切な対策を講じるなど、ガイドラインの利活用を一層推進するべき。その際、政府機関においては、「方策の検討」に関する期限だけでなく、ガイドラインに沿った見直しについてもターゲット年度を決めるべき。 （富士通株式会社）	ご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の一つとさせていただきます。
	③（ア）最適化対象の府省共通業務・システム及び一部関係府省業務・システムの開発との連携	「新たに開発（導入）するシステムについて」とありますが、既存システム及び既存システムの改造を行う場合に対する考え方についても示す必要があると考えます。 （株式会社日立製作所）	各府省庁は、既存システムに対しても、政府機関統一基準を踏まえた省庁基準に基づき、情報セキュリティ対策を実施することとなっています。 なお、ご指摘の部分は、今回とは別の意見の募集の手続きを経て決定された「第１次情報セキュリティ基本計画」からの抜粋であり、今回の意見の募集の対象ではないと考えています。
	③（ア）イ）安全性・信頼性の高いＩＴ製品等の利用推進	ISO/IEC15408の認証制度の利用にあたっては、EAL(評価保証レベル)自体の主旨を踏まえ、徒に高いレベルのEALを訴求するのではなく、業務システムの特性を客観的に評価した上で必要となるレベルを指定するべき。そのためには、業務システムのセキュリティ上の特性を判断する基準を省庁横断的に共有する必要がある。 （富士通株式会社）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	③（イ）四角内４行目から５行目「生体認証等の新規システム（機能）の導入に付いて総合的な検討などを行い、その実現を推進する。」	「人権保障」や「適法性の確保」に留意するのならば、「生体認証」の「実現を推進する」ようなことは控えるべきであります。 （日本セキュアテック研究所）	ご指摘の部分は、今回とは別の意見の募集の手続きを経て既に決定された「第１次情報セキュリティ基本計画」からの抜粋であり、今回の意見の募集の対象ではないと考えていますが、ご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の一つとさせていただきます。

分野	該当箇所	ご意見の概要	ご意見に対する考え方
	③（イ）セキュリティ強化に資する新システム（機能）の導入検討とその実現	導入検討技術として、タイムスタンプを検討するよう進言します。 具体的施策として、 電子データのフローにおけるトレーサビリティを明確にし、当該電子データの証拠性を確保するため、電子データの受付時や作成時に原本として確定保存する時や、当該電子データの改版、可搬媒体への書き出し時等において、誰がいつ、何を承認・修正したかを安全確実に電子的な証拠として残す手段として電子署名に加えてタイムスタンプ利用を推進する。 （セイコーインスツル（株）） 	ご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の一つとさせていただきます。
	同上	次世代OS環境に関しては、開発を推進するとともに、どのようにして高いセキュリティ品質を維持し続けるかの、仕組みも考慮に入れるべき。 （株式会社CSKシステムズ）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。 なお、施策の詳細につきましては、こちらをご参照下さい。 http://www.nisc.go.jp/press/pdf/securevm.pdf
	③（イ）イ）高セキュリティ機能を実現する次世代ＯＳ環境の開発	政府が一ソフトの対策を念頭にソフト作成を行うことは無意味であり、税金の無駄使いである。 作成されるのならば作者を召喚し対策させることを求めたい。 （個人）	本施策は、ご指摘のような「一ソフトの対策を念頭にソフト作成を行う」ものではなく、一般的にＯＳにおいてアプリケーションに依存しない形でセキュリティを確保しようとするものですが、ご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の一つとさせていただきます。 なお、施策の詳細につきましては、こちらをご参照下さい。 http://www.nisc.go.jp/press/pdf/securevm.pdf
	同上	この「セキュア・ジャパン2006」（案）には「高セキュリティ機能を実現する次世代OS環境の開発」が挙げられていますが，この新OSでMicrosoftのWordが動作しないのではないかと思います。そうなると，Wordを使うために，安全なOSを捨ててWindowsを使わなければならないことになり，結果的に「セキュア・ジャパン2006」（案）の目指す方向とは矛盾するように思われます。 （個人）	本施策は、ＯＳ及びアプリケーション等からなる現在の利用者環境を活用可能な、次世代ＯＳ基盤環境の確立を目指すものであり、ご指摘の内容にはあたらないものと考えておりますが、ご指摘を踏まえて、表現の適正化をすべく以下のように修正いたします。 第２章第１節ア③（イ）イ） 第３章第１節②イ）ｂ 　高セキュリティ機能を実現する次世代ＯＳ環境の開発 　２００６年度において、ＩＴの信頼性確保のための喫緊な取組みとして、現在のＯＳ等利用環境及び使用するアプリケーションを維持しつつ、情報セキュリティ機能を利用者環境に依存しない形で集約的に提供する仮想機械（ＶＭ：Ｖｉｒｔｕａｌ　Ｍａｃｈｉｎｅ）機能及びこれを稼動させるための最小限のＯＳ機能（これらの機能を併せて「セキュアＶＭ」と呼ぶ。）の開発を、産学官の連携により推進する。 なお、施策の詳細につきましては、こちらをご参照下さい。 http://www.nisc.go.jp/press/pdf/securevm.pdf
