

「情報セキュリティ2010」(案)に対する意見募集の結果の概要について

経緯

[第23回情報セキュリティ政策会議(2010.5.11)]

- 「国民を守る情報セキュリティ戦略」を政策会議において決定。



- 「情報セキュリティ2010」(案)を作成し、意見募集を実施。

意見募集及び結果の概要

- 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: 2010年6月15日(火) ~ 28日(月)
- コメント総数: 77件【内訳: 10企業・団体から延べ39件、15個人から延べ38件】
- コメント概要: 施策に対する見解、施策実施に当たっての配慮要望等。
 - ・ 中小企業における情報セキュリティ対策の推進に関する施策について、その対象や目的を明確な表現とすべき。
 - ・ クラウド・コンピューティングの定義を明確にすべき。

コメントへの対応

- 中小企業における情報セキュリティ対策の推進に関する施策について、対象となる中小企業の範囲を明確化するなどの修文を行った。
- クラウド・コンピューティングの定義を脚注に追加した。
- 頂いた御意見は、今後の政策運営にあたっての参考とするなど、適切に活用させて頂く。

| 受付番号 | 枝番号 | 提出者 | 概要 | ご意見に対する考え方 |
|------|-----|----------------------------|--|---|
| 1 | 1 | 個人 | 1(1)イ)サイバーテロ対策に係る体制等の強化(警察庁)について、下記の具体的施策を提案する。 《サイバー危機疑似体験》 日本国内のセキュリティ関連省庁と民間企業の偉い人々が参加し、日本全国に関するサイバー危機のケーススタディを開催する。2時間番組などを組んでテレビで放送する。 | 警察庁では、各種啓発活動を通じ、サイバー攻撃等への危機意識の醸成を図って参ります。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 | 1 | エンベ株式会社 | 「銀行口座(=金融資産)」については、口座開設や現金授受の際、「より確実に本人を特定する手段」を用いる事で、犯人グループの特定が可能となる。個人情報に直結する内容に関しては、「登録時点から情報の真偽を確認し判別した上で情報を登録する」手段についても、検討する必要がある。 | 御指摘の内容については、今後の施策の検討の際の参考とさせていただきます。 |
| 2 | 2 | | 【該当箇所】 P33「クラウドコンピューティング化に対応した情報セキュリティ確保方策、標準化」 ア)クラウド化に対応した情報セキュリティ確保方策の検討(内閣官房、総務省及び経済産業省) P62(5)① サイバー空間の安全性・信頼性を向上させる制度の検討等 ウ)「データセンターの安全・信頼性に係る情報開示指針」の活用・普及(総務省) 【意見】 「データセンターの安全・信頼性に係る情報開示指針(第1版)」に記載されている60～72のセキュリティ項目自体に、脆弱性が潜んでいるため、前述の利用指針や情報開示指針の活用・普及を用いたとしても、セキュリティ面の脆弱性は回避できない。「データセンターの安全・信頼性に係る情報開示指針」の改定も含めて、物理面からの情報セキュリティの確保をご検討下さい。 | 物理的な観点からも情報セキュリティについて検討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 | 個人 | クラウドコンピューティングの情報セキュリティ対策にあたっては、クラウド上の属性情報などを活用してはどうか。 | クラウドコンピューティング技術における情報セキュリティの確保の在り方については、今後も引き続き検討してまいります。 |
| 4 | 1 | 個人 | 取組みの背景・目的から始まり具体的な取組み内容および担当すべき所管省庁が明記されており、非常に有意義なものとなっている。 | 情報セキュリティ2010に対し、評価をいただきましてありがとうございます。 |
| 4 | 2 | | 取組みの中心となる内閣官房の「情報の集約」「各政府機関に対して当該分析結果を定期的に提供する」ということが可視化され、継続的に実施されるしくみ等について、もう一歩ふみこんだ記述があっても良いのでは。(例:「定例」委員会の組織図) | 「情報の集約」や「各政府機関に対して当該分析結果を定期的に提供する」ことは、内閣官房が日常的に行う業務であり、定例委員会等の組織を立ち上げて行う業務ではないことをご理解ください。 |
| 4 | 3 | | 日経新聞の記事に、菅首相の経済成長戦略として、ITに視点をあてた構想が種々記載されていたが、「セキュリティ」のキーワードが一言も入っておらず、非常に疑問を感じた。 | 「新成長戦略」(6月18日閣議決定)においては、「個人情報保護、セキュリティ強化などの対策を進めて国民の安心を確保しつつ、…」とのセキュリティに言及した記述が盛り込まれているところです。今後も施策についての周知に努めてまいります。 |
| 4 | 4 | | 情報セキュリティ2010が、今後、単なる「絵に描いた餅」とならぬよう、実行されていくことを願う。 | 情報セキュリティ2010が実効性のあるものとなるように、施策を推進してまいります。 |
| 5 | 1 | 個人 | 【該当箇所】 P57 2. (4)①情報セキュリティ関連の研究開発の戦略的推進等 (セ)セキュアでグリーンなクラウドコンピューティング環境の整備(経済産業省) 【意見】 クラウドコンピューティングの安全性については、監査と並んで情報セキュリティ格付制度に関する環境の整備と検討を行うのが望ましい。 | クラウドコンピューティングの安全性の確保は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。 |
| 6 | 1 | 財団法人 日本情報 処理開発 協会 | 【該当箇所】 2(1)③・中小企業に対する情報セキュリティ対策支援 イ) 【意見】 イ)のc)として、以下を追加 「中小企業における情報セキュリティの底上げを図るべく、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を促進する。」 | 中小企業における情報セキュリティの向上方策は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。 |

