「情報セキュリティ2011」(案)に対する意見募集の結果の概要

経　　緯

第23回「情報セキュリティ政策会議」（2010年５月11日）

■「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2011」（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：2011年6月9日(木)～6月22日(水)
■ コメント総数：**42件**【内訳：12企業・団体から延べ33件、2個人から延べ9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。
■ 主なコメント例

・ 最新の情報通信技術を適切に社会で活用していくためには、省庁間の連携、官民の連携、そして国際的な連携が重要である。
・ スマートフォンのセキュリティを確保するために、利用者に対して正しい知識を広めるとともに、業界を横断する関係者で対策を推進する必要がある。
・ 災害時の可用性を確保するためには、物理セキュリティ、情報漏えい対策、本人認証基盤など構築する必要がある。

コメントへの対応

■ 御意見を踏まえ、「セプター」に係る説明をより明確化するなど、表現を一部修正。
■ コメントを関係省庁と共有し、今後の政策の推進にあたっての参考とするなど、適切に活用。

資料１－２

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	オプテックス 株式会社	P.10、Ⅲ③ P.70、Ⅴ(1)(ア)	情報セキュリティの「可用性」確保のため、国内に分散化が加速するデータセンターやデータバックアップにおける、物理セキュリティと情報漏えい対策が必要である。	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。
	2		P.70、Ⅴ(1)(ア)	政府機関を始めとする重要施設においては、建物の中に入る前の外周警戒、建物に入った後の入退室管理、共連れ対策が必要である。	御指摘の施設と環境に係る対策については、「政府機関の情報セキュリティ対策のための統一技術基準」（平成23年4月21日情報セキュリティ政策会議決定）において遵守事項として記載されています。
2	1	電子的本人認証の検討会	P.70、Ⅴ	災害時に可用性を保持できる本人認証基盤を構築しておくことが必要である。自伝的記憶に基づく画像活用方式による汎国民的な本人認証基盤構築に向けた研究開発を加速させることを進言する。	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。
3	1	札幌市医師会 北区支部	全般	政府は、情報ネットワーク構築の安全性を更に高める努力をし、その工程を定期的に国民に公表する。	御指摘の内容については、今後の施策の施策の当たっての参考とさせていただきます。
	2		全般	政府は、情報ネットワークで発生した有害事象を速やかに公表し、その原因究明と対策を公開する。	御指摘の内容については、今後の施策の施策の当たっての参考とさせていただきます。
	3		全般	政府は、同ネットワーク利用により発生した有害事象への損害賠償義務を負う。また、補償等に関し具体的に広く国民に情報提供をする。	情報ネットワークは政府が自ら管理するものではなく、同ネットワーク上で発生する有害事象に対して政府が損害賠償義務を負う性格のものではないと考えております。
	4		全般	広域な情報ネットワークの一部に障害が発生した際、その障害が国全域に及ぶことがないような設計や、速やかに復旧できる施策を作成する。	御指摘の内容については、今後の施策の施策の当たっての参考とさせていただきます。
	5		全般	政府は今後とも、情報ネットワーク存続の是非を定期的に国民に問う。	情報ネットワークは政府が自ら管理するものではなく、その存続の是非を検討する性格のものではないと考えております。
	6		全般	政府は、同ネットワークの安全性対策等を検証する為に、政府とは独立した専門機関の審査を定期的に受け入れる。	情報ネットワークは自ら政府が管理するものではなく、その審査の具体的方法について言及する必要はないと考えております。
4	1	日本ユニシス 株式会社	P11.Ⅲ③	基本方針では「③東日本大震災を踏まえた情報セキュリティ分野における対応」が挙げられているが、さらに安全保障上の観点から「④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」を追加すべきと考える。	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。
	2		P32.Ⅳ2(1)②ウ	現在省庁毎に別個に存在するセキュリティ基準やガイドラインの共通基礎部分を統合化し、これを土台として必要に応じて業界毎に存在する個別要件を追加したような汎用性に富む『国内で統一されたセキュリティ基準・ガイドラインの策定』を本節(イ)として追加すべきと考える。	御指摘に内容については、「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」の策定に当たっての指針」及びこれを基に策定された「安全基準等」として実現されていると考えます。
	3		P.35、Ⅳ2(1)②カ(ア)	「･･･実態調査し、情報システムの安定運用の視点で･･･」のくだりを以下のように修正してはいかがか。 「･･･実態調査し、さらに物理的テロ攻撃をも想定し、情報システムの安定運用の視点で･･･」	当該部分は、震災の影響への対策を記述した部分であり、情報システム関連設備の物理的脅威も踏まえて実施される施策であることから、原案のとおりの記載とさせていただきます。
	4		P.39、Ⅳ2(1)④ア	スマートフォンを利用したシステム全体のセキュリティ維持方法については混沌としており、未だ統一的な見解がないので、この対応として『日本スマートフォンセキュリティフォーラムなどと連携し、早期にスマートフォン情報セキュリティ基盤の実現を目指す』を本節（イ）として追加してはいかがか。	御指摘の内容については、施策の推進に当たっての参考とさせていただきます。
	5		P.50～53、Ⅳ2(2)	「国民」という用語が複数個所出現するが、この「国民」が国内在住の外国人を含むのか否かが不明確あり、「国民」の定義を明定していただきたい。	日本国憲法上の「国民」を想定しており、改めて定義する必要はないと考えております。
	6		P.51、Ⅳ2(2)①(オ)	各種メディア等の1つとして「日本スマートフォンセキュリティフォーラム」を追加してはいかがか？	当該部分は、政府機関等による主な取組を例示しています。なお、施策の推進に際しては、関係機関等との連携を図ることとしています。