	同上	将来的な国内及びアジア圏への普及も視野に含めて言及頂ける事を切望します。 ＴＲＯＮの二の舞にならぬ事を強く危惧します。 （個人）	ご指摘の内容については、２００７年度以降の施策として、その一部が第５章第３節ウ）に記載されていますが、ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。 なお、施策の詳細につきましては、こちらをご参照下さい。 http://www.nisc.go.jp/press/pdf/securevm.pdf

分野	該当箇所	ご意見の概要	ご意見に対する考え方
	同上	趣旨について 　そもそもWindowsのＯＳ自体がクローズソースとなっていることから個人や組織単位で開発が出来ないようになっている。ＯＳについてもオープンソースを採用し、誰でも自由にセキュリティを高め、チェックする仕組みが大事である。 一企業（マイクロソフト）の対応だけを待っているというのは遅いと思う。 予算について 　計上された予算では現在の政府レベルの知恵では実現が不可能であると思う。 　そこで、予算内でローコストで安全なまったく新しい開発方法を提案する。 １、開発インフラについて 　ＯＳを含め、開発インフラもオープンソース化し、各企業、自治体、個人が自由にソースコードを改善、改良しそれを政府が吸い上げ、良いものだけを配布する仕組みを作る。 ２、開発コストについて 　政府が吸い上げ、良いものと判断し、配布したものだけにコストを払う。 ３、実行環境について 　政府が配布したＯＳ，ツールだけを国民は使うことが出来る。 ４、効果について 　オープンソース化することにより、セキュアなシステムを政府は安価に構築することが出来る 　また日本主導によるセキュア環境を世界に広めグローバルスタンダートとすることができる 具体的な方法 １、ＯＳについて 　一番情報量、開発者のいるＲＥＤＨＡＴをベースにする ２、政府判定について 　政府は改良、改善を評価する組織を作り、認定させるだけでいい ３、開発環境 　すべてオープンにし、政府から課題を出題し対応させる 以上によって、ローコストで確実にセキュアなシステムが完成する （株式会社ＳＲＡ）	ご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の一つとさせていただきます。 なお、施策の詳細につきましては、こちらをご参照下さい。 http://www.nisc.go.jp/press/pdf/securevm.pdf
	同上	1.構想・設計・技術はTRONベースで。 2.あらゆるOSをゲストOSにできる「メタOS」を創る。 3.デフォルトゲストOSにフリーなBTRONを用意する。 （個人）	ご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の一つとさせていただきます。 なお、施策の詳細につきましては、こちらをご参照下さい。 http://www.nisc.go.jp/press/pdf/securevm.pdf
	同上	ウワサでは、Ｘｅｎという技術をベースに、セキュリティ向上を狙ったＯＳ環境を作るようです。この方針はおかしいですね。まだまだ研究段階の技術です。さらに研究方針としても学術的に非常に疑問のある内容があり、研究として行うことすら疑義があります。 （有限会社デジタルインフラ）	本施策に基づき開発する次世代ＯＳ環境については、現時点で詳細な構造等について確定しておらず、どのように開発していくかを含め、今後検討していく予定です。 なお、施策の詳細につきましては、こちらをご参照下さい。 http://www.nisc.go.jp/press/pdf/securevm.pdf
	同上	技術基盤の開発に留まらず、中央省庁が当該技術を組込んだシステムを早期に採用し、わが国の技術によるセキュリティレベルの向上をコミットするべき。 （富士通株式会社）	ご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の一つとさせていただきます。 なお、施策の詳細につきましては、こちらをご参照下さい。 http://www.nisc.go.jp/press/pdf/securevm.pdf