| | | | | |
|----|---|----|---|--|
| 7 | 1 | | <p>【該当箇所】 p.14 サ) 政府機関のドメイン名であることが保証されるドメイン名の使用の推進</p> <p>【意見内容】 政府事業を民間委託した際の当該事業のウェブサイトにおいても、.go.jp ドメインを使用するように環境整備をする必要がある。</p> | 御指摘の環境については、統一基準等で既に整備済みであり、各府省庁への周知を行うなど使用に向けた取組を実施しているところです。 |
| 7 | 2 | 個人 | <p>【該当箇所】 p.28 I) 情報セキュリティインシデントへの対応 p.30 III) ソフトウェアの脆弱性対策</p> <p>【意見内容】 ウェブアプリケーションの脆弱性を善意の第三者が発見した際、その行為が不正アクセス禁止法違反で罰せられないことを明確にし、発見者が脆弱性情報を安心して届け出られるように環境整備をする必要がある。</p> | 御指摘の内容については、今後の政策の検討の際の参考とさせていただきます。 |
| 7 | 3 | | <p>【該当箇所】 p.37 安全な電子商取引の推進</p> <p>【意見】 なりすましによる購入契約によって、なりすまされた本人が支払い責任を負うことのないよう、消費者保護のための環境整備をする必要がある。</p> | 御指摘の内容については、今後の政策の検討の際の参考とさせていただきます。 |
| 8 | 1 | 個人 | <p>【該当箇所】 P60 ②情報セキュリティ人材の育成 エ) 先導的ITスペシャリスト育成推進プログラム</p> <p>【意見】 セキュリティ教育においては、技術的・理論的知識の教育は当然のことながら、そのとりまとめとして「人」と「人」を動かすマネジメント能力が大変重要。先導的ITスペシャリスト育成推進プログラムにおいては、この点を特に重視している。具体的には、インシデント対策をはじめとした情報共有や人的交流などをはじめとして、大学・組織間を超えた「人的ネットワークの形成」が非常に大きな成果。この点を踏まえた記載があると、本プログラムの意義がより分かりやすくなるものではないか。</p> | 御指摘の内容については、文部科学省の施策全般に関するものではなく、個別の大学における取組の特色に関するものです。該当箇所については、文部科学省の施策を記述していますので、個別の大学における取組の特色については記述しないこととさせていただきます。 |
| 9 | 1 | | <p>【該当箇所】 P2</p> <p>【意見】 2009年の米韓におけるサイバー攻撃は実際にはさほど大きな被害のある攻撃ではなかったにもかかわらず、世間から注目されたことで、結果として攻撃としての有効性を持ってしまった。「国民生活を守る」取り組みを立案、実行する上で、国民の冷静な反応を引き出すことが重要。</p> | 御指摘の内容については、今後のサイバー攻撃対処に関する施策推進に当たっての参考とさせていただきます。 |
| 9 | 2 | 個人 | <p>【該当箇所】 P2</p> <p>【意見】 「能動的な情報セキュリティ対策」の定義について説明が必要。</p> | 「能動的な情報セキュリティ対策」につきましては、「国民を守る情報セキュリティ戦略」の2頁に記述がありますので、併せてご覧ください。 |
| 9 | 3 | | <p>【該当箇所】 P2</p> <p>【意見】 「情報セキュリティ分野で指導的な役割を果たす国家」、または「世界最先端の『情報セキュリティ技術先進国』」(技術の2字を追加)ならよいのですが、「世界最先端の『情報セキュリティ先進国』」には賛成できません。</p> | 技術の重要性は申すまでもありませんが、情報セキュリティに関しては、技術を含めた包括的な取組が不可欠であると考えています。 |
| 10 | 1 | | <p>【該当箇所】 全般</p> <p>【意見】 日本独自の先進的な考え方をもっと随時に進めていくべきである。現状、ISOの規格なども含め、欧米にイニシャチフをすべて取られており、その規格が逆輸入され、日本の風土に合っていないものを強引に当てはめている。情報セキュリティは国際的に考えていくべき問題ではあるが、グローバルに関係する企業はほんの一握りである。</p> | 国際戦略の強化は、「国民を守る情報セキュリティ戦略」における「新たな環境変化に対応した情報セキュリティ政策の強化」の5本柱の一つに掲げられているところです。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。 |

