「サイバーセキュリティ2013（案）」に対する意見募集の結果の概要　資料1-3

■ 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：　2013年6月10日（月）～6月24日（月）

■ 意見総数：　69件　【内訳：8法人・団体から延べ59件、8個人等から延べ10件】

（1）賛同意見　全8件

（2）修正意見　全17件

- 全体の構成等に修正を求める意見はなし。
- 「サイバーセキュリティ戦略」（以下「戦略」。）における記載との整合性の確保や表現の明確化等を求めるものについては、必要に応じて趣旨を踏まえて修正（全4件）。戦略で言及している等修正不要の意見については、その旨理由を付して採用しない旨回答（全13件）。

（3）政策展開に係る意見　全44件

- 今後の政策展開に係る意見については、今後の検討又は今後の施策の推進において参考にする旨回答（全44件）

注）提出された意見は必ずしも明確にこれらに分類されるものではないが、事務局で理解した区分にて計上している。

■ 主な意見：

（1）賛同意見

- システムの企画・設計の段階から情報セキュリティ対策を組み込む「セキュア・バイ・デザイン」の考え方が非常に大事であると考えます。（p7（タ））
- 不正アクセス、不正プログラムは我が国においても急速に拡大し、かつ巧妙化しています。これらを検出するためのアプリケーションや仕組み、セキュリティ機材の整備は急務であると考えます。（p48（イ））
- 新種のサイバー攻撃、ゼロディ・アタック等を考慮した場合、情報流出を防止するための技術は非常に重要です。（p57（ウ））

（2）修正意見

- 「サイバーセキュリティ戦略」のパブリックコメントで追加された最も優先度の高い「今までの取組とは異なる新しい対応」としての「脆弱性への対処」の文言を追加されたい。（p3、7行目、下記のとおり修正）

> サイバー空間の持続性を確保するため、サイバー攻撃への対応を増強するとともに、脆弱性への対処、サイバー攻撃に関するインシデントの認知・解析やインシデント等関連情報の共有等の機能を高めること等により・・・

- 公的機関における調達に際して、サイバーセキュリティ分野においては技術評価を特に重視することが可能な評価の仕組みを取り入れることを提案する。（p9、下記のとおり追記）

> （テ）政府調達の在り方 （内閣官房）
>
> 内閣官房において、新興企業を含む我が国サイバーセキュリティ産業の能力の活用等を通じて、サイバーセキュリティの確保に実質的に有効な製品、システム等の調達を図るべく、応札事業者の技術力評価の在り方など政府による調達の在り方について検討を行い、結論を得る。

（3）政策展開に係る意見

- 国の安全に関する重要な情報について、収集及び高度な解析を実施することは非常に重要です。また、その収集情報や解析情報及び結果・対策等を関係する事業者等へ共有し、事業者の対策に活用することも非常に重要と考えます。（p21（ア）・（ウ））

- 分野横断的演習ならびに個別分野におけるサイバー演習の対象として、大規模データセンターを取り上げることを提言する。クラウドサービスやデータセンターサービスが社会経済の随所で利用され、それらを提供するデータセンターやその機能は社会インフラとなっている。（p24（ス）・（セ））

- 営業秘密保護は特に日本企業の海外進出先における情報漏えい・流出リスクが深刻化している現状があり、その点に対する対策も検討対象とするよう提言する。（p31（オ））

- 啓発の一丁目一番地は「一般利用者等に当事者であることを気づいてもらうこと」である。一般利用者、家族、先生・教師、会社員、組織の長等毎に、無関係な人は存在しないことを出発点として、しっかり国民に伝えるべきである。（p35）

- 民間企業が外国政府等の関与が疑われる国家レベルのサイバー攻撃を受けた場合に、自衛隊のサイバー防衛隊はどこまでの責任範囲で対処できるのか、またその際の警察庁等の他の府省庁との連携や責任範囲は曖昧なままである。（p53）

- 情報セキュリティ産業自体の活性化と能力向上を支援するために、1）研究開発支援施策の実施、2）ベンチャー企業育成・支援施策の重点的適用、3）需要喚起策としての情報セキュリティ投資減税等の実施、4）公的調達における国家安全保障の視点からの調達選抜の仕組みの導入、5）海外進出支援、等の施策が実施されることを期待する。（p54）

- 米国、EU、韓国及びASEAN地域等との政府レベルでの連携が本取り組みにて強化されており、高く評価できる施策である。一方で当該地域に進出する民間企業においては、現地におけるセキュリティ情報を収集する経路が限られている。（p69・72）