	同上	次世代ＯＳ環境を開発するに際して、ソフトウエア的解決策のみでなく　、ファイルシステムのH/Wに物理的セキュリティ対策をかけるなどハード、ソフトの融合した抜本的対策を推進されるよう提案させて頂きます。 （インテリジェントディスク株式会社）	ご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の一つとさせていただきます。 なお、施策の詳細につきましては、こちらをご参照下さい。 http://www.nisc.go.jp/press/pdf/securevm.pdf
	③（イ）エ）電子政府システムのＩＰｖ６化	IPv6導入反対。 （有限会社デジタルインフラ）	ＩＰｖ６の電子政府における利用は、電子政府サービスにおける不正使用・情報漏えい防止等のセキュリティ強化、インタラクティブ化、府省庁をまたがる共同利用システム構築等に有益であり、また、早ければ２０１０年頃にＩＰｖ４アドレスが枯渇するとの予測があることから、本施策は必要なものであると考えております。

分野	該当箇所	ご意見の概要	ご意見に対する考え方
	③（ウ）イ）政府機関から発信する電子メール及び政府機関のホームページからダウンロードされる電子文書に係る成りすまし及び改ざんの防止	電子メールやダウンロードされる電子文書に限らず、政府機関のホームページ自体の成りすまし及び改ざんを防止する検討が必要であると考えます。 （株式会社日立製作所）	ご指摘の内容については、その一部が第２章第１節ア③（ウ）ア）に記載されていますが、ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	同上	電子署名が付された文書の有効期間に応じた中・長期的な保証方法について、ガイドラインが必要であると考えます。 （株式会社日立製作所）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	③（エ）ファイル（電磁的記録）のセキュリティ対策の推進	光ディスクなど可搬記録媒体のセキュリティ確保には暗号化による秘匿化ソフトのみでは十分でなく、媒体自身に物理的な暗号ｷｰを搭載する方式も同時に導入を検討して頂きたい。 （インテリジェントディスク株式会社）	ご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の一つとさせていただきます。 なお、本施策は、一連の情報流出事案の発生を踏まえ、部外への情報流出の防止を目的としたものであり、具体的なセキュリティの方式については、この目的にかなうよう適切に判断してまいります。
	④サイバー攻撃等に対する政府機関における緊急対応能力の強化	サイバー攻撃以外の、有事の際に対する障害対策も考慮すべき。 （株式会社CSKシステムズ）	ご指摘のとおり、「サイバー攻撃」以外の緊急事態への対処も重要であると考えていることから、 ご指摘の項目において、「政府機関に対するサイバー攻撃」に加え、「政府機関における情報漏えいや情報システムの障害等」（これらには、ご指摘のような、災害に起因するシステム障害も当然に含まれます。）の「発生を防止し、発生した場合には迅速かつ的確に対応するための」施策が記述されているものですが、ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	④ア）ａ）情報収集、分析・解析機能の強化	「各政府機関のホームページ等の監視」を「各政府機関のWebサーバ等の監視」に変更する。 （個人）	ご指摘を踏まえて、以下のような修正を加えます。 第２章第１節ア④ア）ａ）情報収集、分析・解析機能の強化 （前略）２００６年度において、各政府機関のwebサーバ等の監視を試行的に開始するとともに、（後略）
	⑤政府機関における人材育成	情報処理技術者試験以外に、国際的に通用する資格を見据えた人材育成も、検討が必要。 （株式会社CSKシステムズ）	ご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の一つとさせていただきます。
	同上	１行目から２行目「必要な知見や専門性を有する人材」を「必要な知見や専門性を有し国際的にも通用する人材」と修正するべき。 （(ISC)2 Japan）	ご指摘の部分は、今回とは別の意見の募集の手続きを経て既に決定された「第１次情報セキュリティ基本計画」からの抜粋であり、今回の意見の募集の対象ではないと考えていますが、ご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の一つとさせていただきます。
第１節イ　地方公共団体	②情報セキュリティ監査実施の推進	手引書，ガイドブックの作成・普及が必要 （個人）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	④イ）地方公共団体を対象とする情報セキュリティ研修の実施	１行目から２行目「高度な知識・技術を持つ人材育成」を「高度な知識・技術を持ち、国際的に通用する人材育成」と修正するべき。 （(ISC)2 Japan）	ご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の一つとさせていただきます。