| | | | | |
|----|---|----------------------------------|--|--|
| 10 | 2 | ArmzNET (アームズ ネット) | 【該当箇所】 全般 【意見】 クラウドコンピューティングも区分を明確に整理し、グローバルなクラウドの場合はトラブル時の法的な問題についても、十分言及しておくべきである。 | 御指摘の内容については、今後のクラウドコンピューティングの技術戦略の検討に当たっての参考とさせていただきます。 |
| 10 | 3 | | 【該当箇所】 全般 【意見】 個人情報や情報セキュリティの事故が、官公庁などで依然として多い。官公庁もマネジメントシステムを導入していくべきではないか。 | 「国民を守る情報セキュリティ戦略」に明記された「事故前提社会」の考え方に基づき、情報セキュリティに係る事故に適切に対応していくため、各府省庁における情報セキュリティ対策を引き続き検討していきます。 |
| 11 | 1 | 個人 | 【該当箇所】 「Ⅱ 具体的な取り組み」全般について 【意見】 政府機関や重要インフラ事業者の情報システムについては、これまでに発生した事故や事件などで判明している脆弱な部分および今後発生が予想される部分を複数の方式で多重化すべきであるとする。 | 御指摘の内容に対する取り組みについては、各主体の情報セキュリティガバナンスの考え方を踏まえて対策を講じていくことが重要であると考えます。御指摘の内容については、今後の政策運営の参考とさせていただきます。 |
| 12 | 1 | 個人 | 【該当箇所】 P29 ③ その他の基盤強化、マルウェア対策等の充実・強化等 【意見】 インシデント発生時の複製を許可する為の著作権法の改定 | 裁判手続きで用いる証拠の保全のための複製については、著作権法第42条により、一定の条件の下で著作権者の許諾なく行うことが認められています。また、文化審議会著作権分科会報告書(平成21年1月)では、コンピュータ・プログラムのリバース・エンジニアリングについて障害の発見等の一定の目的のための調査・解析について権利制限を早期に措置する必要がある旨報告されています。御指摘の点については、同報告書の内容も踏まえ、今後の政策運営に適切に反映してまいります。 |
| 12 | 2 | | 【該当箇所】 P47 ④ サイバー犯罪に対する態勢の強化 【意見】 オープンソースのデジタル・フォレンジック ツールの捜査への活用を推進すべき | 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。 |
| 13 | 1 | データベース・セキュリティ・コンソーシアム (DBSC) | 【該当箇所】 2(1)③中の「IV)他の関連取り組み」 【意見】 以下を追加して頂きたい。 「データベース強化への取組： 個人情報等機密情報が格納されているRDBMSに関わる管理者権限取り扱い方法の改善、暗号化、ログの収集などの対策を促進するための基準の策定、普及促進のための検討を行う。」 | 様々な観点からプライバシー保護技術について検討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、今後の政策の推進にあたっての参考とさせていただきます。 |
| 14 | 1 | 日本コンピュータセキュリティリサーチ株式会社 (JCSR) | 【該当箇所】 ③国際連携の強化 【意見】 AVAR、及びJCSRが、「情報セキュリティ2010」の趣旨にある、「国際連携の強化」に関する具体的な取り組みに参加する事で、より有効なものになると考える。 | 国際連携の推進は重要であると認識しており、具体的な取組については今後検討してまいりたいと考えます。 |
| 15 | 1 | (社)電子情報技術産業協会 情報法規 専門委員会 | 【該当箇所】 P44 「各事業分野ごとの個人情報保護に関するガイドラインの見直し」 【意見】 【具体的施策】ア)の内閣官房及び関係府省庁においても、「暗号化等を行うインセンティブの在り方を検討する」こととまらず、総務省の取り組みを参考に、技術的措置が講じられていた場合の事業者の手続きの緩和について、内閣府による標準的ガイドラインや各省庁のガイドライン等に明記し、実施するよう検討していただきたい。 | 個人情報に対する技術的保護措置の適用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、経済産業省では技術的措置が講じられていた場合の事業者の手続き緩和について平成21年10月9日にガイドラインを改正し、対応しています。 |

| | | | | |
|----|---|-----------------|---|---|
| 16 | 1 | 株式会社 インフォセック | <p>A.担当省庁について (A)現在の案 現在の案を纏めると以下のような構造になっていると解釈しました。 (情報セキュリティ事案) (担当省庁) サイバー犯罪 :警察庁 サイバーテロ対策 :警察庁 サイバー攻撃(インシデント)対応調整:経済産業省 サイバー攻撃等 :防衛省</p> <p>(B)当社意見 事案の重要性に鑑み、以下のような構造が必要だと考えます。 (情報セキュリティ事案) (担当省庁) サイバー犯罪 :警察庁 サイバーテロ対策 :防衛省 サイバー攻撃(インシデント)対応調整:防衛省 サイバー攻撃等 :防衛省</p> | 各施策の担当府省庁を記載しておりますが、実際の事案に際しては、個々の具体的な状況に応じて関係省庁が緊密に連携しつつ対応します。 |
| 16 | 2 | | <p>B.対応調整について (A)現在の案 サイバー攻撃(インシデント)対応調整に経済産業省があたることとなっています。 (B)当社意見 サイバー犯罪、テロ、攻撃、インシデントの全ての事象で対応調整が必要です。その調整は、国家防衛の局面をもつと考えられるので、防衛省を中心に、関係省庁が連携をもつ必要があると考えます。</p> | 一般ユーザや企業等に対するサイバー攻撃対応調整に関しては、経済産業省の事業の一環として、国際的なCSIRT連携の枠組みを利用して行っています。 御指摘のサイバー犯罪、テロ攻撃、インシデントについて、各省庁がそれぞれの役割を果たすとともに、連携し、内容に応じて適切に対処してまいります。 |
| 17 | 1 | | <p>【該当箇所】 全体 【意見】 現実に大規模サイバー攻撃が発生した場合に「国民を守る」ためには、正しい情報の迅速な把握と、国民への周知が必須であるが、情報収集ばかり記載され、国民に知らしめる組織、手段等の記載がみあたらない。</p> | 大規模サイバー攻撃事態が発生した際には、情報の集約のみではなく広報が重要であることは御指摘のとおりです。「緊急事態に対する政府の初動対処体制について(平成15年11月21日閣議決定)」に基づき定められる「緊急事態に対する政府の初動対処体制実施細目」において、当該事態及びこれへの対処に関する状況について、積極的に広報を行うことが定められております。これに基づき、政府は国民への周知を推進してまいります。 |
| 17 | 2 | | <p>【該当箇所】 P5「大規模サイバー攻撃事態等発生時の初動対処に係る訓練の実施等」 【意見】実施主体が内閣官房及び関係省庁となっているが、これは防衛省も大きくかかわるべきである。</p> | 関係府省庁に防衛省も入っており、訓練の実施に際して必要に応じ関わって参ります。 |
| 17 | 3 | | <p>【該当箇所】P5「サイバーテロ対策に係る体制等の強化」 【意見】サイバーテロ犯人の目的がサービスの停止や対応の混乱の露呈を目論んでいる可能性は十分に想定される。そのため、首謀者やその背後関係や使用手口の捜査の目線もあるが、攻撃を受けている最中においても、サービスを継続していくかの観点が極めて重要である。そのためには、情報収集や技術的な向上を図るだけでなく、最悪の想定と代替策の事前検討、並びにその発動と解除にかかわる体制の整備と訓練の実施を並行して行い、必要技術や情報へのフィードバックを行える体制を整備いただきたい。</p> | 御指摘の内容については、P5「大規模サイバー攻撃事態発生時の初動対処にかかる訓練の実施等」において検討することとなっております。 |
| 17 | 4 | | <p>【該当箇所】P5「重要インフラに対するサイバーテロ対策に係る官民の連携強化」 【意見】サイバー攻撃に対する連携の強化の主体が警察庁であることに異存はないが、サブに防衛省と法務省を加えてはいかがか。</p> | 当該施策は実施主体が警察庁であることから、警察庁のみの記述となっておりますが、訓練・演習の際には必要に応じ関係する省庁と連携することを否定する趣旨ではありません。 |
| 17 | 5 | | <p>【該当箇所】 P6「サイバー企画調整官(仮称)の新設(防衛省)」 【意見】企画調整官の新設とは、当該任務を担う部署を新設頂きたい。単に役割を持った人を立てるだけでは、機能しないと考える。</p> | 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。 |
| 17 | 6 | | <p>【該当箇所】 P7「デジタルフォレンジックに係る取組の推進(警察庁)」 【意見】最近では、被害対象が現実的には国内組織であるにもかかわらず、仮想技術やクラウドの活用により、技術的にフォレンジックを実施出来ないこと、また、データや処理しているサーバの物理的な場所を特定することも難しいケースも予想される。適切に、日本や関連組織を守っていける法整備や運用の想定を実施いただきたい。</p> | 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。 |