5	1	データベース・ セキュリティ・ コンソーシアム	全般	ICTの根幹を支えるデータベースに係る方向性が必要である。	御指摘の内容については、施策の推進に当たっての参考とさせていただきます。
6	1	個人	全般	情報セキュリティ技術に偏っているが、情報セキュリティは総合科学として対応する必要がある。	本文書は、情報セキュリティ政策について、技術面のみならず、全般的に記述しているものと考えております。
	2		P.14、Ⅳ1(1)エ(ア)	デジタルフォレンジックに関しては、体制の強化だけでは問題が解決せず、記憶装置の大容量化への対応、ISP等に設置してある記憶装置の押収、法改正を考える必要がある。	御指摘の内容については、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、第177回通常国会において、「情報処理の高度化等に対処するための刑法等の一部を改正する法律」により、刑事訴訟法の一部が改正され、電磁的記録に係る記録媒体の差押えの執行方法等に関する規定が整備されました。
	3		P.25、Ⅳ2(1)①カ(オ)	「ITセキュリティ評価及び認証制度」製品を取り扱うとのことだが、UNIXやWindowsでこの認証を取得しているものを考える必要がある。	「IT セキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」（平成23年4月21日経済産業省）においては、サーバOSがその対象製品分野となっております。
	4		P.34、Ⅳ2(1)②オ(ア)及び(イ)	2002年頃に、米国ではSCADA等の制御システムの脆弱性の調査・研究を行っており、それらを含めて日米を含め、関係国を巻き込んで検討・対応をすることが大切ではないか。	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。
	5		P.37、Ⅳ2(1)③	情報セキュリティ産業が国内には殆どないとの認識を持つべきではないのか？	国内の情報セキュリティ産業については、その振興を図ることが重要であると考えております。
	6		P.62　Ⅳ2(4)	情報セキュリティは、ここで述べている技術戦略だけでは対応できない。	御指摘については、今後の施策の検討の際の参考とさせていただきます。
	8		P.31、Ⅳ2(1)②ア(ウ)	「セプター」(Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略。情報共有・分析機能である)としているが適切な訳か？	当該部分は、和訳ではなく、セプターの機能を簡記したものです。 ご指摘を踏まえ、修正しました。
7	1	個人	P.38、Ⅳ2(1)③(キ)	「再掲2（1）④エ」 は対応していないのではないか。	御指摘を踏まえ、修正しました。
	2		P.67、Ⅳ2(4)③(イ)c)	「・・・情報セキュリティ報告書モデルの普及を図る。・・・情報セキュリティ報告書の普及に努める」とあるが、その前に、現在の情報セキュリティ報告書モデルを改訂する必要がある。	御指摘頂いた御意見につきまして、情報セキュリティ報告書モデルは、1つの参考モデルであり、情報セキュリティ報告書として対外的に開示するために、モデルの中で記載した情報セキュリティマネジメント体制（情報セキュリティガバナンス）が報告されていれば良いと認識しており、改訂する必要性はないと考えています。
8	1	ネットワンシステムズ（株）	P.14、Ⅳ1(1)ウ	サイバー攻撃の技術に対する調査研究はあるものの、テロ組織および仮想敵国となる組織(以下 敵組織と呼ぶ)に対する調査研究がない。 この為、技術優先の戦略が先行して危機が訪れたとき、有事の際に危機を乗り越えるためには、技術的な戦略のみで事足りるのか、という印象を読者に与えることから、下記の項目を追加すべきであると考える。 （追加案） (カ)サイバー攻撃の攻撃者となり得る組織動向の調査研究 （防衛省） サイバー攻撃に係わる攻撃者が属する、ハッカーグループ、テロ組織・仮想敵国等の調査研究を実施する。	御指摘の部分は、23年度予算に計上した民間への委託研究事業を指していますが、ご指摘の内容の調査研究を民間に委託することはなじまないと考えています。また、サイバー攻撃事態への対処に資する情報の収集・分析・共有体制の強化については、Ⅳ1（2）アにおいて記述しています。