第２節　重要インフラ	④ウ）ａ）電気通信事業分野におけるサイバー攻撃への対応強化	２行目から３行目「高度なＩＴスキルを有する人材の育成」を「高度かつ国際的に通用するＩＴスキルを有する人材の育成」と修正するべき。 （(ISC)2 Japan）	ご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の一つとさせていただきます。
	その他	Operating System の日本内製化（Virtual OS ではないもの）。 （(株)イマオコーポレーション）	ご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の一つとさせていただきます。
第３節　企業	①企業の情報セキュリティ対策が市場評価に繋がる環境の整備	４行目「普及・改善を図るとともに、」を「普及・改善を図るとともに人材育成評価自分を策定し、」と修正するべき。 （(ISC)2 Japan）	ご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の一つとさせていただきます。
	①ア）ｂ）電気通信事業における情報セキュリティマネジメントの強化	ISM-TG(電気通信事業における情報セキュリティマネジメント指針)の英文名称を、(ISM-TG: Information Security Management Guideline for Telecommunication)に訂正する。 (個人)	ご指摘を踏まえて修正を加えます。

分野	該当箇所	ご意見の概要	ご意見に対する考え方
	①ウ）情報セキュリティ関連制度と内部統制制度等との整合性確保	法律・ガイドライン等については、民間の意見を十分に踏まえつつ、各ルール間の整合性を確保するよう、関係するすべての省庁等が協力して検討すべきである。 例示されている内部統制についても、「会社法」およびいわゆる「日本版SOX法」の要請内容と、既存のセキュリティ対策基準等の要請内容との整合性確保について、法務省、経済産業省、金融庁、その他関係者が、NISC のリーダーシップの下で協力して検討すべきである。 （経団連）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	②質の高い情報セキュリティ関連製品及びサービスの提供促進	日本の企業内での情報伝達速度を速めるためには、メッセージング・アプリケーションが有効です。ただし、企業においては、MSNメッセンジャー、skype、Winnyなどの技術的にセキュリティの考慮がされていないコンシューマ向けのフリーコンテンツが利用されており、企業内情報漏洩の根源をなしています。 セキュアなメッセンジャーやファイル転送機能などの企業向けのセキュアなインターネット・アプリケーションの利用促進を行い、コンプライアンス犯罪の抑止を行うべきであるという一文を盛り込むべきであると考えます。 （株式会社Qript）	ご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の一つとさせていただきます。
	同上	システムインテグレーター向け施策が必要と思われる。 　具体的には、中小規模のシステムに適用可能なセキュアシステム設計・構築手法の研究等があげられる （NPO 日本ネットワークセキュリティ協会）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	②ア）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研究 その他 第３章第１節②ア） ｈ）	リスクの定量化や対策評価、対策費用対効果などの定量化の精度を向上させるために、被害の算出方法に関する取り組み強化が必要。 （NPO 日本ネットワークセキュリティ協会）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	②イ） ａ）情報セキュリティマネジメントシステム適合性評価制度の普及促進	「情報セキュリティマネジメントシステム適合性評価制度の内容を再検討し、セキュリティを向上させる施策と共に」を加えてください。 （有限会社日本ネット技術研究所）	ご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の一つとさせていただきます。
	②イ） ｂ）情報セキュリティ監査制度の普及促進	契約書に監査のベースとなる情報セキュリティ監査基準を付帯する保証型監査等、実効性の高い監査サ―ビスを推進するべき。 （富士通株式会社）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	②ウ）税制優遇措置	「ｃ）高度情報セキュリティ人材育成に関する研修等への参加及び資格取得をした場合の税制支援措置を実施する。」を追加するべき。 （(ISC)2 Japan）	ご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の一つとさせていただきます。