| | | | | |
|----|----|-------------|---|---|
| 17 | 7 | | <p>【該当箇所】 P11「公開ウェブサーバに対する脆弱性検査の実施」 【意見】 検査実施を「希望府省庁」としているが、公開サーバ全てに行うべきと考える。</p> | <p>公開ウェブサーバに対する脆弱性検査については、既に一部の府省庁で実施しているところであり、未だ実施できていない府省庁に対して、NISCが可能な範囲で協力をを行うものです。</p> |
| 17 | 8 | 株式会社 ラック | <p>【該当箇所】 P12「政府全体でのPDCAサイクルの定着と浸透」 【意見】 PDCAの評価結果だけでなく、今後どういうプランで改善していくかの具体的指針を公表することを望む。</p> | <p>御指摘の具体的指針については、PDCAサイクルの中で見いだされるものであると理解しています。</p> |
| 17 | 9 | | <p>【該当箇所】 P13「コ」政府機関から発信する電子メールに係る成りすましの防止」 【意見】 電子メール以外の新たなメディアへの対応も必要である</p> | <p>今後も、国民生活に密接に関係してくる新たなサービスに、適切に対応していきたいと考えています。</p> |
| 17 | 10 | | <p>【該当箇所】 P15「政府機関統一基準の見直しの実施」 【意見】 見直しにあたっては、肝心要のデータの格納場所であるデータベースセキュリティにかかわる基準の策定と、事後の調査(フォレンジック)が可能な基準の策定をお願いしたい。</p> | <p>当センターでは、現在、政府機関統一基準の見直しを実施しているところであり、御指摘の内容については、その参考とさせていただきます。</p> |
| 17 | 11 | | <p>【該当箇所】 P29「ア」マルウェアの難読化に対応したウイルス検出・対応技術の検討」 【意見】 ウイルス検出・対応技術の検討結果の実用化について、調査によって洗い出された「マルウェアの検体解析・対策の研究開発における課題」が実用性を伴った技術開発に反映されるよう期待する。攻撃手法や攻撃対象の変遷が早い、情報セキュリティの分野の中で、新しい技術が、実際の運用や実用に耐えうる設計がされることが必要であると考ええる。</p> | <p>御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。</p> |
| 17 | 12 | | <p>【該当箇所】 P37「プロバイダによる侵害対策措置の促進」 【意見】 「インターネット上の侵害コンテンツに対する新たな対策措置」とあるが、日本においてはフェアユースの考え方が著作権法上認められていない。その中で何を「侵害コンテンツ」とするのかは議論も多いところである。我国の成長と適切な権利保護のための仕組みの再構築をにらんで対応をお願いしたい。</p> | <p>プロバイダと権利者の協働による侵害対策措置の促進を図るに当たっては、権利の保護や制限が適切に行われる制度が構築されていることが重要と考えます。</p> |
| 17 | 13 | | <p>【該当箇所】 ・P44「ア」各事業分野における個人情報保護に関するガイドラインの見直しの検討」 ・P44「安全管理措置に係る「電気通信事業における個人情報保護に関するガイドライン」の見直し」 【意見】 大賛成である。適切な暗号化並びに管理運用を行っている場合の、流出事故に関する報告・連絡・再発防止策提示などにかかわる運用の軽減(適切化)を行っていただきたい。</p> | <p>個人情報に対する技術的保護措置の適用は重要であると考えており、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。</p> |
| 17 | 14 | | <p>【該当箇所】 P59「ウ」情報セキュリティ資格の周知」 【意見】 我国の国際競争力を図る上で、「国際的」に通用する資格の周知と徹底は政策上極めて重要である。</p> | <p>情報セキュリティ資格の周知は重要であると考えており、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。</p> |
| 17 | 15 | | <p>【該当箇所】 P58「b」情報セキュリティ人材育成に係る枠組みの検討」 【意見内容】 文章内に「職種ごとのモデルキャリア開発計画を広報・普及する」という記載があるが、この取組には大いに賛成である。人材を有効に活用する上でも有効であると考ええる。</p> | <p>今後とも引き続き、情報セキュリティ人材を含めた高度IT人材の育成に取り組んで参ります。</p> |
| 18 | 1 | 個人 | <p>【該当箇所】 19ページのイ)ウ) 【意見】 一般の会社組織で通常実施されているような個人情報保護教育を、教職員に対し定期的実施するといった、より具体的に効果の期待できる内容を、盛り込むことはできないのでしょうか？</p> | <p>御指摘のとおり、教職員に対する個人情報保護教育は非常に重要であると考えており、子どもたちのインターネットの安全・安心な利用に向けた啓発のための講座(「eネットキャラバン」)を通信関係団体と連携しながら実施しております。今後とも個人情報保護教育を推進してまいります。</p> |