9	9	株式会社ラック	P.6、Ⅱ④	ジャスミン革命などの指摘内容はもっともなことと考える。このような事象の背景にはグローバル化だけではなく、これまでICTが先進国の限られた人々の利用に限られたのが、ピラミッドの中間から底辺に向けての利用推進も同様に大きなインパクトをもたらすものと考える。この課題へも、日本のリーダシップの有りようも合わせてご検討をお願いしたい。	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。
	1		P.8、Ⅲ②	事故検証、反省、教訓などの共有化が重要とあるが、まったくその通りである。その為には、セキュリティインシデント＝不祥事ではないことを徹底する。開示すべきことを開示しない、運用時或いはインシデント発生時に実施すべきことが適切に実施できないことが不祥事である。	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。
	1		P.8、Ⅲ②	閉鎖環境が前提でセキュリティ対策を為されている重要システムへの運用実態の把握と再評価が急務である。	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。
	1		P.10、Ⅲ③	大災害発生時の情報セキュリティ関連法律の運用の特例に関して考えておく必要がある。	御指摘の内容については、必要に応じ、Vに記載された施策の推進の際の参考とさせていただきます。
	2		全般	政治主導で進める必要がある。	本文書は、官房長官を議長とし、関係閣僚が参加する情報セキュリティ政策会議により決定されます。
	3		P.12、Ⅳ1	訓練は、当該組織が主体的にやるだけではなく、監査などのように当該組織から独立したところで実施し実効性を上げて頂きたい。	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。
	1		P.12、Ⅳ1	国において重要インフラ分野や該当企業を指定する手順を明確にして置いて頂きたい。	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。
	2		P.49、Ⅳ2（1）⑤	大賛成である。その為に必須なのは、政治主導である。バランスと意思を持ったかたに専任して引きいて頂きたい。	本文書は、官房長官を議長とし、関係閣僚が参加する情報セキュリティ政策会議により決定されます。
10	1	日本スマートフォンセキュリティフォーラム	P.4、Ⅱ	記載されている通り、スマートフォンはパソコンと同じであるという認識が重要であるが、一般的には高機能携帯電話と呼称されることもあって、誤解を生じさせ、事業関係者においても適切な普及が阻害させる危険性もはらんでいると考える。 重要なことは、まずは利用者に対して正しい知識を広めることであると考える。それが、今後の高度情報社会を安全に形成し最大限に活用して行くために重要なことと考える。 出回り始めているウイルスに関してもパソコンとは異なり、持ち主個人を標的にすることも考えられ、これまでのパソコンでのセキュリティ対策と同様にウイルス対策を行っておけば良いという、考え方は通用しないと考える。 その為、業界を横断する関係者で推進する必要があると考える。	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。
11	1	インテル株式会社	P.7、Ⅲ①	安全なサイバー空間を構築するための情報せキィリティ技術の重要性は年々増加し、最新の技術をいかに適切に社会で活用していくかが鍵となる。そのためには、官民の連携、そして国際的な連携が重要となり、その中でも技術革新と商品やサービスの提供を行う民間企業の役割が重要であると考える。官民、そして国際連携を柔軟に行い、その結果を社会で利活用していくための迅速な施策の適用が重要と考える。	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。
	2		P.7、Ⅲ①	当該箇所において記述されるオープンな環境を活用しつつセキュアな環境を実現するための国際連携の重要性に同意する。	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。
	3		P.25、Ⅳ2(1)①カ(オ)	せキィリティ機器の民生品市場における信頼を確立するための枠組みは重要と考える。そのために利用される認証制度については、民生品市場の商習慣、技術の進歩のスピード、機器のライフサイクルなどを考慮し市場が利用可能となるよう、過大なオーバーヘッドがかからないものが望ましい。	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。
	4		全般	パブリックコメントの募集期間は30日に、そして可能であれば英語での文書も提供していただきたい。	御指摘の内容については、今後の情報セキュリティ政策の検討の際に参考とさせていただきます。

12	1	一般社団法人 ITセキュリティセンター	P.24、Ⅳ2(1) ①エ(イ)	原文を改案のように改良する。 【原文】安全性の高い暗号モジュールの活用を推進するため、引き続き、IPA の運用する暗号モジュール試験及び認証制度を推進するとともに、暗号モジュールを調達する際には、必要に応じて同制度により認証された製品等を優先的に取り扱う。 【改案】安全性の高い暗号モジュールの活用を推進するため、引き続き、IPA の運用する暗号モジュール試験及び認証制度を推進するとともに、暗号モジュールを調達する際には、同制度により認証された製品等を優先的に取り扱う。 （原案の下線部削除）	御指摘の暗号モジュール試験及び認証制度については、同制度により認証された製品数がまだ少なく、特定の機関で既に実施している同等以上の独自対策を排除することになることから、原文のとおりとします。
13	1	株式会社 ニーモニック セキュリティ	P.70、Ⅴ	大災害時を想定した本人認証システムを準備しておくことが望ましいと考える。	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。
14	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	Ⅱ　情報セキュリティを取り巻く環境の変化	記載されているとおり、情報セキュリティは、国際連携と省庁をまたいだ対応が求められている。それは、先進国としてのリーダシップを発揮しこれからの社会における日本自身のプレゼンスを確保する意味でも極めて重要である。震災復興や原発への対応も重要であるが、この時期この分野こそ政治主導を発揮いただきたい。具体的には実際に担当する政治家がリーダーシップを発揮し、官庁を取りまとめ、バランス良く実施を頂きたい。	本文書は、官房長官を議長とし、関係閣僚が参加する情報セキュリティ政策会議により決定されます。