	②ウ） ａ）情報セキュリティ対策装置の取得時における税制優遇措置	企業におけるセキュリティ対策の向上と環境の整備としては物（セキュリティ機器）だけに限定されない「サービス」を対象とした税制優遇措置または、その他の支援措置として、地方の中小企業も視野に入れた、融資制度などをご検討頂きたい。 （NPO 日本ネットワークセキュリティ協会）	ご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の一つとさせていただきます。
	③企業における情報セキュリティ人材の確保・育成	ISMS監査員認定試験の創設を。 （個人）	ご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の一つとさせていただきます。
	同上 他に第２章第４節①及び②	初等教育の拡充をはじめ、広報啓発および情報発信の強化・推進、教育スタッフの育成および手法の研究等、多岐にわたる施策を統一的に推進すべきである。同時に、セキュリティに関する専門家の育成も重要であるので、文部科学省、経済産業省、総務省その他関係機関は、統一方針に従った施策を推進すべきである。 （経団連）	ご指摘の点については、第４節において「具体的施策の推進にあたっては、～（中略）～内閣官房及び関係省庁が整合性をとりつつ緊密に連携することとする。」と記載されているところですが、ご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の一つとさせていただきます。

分野	該当箇所	ご意見の概要	ご意見に対する考え方
	③ア）情報通信セキュリティ人材を育成するための研修事業への支援	「２００６年度において、情報通信ネットワーク・システムに対する攻撃や不正侵入などに対する多面的、双方的知識及び実践的な対処法を習得するための人材育成センターの開設を支援するとともに、セキュリティ人材を含む情報通信分野の専門的な知識かつ国際的に通用する技術を有する人材を育成するための研修事業に対し助成を行う。」と修正するべき。 （(ISC)2 Japan）	ご指摘を踏まえて、以下のような修正を加えます。 第２章第３節③ア）情報通信セキュリティ人材を育成するための研修事業への支援 ２００６年度において、情報通信ネットワーク・システムに対する攻撃や不正侵入などに対する多面的、双方的知識及び実践的な対処法を習得するための人材育成センターの開設を支援するとともに、セキュリティ人材を含む情報通信分野の専門的な知識や技術を有する人材を育成するための研修事業に対し助成を行う。
	④コンピュータウイルスや脆弱性等に対応するための体制の強化	コンピュータウイルス感染によるファイル交換ソフトへの情報漏洩を早期に発見対処するための官民連携体制の強化が必要。 （ドコモ・システムズ（株））	ご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の一つとさせていただきます。
	その他	実際の職場におけるセキュリティと法との温度差。 （個人）	ご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の一つとさせていただきます。
	その他	知財立国政策の中での知財経営・知財流通と情報セキュリティの観点を取り入れるべきであり、経済産業省・特許庁・文部科学省等との連携も必要である。 （テッドインパクト株式会社）	ご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の一つとさせていただきます。
	その他	レベルの低い民間企業、特に、地方の中小企業を対象としたレベルアップの施策が必要と思われる。 　具体的には、地方公共団体も政府機関と同等のセキュリティレベルとするべく支援することで、外注委託先の水準確保などにより、その委託先である地方の企業にも、効果を波及させるなどの枠組みを盛り込んでいただきたい。 （NPO 日本ネットワークセキュリティ協会）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
第４節　個人	本文３行目	「個人が情報セキュリティを当たり前のこと」の部分について、個人が、1）情報セキュリティ対策の実施を当たり前のこととして認識するのか、2）情報セキュリティが確保されていることを当たり前のこととして認識できる環境にするのかが不明であるため、どちらかを明確化した表現に変更する。 （個人）	ご指摘を踏まえて、以下のような修正を加えます。 第２章第４節個人 （前略）なお、①及び②の具体的施策の推進にあたっては、個人が情報セキュリティ対策を可能な範囲内で自主的に実施することが当たり前のこととして認識できる環境の整備や、（後略）
	①イ） ａ）全国的な普及啓発活動の実施 ｂ）ｅーネットキャラバンの実施	「無線LAN」の記述が全く無い。 （北陸無線データ通信協議会）	ご指摘の内容については、③ウ）「無線ＬＡＮのセキュリティ対策」にその内容を含める趣旨で記述しているものであり、今後の政策運営においても適切に対応してまいります。
	①イ）ａ）全国的な普及啓発活動の実施	内容の充実・強化を具体的に表すため、「新たな脅威としてのスパイウエア対策、フィッシング対策などの～」を付け加えてほしい。 （NPO 日本ネットワークセキュリティ協会）	ご指摘を踏まえて、以下のような修正を加えます。 第２章第４節①イ）ａ）全国的な普及啓発活動の実施 ２００６年度において、新たな脅威の動向を教材に反映する等、「インターネット安全教室」の内容の充実・強化を図りつつ、（後略）