| | | | | |
|----|---|----|---|--|
| 19 | 1 | 個人 | <p>【該当箇所】本文44ページ ③ 個人情報保護の推進「プライバシー保護技術の適切な利用促進」に関する【具体的施策】ア)各事業分野における個人情報保護に関するガイドラインの見直しの検討 【意見】原文の「…インセンティブの在り方を検討する。」の次に、「それを踏まえて、省庁毎のガイドラインの整理統合をさらに推進する。」の文を追記していただきたい。</p> | 御指摘の内容については、今後、個人情報保護に関するガイドラインの見直しの検討の実施に当たっての参考とさせていただきます。 |
| 19 | 2 | | <p>【該当箇所】本文45ページ ③ 個人情報保護の推進「国際的なフレームワークへの対応」に関する【具体的施策】ア)個人情報の保護に関する国際的な取組への対応 【意見】原文の「…国際的な理解を求める。」の次に、「平行して、第三者機関による執行の制度の実現について検討を進める。」の文を追記していただきたい。</p> | 御指摘の内容については、各種の国際的な取組や今後の消費者委員会における審議等を踏まえ、今後の検討に当たっての参考とさせていただきます。 |
| 19 | 3 | | <p>【該当箇所】P45③ 個人情報保護の推進「個人情報保護法の見直し」に関する【具体的施策】ア)個人情報保護法の見直し 【意見】原文の「…審議を踏まえ検討を行う。」の次に、「その際、個人の権利・利益(プライバシー)に基づいた保護と利用のバランスを考慮し、現実的なリスクに応じた個人情報の保護とデータの利活用のための法改正を検討する。」の文を追記していただきたい。</p> | 御指摘の内容については、今後の消費者委員会における審議を踏まえ、今後の検討に当たっての参考とさせていただきます。 |
| 20 | 1 | 個人 | <p>【該当箇所】全般 【意見内容】文字パスワードには人間の記憶の特性から避けることのできない脆弱性があり、運用の厳格化だけでは解決することができない。国民が安全に安心して使える本人認証方法として、「文字に加え画像なども扱える拡張型パスワードシステム」を提言する。</p> | 御提言いただいたような新たな認証方法が提唱されているところ、現状では、セキュリティ強度やユーザビリティにおける課題が依然としてあるものと認識しています。今後ともよりよい本人認証方法について検討してまいります。 |
| 21 | 1 | | <p>【該当箇所】P.36「中小企業に対する情報セキュリティ対策支援」ア)中小企業における高度な情報セキュリティが確保された情報システムの普及 【意見】b)…業務効率化の修飾語として『経営改善のため』を追記し、『中小・小規模企業でも安価かつ容易に経営改善のための業務効率化が行える、…とする。』</p> | 御指摘を踏まえ、以下のとおり修正いたします。 「中小・小規模企業でも安価かつ容易に業務効率化及び経営改善を行える、～」 |
| 21 | 2 | | <p>【該当箇所】イ)中小企業における情報セキュリティ対策の推進(経済産業省) 【意見】「中小企業情報セキュリティ指導者育成セミナー」と「地域の中小企業等向けの情報セキュリティセミナー」の記述を次の通り、個別に記述するものとする。 a)地域の中小企業等向けの「情報セキュリティセミナー」を開催し、情報セキュリティに関する知識の向上を図ると共に、中小企業を指導する立場にある者等を対象とした、中小企業情報セキュリティ指導者育成セミナーを開催し、当該セミナーにおいて情報セキュリティに関する知識及び中小企業への指導方法を習得させ、適切な指導を実践させることにより、中小企業のセキュリティレベルの向上を図る。</p> | 「中小企業指導者育成セミナー」と「地域の中小企業等向けの情報セキュリティセミナー」が相まって中小企業の情報セキュリティレベルの向上を図ることを目的としていることから1つの文章にまとめて記載しております。よって、原文のままさせていただきます。 |
| 21 | 3 | | <p>【該当箇所】イ)中小企業における情報セキュリティ対策の推進(経済産業省) 【意見】b) 中小企業における…の「中小企業」の対象を具体的にするため、次の記述を加える。 『情報セキュリティ対策の推進が困難と感じている中小企業』における…</p> | 御指摘のとおり、修正いたします。 |
| 21 | 4 | | <p>【該当箇所】ウ)中小企業を対象とした情報セキュリティに係る相談窓口の対応と適切かつ確かな情報提供(経済産業省) 【意見】文章が箇条書きベースで段落により区分されている上記のア及びイと同様に、ウについても整理すればどうか？ ・『中小企業情報セキュリティ指導者育成セミナー』を受けた中小企業に指導する立場にある者等が…の部分等をa)とする。 ・また、…の部分等をb)とし、「また」を削除し、『IPAが…開発の検討を行う』とする。 ・『さらに…』の部分等をc)とする。「さらに」を削除し、Cの主導者？が…検討を行う。」とする。</p> | 御指摘のとおり、修正いたします。 |
| | | | | |

| | | | | |
|----|----|------------------|--|---|
| 21 | 5 | | <p>【該当箇所】全体 【意見】第2次基本計画においては、第1次基本計画が完全性を求めた事に対する反省として、「合理性に裏付けられたアプローチの実現」をめざしていたが、本文章の元となる「国民を守る情報セキュリティ戦略」では、 ・すべての国民が安心して利用できる環境を整備 ・世界最先端の「情報セキュリティ先進国」 ・すべての国民が不安を感じず、情報通信技術を利用できる環境を構築 など、再び、無謬性を求める方向に戻っているのではないかと危惧するところ。サイバーテロ対策とは言え、経済原則から逸脱出来ないと考えるところで、実効性・費用対効果を如何にして担保すべきかも含めて検討いただきたい。</p> | <p>「国民を守る情報セキュリティ戦略」では、「具体的な取組」のところで記述していますが、「事故前提社会」との認識の下、取組の持続的な改善を図ることとしており、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。</p> |
| 21 | 6 | 日本ネットワークセキュリティ協会 | <p>【該当箇所】P5「官民連携の推進」、P5「サイバーテロ対策に係る体制等の強化」、P28「サイバー攻撃停止に向けた枠組みの構築」 【意見】DDoSなど、現実発生しうる脅威についての対応としては、近々の課題であることからさらに踏み込んだ対応が望ましい。現実発生しうるサイバー攻撃として、「はじめに」にあるとおりDDoS攻撃が想定されている。DDoSへの対策は、警察の想定するサイバーテロではなく、ISPやAVV(アンチウイルスベンダ)等その他関連機関との迅速な情報共有および連携が必要不可欠であると考え。しかるに、その具体的な対策が「重要インフラ事業者等の理解と協力の促進に努める」(p5)、「2010年度までに総合的な枠組みを構築することを目標に、技術面及び対策面を含めた試行、検討を実施する。」(p28)では、今そこにある危機への対応としては遅きに失することを懸念する。既存の関連機関やすでにあるフレームの更なる活用と推進を図っていただきたい。</p> | <p>関連する取組の推進に際しては、関連機関との連携や既存の枠組みの活用を図ることが重要であると考えており、御指摘の内容については、今後の政策の推進に当たっての参考とさせていただきます。</p> |
| 21 | 7 | | <p>【該当箇所】P5、P6 【意見】政府機関における縦割りの施策についてのみならず、省庁連携の枠組みの強化を図って頂きたい。</p> | <p>御指摘の内容については、内閣官房において、行政各部の施策に関するその統一保持上必要な総合調整を行うことで、今後の政策運営に適切に反映して参ります。</p> |
| 21 | 8 | | <p>【該当箇所】P14「(サ) 政府機関のドメイン名であることが保証されるドメイン名の利用の推進」 【意見】「.go.jp」ドメイン取得/利用の基準を明確化した上で、利用組織の整理/統一を行い、内閣官房などのWebサイトに一覧を公表してはどうか。</p> | <p>「.go.jp」ドメイン名の登録基準については、当該ドメイン名を管理する株式会社日本レジストリサービスによって定められているところ、各府省庁への周知を行うなど、政府機関のドメイン名であることが保証されるドメイン名利用の推進の取組を実施しているところです。また、政府機関における電子証明書についても、GPKIの活用を推進するなど、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。</p> |
| 21 | 9 | | <p>【掲載箇所】P15「政府統一基準の見直しの実施」 【意見】政府統一基準に関しては、全体的に権限者、実施者等による分冊化をご検討いただきたい。</p> | <p>当センターでは、現在、政府機関統一基準の見直しを実施しているところであり、御指摘の内容については、その参考とさせていただきます。</p> |
| 21 | 10 | | <p>【掲載箇所】P15「政府統一基準の見直しの実施」 【意見】政府調達基準にST評価・ST確認を推進されているが、現実的にはST評価・ST確認について、政府機関の認証が少ないということは、政府機関に係わる部分については重要なセキュリティ要件があるシステムがないという誤解も生じかねない。したがって現実的な調達要件としてのさらなる充実、もしくは民間製品へのST評価・ST確認も視野にいれつつ調達要件も必要に応じて見直すべきではないか？</p> | <p>当センターでは、現在、政府機関統一基準の見直しを実施しているところであり、御指摘の内容については、その参考とさせていただきます。</p> |
| 21 | 11 | | <p>【掲載箇所】P17「政府機関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」 【意見】「(ア) 予算面での取組」について、各府省庁において適切に予算が組み込まれているかどうかを精査する取り組みを行って欲しい。</p> | <p>政府機関情報システムに情報セキュリティ対策が適切に組み込むための予算面での取組は全省庁にとって重要であると認識していることから、適宜、関係府省庁との調整を行ってまいります。</p> |
| 21 | 12 | | <p>【掲載箇所】P32「(ウ) DNSSEC導入の促進」 【意見】DNSSEC導入の促進が、「周知等の実施」ではなく「周知のさらなる推進」とすべき。さらには公的機関が優先的に導入し、問題点への対策の公表等を行うべきと考え。</p> | <p>我が国へのDNSSECの円滑な導入には、DNSSECジャパンが中心となって進めているDNSSEC導入・運用に関する課題の整理、技術検証等の活動等、DNSSEC導入に資する情報を適切に周知し、各主体における対応に反映させることが重要と考えます。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とさせていただきます。</p> |