	②広報啓発・情報発信の強化・推進	「各省庁・行政機関のセキュリティ情報及び民間のセキュリティ情報を一手にまとめたポータルサイトの構築」を加えてください。 （有限会社日本ネット技術研究所）	ご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の一つとさせていただきます。
	②ア）ａ）情報セキュリティに関する周知・啓発活動の推進	周知・啓発の手段として、政府広報と、地方自治体広報など、記載されていない既存の広報手段も明記いただきたい。 （NPO 日本ネットワークセキュリティ協会）	ご指摘の内容については、「国民一人一人に対する適切な情報提供や、メディア等を活用した広報啓発活動」として記載されていますが、ご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の一つとさせていただきます。

分野	該当箇所	ご意見の概要	ご意見に対する考え方
	③個人が負担感なく情報関連製品・サービスを利用できる環境整備	ア） は、毒は毒をもって制するという考え方は危険きわまりないため廃止！ 代わりに「ＷＥＢでウィルス・チェックやスパイウェア・チェックのできるサイト（オンライン・チェックのサイト）の作成公開」を追加。 （有限会社日本ネット技術研究所）	１つ目のご指摘につきましては、当該施策は、ボットプログラムに感染したコンピュータに対する対策についての検討を開始するものであり、ご指摘のような考え方に基づくものではありません。また、２つ目のご指摘につきましては、そのようなサイトは既にいくつかあります。
	同上	ファイル交換ソフト利用等によるリスク分析ツールの提供が必要。 （ドコモ・システムズ（株））	ご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の一つとさせていただきます。
	③ウ）「無線ＬＡＮのセキュリティ対策」	以下に修正をお願いできないか。 『2006年度において、無線LANのセキュリティに関するガイドライン「安心して無線LANを利用するために」を時代に合った形に改訂し更なる普及の推進を図るとともに、「インターネット安全教室」の冊子等においても、無線LANの安全な使い方に関するコンテンツの充実を図る。』 （北陸無線データ通信協議会）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	その他	全ての省庁について、パブリックコメント募集によって収集された個人情報は、全て、非公開とするべきと考える。どうしても公開したい場合は、意見募集時に、場合によっては公開する旨を公示するだけでなく、具体的に、どのような場合に個人情報を公開するのか、具体的なガイドラインをあらかじめ策定して示し、意見募集のウェブページ上に、そのガイドラインへのリンクを明示しておくべきである。 （個人、その他同旨１件）	ご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の一つとさせていただきます。 なお、行政手続法に基づく意見公募手続については、「行政手続法第６章に定める意見公募手続等の運用について」（総管１３９号平成１８年３月２０日総務省行政管理局長）があり、この通知の【５．意見提出方法】（２）において、意見提出を実質的に制約するような条件を付してはならないことの例として、「不必要な個人情報の記載を強制し、また、これを公表すること。」が挙げられています。

第３章　横断的な情報セキュリティ基盤の形成			
分野	該当箇所	ご意見の概要	ご意見に対する考え方
第１節 情報セキュリティ技術戦略の推進	②情報セキュリティ技術開発の重点化と環境整備	研究開発項目として、携帯端末など組込み系に関するセキュリティ対策の調査研究も実施してほしい。 （NPO 日本ネットワークセキュリティ協会）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。なお、ご指摘の内容については、「組込みシステム向け情報セキュリティ技術」（平成１８年度科学技術振興調整費の採択課題）等において研究開発に取り組まれるものと承知しております。
	②ア）ｇ）フェイルセーフな情報セキュリティ技術の研究開発	情報を預かる際に保証金を支払う仕組みを政府主導で作って欲しい。 具体的にはAmazonギフト券のようなWebサービスが良い。 （ＫＮＣ）	ご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の一つとさせていただきます。
	②イ）短期的な研究開発・技術開発の施策	「高セキュリティ機能を支援する次世代検疫ネットワーク環境の開発」について。 （個人）	ご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の一つとさせていただきます。