| | | | | |
|----|----|-------------------------------|---|--|
| 21 | 13 | | <p>【掲載箇所】ア「情報セキュリティ安心窓口(仮称)」の検討 【意見】国民からみて、複数の窓口が乱立しないよう、整合をとり、有益なものとするべきと考える。次節イ)にあつとあり、既にIPAや、JPGET/CG等に窓口が設けられているところ。個人情報に関しては、国民生活センターなども存在することから、新たな窓口を検討するに際しては、利用者の混乱を招かぬよう真に国民にとって有益なものとなるように、国民が混乱することなく、既存の仕組みも含めて、前広に「在り方を検討」していただきたい。</p> | <p>「情報セキュリティ安心窓口(仮称)」が真に国民にとって有益なものとなるように検討を実施することが重要であるの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つての参考とさせていただきます。</p> |
| 22 | 1 | 特定非営利活動法人 日本セキュリティ監査協会 (JASA) | <p>【該当箇所】P10 2 ①・最高情報セキュリティ責任者(CISO)の機能強化 イ「情報セキュリティに係る年次報告書」(情報セキュリティ報告書)に係る取組の推進(内閣官房及び全府省庁) 【意見】 「a) (略) その際、情報セキュリティ報告書の客観性を確保する観点から、外部監査制度の活用についても、可能な限り推進する。」 とあるが、積極的に外部監査を利用するように指導していただきたい。情報セキュリティ報告書への信頼性を高めるためにも、外部監査を利用した部分とそうでない部分がかかるように明記するように指示願いたい。</p> | <p>御指摘のとおり、客観性を確保する観点から、外部監査制度を活用することは重要であると認識しており、既に統一基準において外部監査の活用を推奨しているところです。</p> |
| 22 | 2 | | <p>【該当箇所】P19 2(1)①・地方公共団体、独立行政法人等における情報セキュリティ対策の促進 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 【意見】「a) 地方公共団体における ICT 部門の業務継続計画の策定、情報セキュリティ監査の実施、(略) 内部監査アドバイザーの派遣を実施する。」とあるが、内部監査のみでなく外部監査も活用し、監査の実効性を高めるよう追加してほしい。また、内部監査及び外部監査の品質の確保のため、情報セキュリティ監査制度に基づく品質管理の徹底を行う必要がある旨の記述がほしい。</p> | <p>情報セキュリティ対策の実効性を担保するためには、内部監査に加え、外部監査を行うことも重要であると認識していますが、監査の実施は専門的であるため地方公共団体の実施状況は低調であるのが実態です。 従つて、まずは内部監査の実施を普及させることにより、情報セキュリティに対する意識を高めることが重要であると考慮しており、外部監査については、内部監査の実施の普及状況を踏まえ、普及方策を検討して参りたいと思います。 また、監査品質確保のための品質管理の徹底についてはご指摘のとおり重要な視点と考慮しており、今後総務省において監査品質確保の考え方について検討し、地方公共団体に示して参りたいと思います。</p> |
| 23 | 1 | 個人 | <p>【該当箇所】P7 ア) デジタルフォレンジックに係る取組の推進(警察庁)および イ) サイバー犯罪の取締りのための国際連携の推進(警察庁) 【意見】ISO/IEC NP 27037 Guidelines for identification, collection and/or acquisition and preservation of digital evidence の制定に対して我が国がどのようなコミットを行うかについて方向付けをするべき。</p> | <p>御指摘の内容については、今後の政策の推進に当たつての参考とさせていただきます。</p> |
| 23 | 2 | | <p>【該当箇所】P13 コ) 政府機関から発信する電子メールに係る成りすましの防止(内閣官房、総務省及び全府省庁) 【意見】SPF等のドメイン認証はなりすましに関して限られた効果しかない。GPKIの活用を含め、S/MIMEの本格的運用によって解決を目指すとともに、公的機関においては個人証明書の利用を率先して進めるべき。</p> | <p>御指摘のとおりであることから、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。</p> |
| 23 | 3 | | <p>【該当箇所】P18 ア) 社会保障・税に関わる番号制度及び国民ID 制度に対応した情報セキュリティ対策の検討(内閣官房及び関係府省庁) 【意見】国民IDのシステムデザインについて、開かれた議論が行われるよう期待。プライバシーコミッショナー制度についても、議論が開始されることを期待。</p> | <p>国民ID 制度については今後政府内での検討が進められる予定であるところ、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。</p> |
| 23 | 4 | | <p>【該当箇所】P33 ・クラウドコンピューティング化に対応した情報セキュリティ確保方策、標準化 【意見】クラウドコンピューティングに関して、国際的連携についての記述がないが、その方向性を示す時期ではないか。</p> | <p>クラウド・コンピューティングに係る情報セキュリティについての国際連携の推進については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つての参考とさせていただきます。</p> |
| 23 | 5 | | <p>【該当箇所】P40 ウ) 各種メディア等を通じた普及・啓発の推進(内閣官房、警察庁、総務省、経済産業省及び文部科学省) 【意見】初等中等教育での学習指導要領改訂に伴う情報モラル教育の充実に対し、教職員がそれに備えて情報モラル教育を行う能力を育成するための政策が欠けている。教職員に対する適切な内容の研修を行うことを明記するべき。</p> | <p>御指摘の内容に関しては、P41ウ)e)に記載されているe-ネットキャラバンにおいて、教職員等に対し、児童生徒への情報モラル教育に関する内容も実施しています。</p> |
| 23 | 6 | | <p>【該当箇所】P46ページ ア) サイバー犯罪の取締りのための態勢の強化(警察庁) 【意見】いわゆるサイバー犯罪だけではなく、ネットワークを利用した犯罪全般に対し、これまでのサイバー社会が保つてきた秩序に大きなひずみを生じさせないような形で法運用のためには「サイバー犯罪捜査に従事する全国の警察職員に対する部内外の研修を積極的に実施する」だけではなく、広義のネットワーク利用犯罪捜査に従事する可能性のある全ての警察職員に対し、一定の研修が必要となるのではないかと。</p> | <p>警察庁では、ネットワークを利用した犯罪も「サイバー犯罪」と定義し、すべての警察職員に対して、サイバー犯罪の基礎的な教育を実施しております。 また、サイバー犯罪捜査に従事する警察職員へは、より知識を高めるための高度な内容の教育を実施しております。 情報通信技術は日進月歩の世界であり、我々としても日々新しい技術を利用した犯罪に対応できるよう、今後とも継続的な教育・研修を実施してまいりたいと考えております。</p> |

| | | | | |
|----|---|----|---|---|
| 23 | 7 | | <p>【該当箇所】P47 イ) 情報セキュリティに関する講習の実施(警察庁) 【意見】既にいくつかの都道府県で行われているとおり、この講習の実施に関してNPO協業事業等の活用をさらに進め、啓発活動に関する官民連携を深めるべき。</p> | 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。 |
| 23 | 8 | | <p>【該当箇所】P59 エ) 先導的IT スペシャリスト育成推進プログラム(文部科学省) 【意見】本案では同プログラムに基づく人材育成拠点の形成支援がうたわれる一方、先日の事業仕分けにおいて本プログラムに対する予算が打ち切られるなど、行政の対応が矛盾している印象がある。高度セキュリティ人材育成はIT先進国となることを掲げる我が国における政策の根幹であって、より強力に推し進められるべき性質のものなのではないか</p> | 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。 |
| 24 | 1 | 個人 | <p>【該当箇所】全般 【意見】以下の用語の定義と注意を追加することを提案する。 「コンピューティングの形式としてのクラウドと、利用者から見えるインターネット経由の情報サービスを指すクラウドとは違いがあり、前者により期待されるメリットが後者では得られないことがある。この定義は別記する。国民・利用者はこの点に注意する必要がある。」</p> | 御指摘を踏まえ、以下のとおり修正いたします。 ※「新たな情報通信技術戦略」の用語集より、「クラウド」の注記として、次の説明を追加します。 データサービスやインターネット技術などがネットワーク上にあるサーバー群(クラウド(雲))にあり、ユーザーは今までのように自分のコンピュータでデータを加工・保存することなく、「どこからでも、必要な時に、必要な機能だけ」を利用することができる新しいコンピュータネットワークの利用形態。 |
| 24 | 2 | | <p>【該当箇所】2(1)③ その他の基盤強化 【意見】「ウ) クラウド・サービス・レベルのチェックリストの策定(経済産業省)」に「安全・安心なコンピューティングリソースの提供」が得られるような水準の保証基準を明確にする。また、どのようなリスクが想定し得るか、例示を併記する。これを以って、セキュリティ基準として参照されるようにする」を追加することを提案する。</p> | クラウド・サービス・レベルのチェックリストは、クラウド・サービスを推進するに当たって責任主体を明確化し、サービスの信頼性を可視化するために整備するものであり、御指摘のセキュリティ基準とは基本的に性格が異なるため、原文のままさせていただきます。なお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。 |
| 24 | 3 | | <p>【該当箇所】2(2)② 情報セキュリティ安心窓口の検討 【意見】ア) 情報セキュリティ安心窓口の検討(内閣官房および関係府省庁)の「国民・利用者からの情報セキュリティに関する相談を受け付けるため、」を「国民・利用者からの海外事業者のサービス利用を含めた情報セキュリティに関する相談を受け付けるため、」に変えることを提案する。</p> | 「情報セキュリティに関する相談」には「海外事業者のサービス利用」に関する内容も当然含まれており、これを特記することは必須ではないと考えられるため、原文のままさせていただきます。 |
| 24 | 4 | | <p>【該当箇所】2(2)① 普及・啓発活動の充実・強化 【意見】ウ) 各種メディア等を通じた普及・啓発の推進に、以下の文言を追加することを提案する。 「モデル取引・契約書など、今回の案に沿った内容への見直しも行き、普及・啓発活動の促進も図る」</p> | モデル取引・契約書につきましては、③情報セキュリティガバナンスの確立 に、普及・啓発を推進する旨の記述がありますので、当該箇所は原文のままさせていただきます。 |
| 24 | 5 | | <p>【該当箇所】2(2)③ 個人情報保護の推進、2(4)① 情報セキュリティ関連の研究開発の戦略的推進等 セキアでグリーンなクラウドコンピューティング環境の整備(経済産業省) 【意見】クラウドコンピューティング・セキュリティに関する監査の枠組み及び基準案を策定を2010年度に行うとしているが、喫緊の課題であり、できるだけ早期の取組みが必要である。</p> | 御指摘の内容については、喫緊の課題であると考えるところ、今年度(2010年度)においても、早い段階で取組を行う予定をしております。 |
| 25 | 1 | | 個人 | <p>【該当箇所】 ①P.40 内閣官房情報セキュリティセンターの機能強化 ②P55ページ 情報セキュリティ関連の研究開発の戦略的推進等 ③P59ページ 情報セキュリティ人材の育成について 【意見】産官学の連携のため、若手研究者、若手技術者、若手官僚の人材交流のスキームを提案する。</p> |