	②ウ）ｂ）高信頼性端末の電子認証基盤の研究開発	PCのマザーボードにセキュリティチップTPM（Trusted Platform Module）を搭載する方式のみでなく、記憶メディア（光ディスク、ハードディスク、他）にセキュリティチップを搭載する方式についても、併せて研究開発の対象としてご検討賜りたく。 （インテリジェントディスク株式会社）	ご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の一つとさせていただきます。
	その他	Microsoft社に依存しない独自ＯＳの開発。 （(株)まりも）	ご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の一つとさせていただきます。
第２節 情報セキュリティ人材の育成・確保	全般 （その他に第２章 第１節 ア ⑤、および 第３章 第１節 イ ④、 第２章 第２節 ④、 第２章 第３節 ③、 第２章 第４節 ①、 第３章 第２節 ①）	政府として関与すべき人材育成については、高度人材育成だけでなく、啓蒙教育を積極的に実施する必要がある。 上記該当箇所に人材育成の記述があるが、高度人材育成以前の問題として、政府によりマインドセットとしての啓蒙教育を実施する必要があると考える。 学校教育の場についても、教師を通じた啓蒙や教育ではなく、セキュリティ専門家から直接啓蒙や教育を出来る場を作る。 （SEA/J事務局）	ご指摘の啓蒙教育については、第２章第４節②等に記述されているところですが、ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	具体的施策部分全般	離職者・在職者を含めた幅広い労働者に対し、実践技術の訓練の場を提供している職業訓練も施策に位置づけるべき。 （神奈川県立産業技術短期大学校）	ご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の一つとさせていただきます。
	②情報セキュリティに関する資格制度の体系化	情報セキュリティ関連の資格は「情報セキュリティアドミニストレータ」を代表とする技術系が有名だが個人情報保護～内部統制～BCP（企業継続）を推進する場合に必要な情報セキュリティ「マネジメント系」の資格についてもご検討いただきたい。 （株式会社ニューオータニ）	ご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の一つとさせていただきます。
	②情報セキュリティに関する資格制度の体系化	ISMS監査員認定試験の創設を。 （個人）	ご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の一つとさせていただきます。

分野	該当箇所	ご意見の概要	ご意見に対する考え方
	②情報セキュリティに関する資格制度の体系化（資格制度の創設について）	第２章 第２節（1）の「競争的活動・自主的取組みを促進する部分」として考えた場合、政府として新たに資格制度を創設するのではなく、市場に現存する資格の有効性を検討し、ロードマップとして示していく必要があると考える。 既に、NPO 日本ネットワークセキュリティ協会では、同様の取り組みを始めており、推奨教育や資格を検討し、ロードマップを示していこうとしている。 JNSA該当URL： http://www.jnsa.org/active/2005/active2005_4_2.html （SEA/J事務局）	ご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の一つとさせていただきます。
	その他	人材を育成した後のキャリアパスや人事評価制度に関する調査・研究も行うべき。 （神奈川県立産業技術短期大学校）	ご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の一つとさせていただきます。
第４節 犯罪の取締り及び権利利益の保護・救済	①ア）d）サイバー犯罪に適切に対処するための法整備等の推進	「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」におけるサイバー犯罪条約締結のためのいわゆるサイバー取り締まり法案について、定義や範囲が不明確かつ広すぎるので、国民生活を圧迫しかねません。国際条約を優先するあまり国民が不利益をこうむるのでは本末転倒ではないでしょうか。通信記録の傍受を認める条約は通信の秘密の保障を明記しているわが国の憲法とも対立します。日本の法制度にあわない条約に無理に批准すべきではないと考えます。現在の政府与党案は廃案にすべきです。 （個人）	「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」におけるハイテク犯罪に対処するための法整備は、これによって国民生活を圧迫するものではなく、また、我が国の憲法と対立するものでもないと考えております。
	②サイバー空間の安全性・信頼性を向上させる技術の開発・普及	電子証明書（電子署名）普及のため、個人については、公的個人認証サービスによる電子証明書の無償配布および利用可能範囲の拡大、法人については、いわゆる「職印」に相当する電子証明書の利用を許容するといった、思い切った施策を検討すべきである。 （経団連）	ご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の一つ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			
分野	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	（１）内閣官房情報セキュリティセンター（NISC）の強化	内閣官房情報セキュリティセンター（以下、NISC という。）の強力なリーダーシップの下、政府のあらゆる機関が、「セキュア・ジャパン２００６（第１次情報セキュリティ基本計画）」に従い、統一の取れた施策を実施することを徹底すべきである。 （経団連）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。
	（２）各府省庁の強化	全ての省庁について、パブリックコメント募集によって収集された個人情報は、全て、非公開とするべきと考える。どうしても公開したい場合は、意見募集時に、場合によっては公開する旨を公示するだけでなく、具体的に、どのような場合に個人情報を公開するのか、具体的なガイドラインをあらかじめ策定して示し、意見募集のウェブページ上に、そのガイドラインへのリンクを明示しておくべきである。 （個人）	ご指摘の手続制度については、総務省の所掌事務となっており、内閣官房情報セキュリティセンターにおいては、意見提出上の留意点をホームページにお示ししております。
	その他	内閣（首相官邸）の役割が明確でない。 （神奈川県立産業技術短期大学校）	ご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の一つとさせていただきます。
第３節 持続的改善構造の構築	（３）評価指標の確立	公表できるレーダーチャートのような指標を。 （個人）	ご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の一つとさせていただきます。
	同上	指標に人材育成に関する評価指標も入れていただきたいと考えます。 （(ISC)2 Japan）	ご指摘の点は重要と認識しており、今後の政策運営に適切に反映してまいります。

第５章　２００７年度の重点施策の方向性			
分野	該当箇所	ご意見の概要	ご意見に対する考え方
第１節 模範となる領域の情報セキュリティ対策の底上げ	ア）ａ）PDCAサイクルの定着と本格的評価の推進	各府省庁内における情報セキュリティ対策の成果（ベストプラクティス）を横展開することにより、政府全体の情報セキュリティ対策が効率的に推進できることを、盛り込んでは如何か。 （株式会社日立製作所）	第２章第１節ア①ウ）「実施手順の作成支援及び技術的情報の提供と情報の共有」において記載しております。
	イ）ａ）重要インフラ分野横断的な対策の推進に向けた状況把握能力の強化	情報漏洩を防止するため、企業のWinny等のP2Pネットワークの遮断状況等の調査を行うべきであるという趣旨で、「現状の脅威調査と対策を行った後に」を先頭に入れてください。 （有限会社日本ネット技術研究所）	ご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の一つとさせていただきます。
	イ）ｄ）重要インフラ機能的演習の推進	機能的演習を行う際には、ハード・ソフトの環境整備と具体的な演習フローの準備をすすめるべき。 （富士通株式会社）	ご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の一つとさせていただきます。
	その他	机上演習を行う上で重要な、各種テーマに基づいたシナリオに関する調査・研究も行うべき。 （神奈川県立産業技術短期大学校）	ご指摘の内容については、今後の政策の推進に当たって参考の一つとさせていただきます。
第２節 取組みが遅れがちな主体の対策の底上げ	その他	遅れている業務基盤（PC,DBを含めた業務インフラ）の確立をまず優先するべき。 （セキュリティ計画に相応しいかは疑問ですが、現場レベルでは非常に問題であると思っています。トップダウン以外、現状を変えることは出来ないでしょう。資源の無い国、日本の唯一の資源である教育を助けて頂ければ幸いです。） （神奈川県立産業技術短期大学校）	ご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の一つとさせていただきます。
第３節 横断的な情報セキュリティ基盤の底上げ	その他	高セキュリティ機能を実現する次世代ＯＳ環境だけでなく、次世代データベースと情報セキュリティの観点も取り入れるべきである。 （テッドインパクト株式会社）	ご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の一つとさせていただきます。 なお、施策の詳細につきましては、こちらをご参照下さい。 http://www.nisc.go.jp/press/pdf/securevm.pdf