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
1	1	法人・団体 （一般社団法人ITセキュリティセンター）	5	（ケ）複合機等のセキュリティ対策の強化（内閣官房及び全府省庁） （原文） 内閣官房において、関係府省庁と協力し、ネットワーク機能をもつ複合機等に求められる情報セキュリティ対策について検討を行い、各府省庁で保有している複合機の情報セキュリティ機能の検査を実施する。 （修正案） ・・・各府省庁で保有している複合機の情報セキュリティ機能についてISO/IEC15408に従った適合性評価を実施する。 （理由） 「複合機の情報セキュリティ機能を検査する」とあるが、検査方法が明確ではない。具体的な適合性評価方法を記述すべきである。	ご指摘の「複合機の情報セキュリティ機能の検査」につきましては、ISO/IEC15408に従った適合性評価のほかにも複合機に求められる情報セキュリティ機能の検査を行うことを検討しており、原案のとおりとさせていただきます。
1	2	法人・団体 （一般社団法人ITセキュリティセンター）	8	(ツ) 政府調達における情報セキュリティの確保（内閣官房及び経済産業省） （原文） b) 経済産業省において、独立行政法人情報処理推進機構（IPA）を通じ、経済産業省に対する「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」の適切な製品分野の検討協力及び最新のプロテクション・プロファイル（PP）等の情報提供を行う。 （修正案） b) 経済産業省において、独立行政法人情報処理推進機構（IPA）を通じ、「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」の適切な製品分野の検討及び最新のプロテクション・プロファイル（PP）等の情報提供を行う。 （理由） 1行目後半にある「経済産業省に対する」及び3行目の「検討協力」が本文の実施主体を不明確にしている。この「経済産業省に対する」と「協力」を削除する。	ご指摘を踏まえ、修正させていただきます。
1	3	法人・団体 （一般社団法人ITセキュリティセンター）	8	(ツ) 政府調達における情報セキュリティの確保（内閣官房及び経済産業省） （原文） c) 経済産業省において、独立行政法人情報処理推進機構（IPA）を通じ、・・・統一管理基準への活用の検討を行い、結論を得る。 （修正案） c) 経済産業省において、独立行政法人情報処理推進機構（IPA）を通じ、・・・統一管理基準の適用を促進する。 （理由） 統一管理基準では、本制度での認証取得製品を調達することが既に明確に規定されているため、「活用の検討を行い、結論を得る」のではなく「適用を促進する」として実績を上げることに主眼を置くべきである。	現段階では、統一管理基準の適用を促進するための準備を行っているため、記載については原案のとおりとさせていただきます。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にさせていただきます。
1	4	法人・団体 （一般社団法人ITセキュリティセンター）	8	(ツ) 政府調達における情報セキュリティの確保（内閣官房及び経済産業省） （原文） d) 内閣官房及び経済産業省において、・・・国際規格に基づく適合性評価の活用については、検討の上、結論を得るべく取り組む。 （修正案） d) 内閣官房及び経済産業省において、・・・国際規格に基づく適合性評価の活用を促進する。 （理由） 統一管理基準では、ISO/IEC15408に従った適合性評価を行うことが既に明確に規定されているため、「適合性評価の活用については、検討の上、結論を得る」のではなく「活用を促進する」として実績を上げることに主眼を置くべきである。	今後、業務で扱う情報の機密性の要求度等に応じた対策の重点実施のための枠組みを構築するため、政府機関統一基準群の見直しを行い、その中において、より効果的な適合性評価の活用について検討を行うこととしており、記載については原案のとおりとさせていただきます。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にさせていただきます。
1	5	法人・団体 （一般社団法人ITセキュリティセンター）	10	（ニ）安全性・信頼性の高い暗号モジュールの利活用推進（内閣官房、経済産業省及び全府省庁） （原文） b) 各府省庁において、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取り扱う。 （修正案） b) 統一管理基準に「暗号モジュール試験及び認証制度」の利用を明記し、各府省庁において、暗号モジュールを調達する際には、統一管理基準に従って認証された製品等を取り扱う。 （理由） 暗号機能は、最近のほとんどのIT製品に搭載されており、IT製品のセキュリティ機能の重要なコンポーネントであるが、「ITセキュリティ評価及び認証制度」だけを適用しても暗号機能部分の認証は行われないため、統一管理基準において「暗号モジュール試験及び認証制度」も「ITセキュリティ評価及び認証制度」と同等に扱うべきである。	ご指摘の「暗号モジュール試験及び認証制度」の統一管理基準への利用明記につきましては、今年度統一基準の見直しを検討しています。ご指摘の内容については、今後の施策の検討にあたっての参考にさせていただきます。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
1	6	法人・団体 （一般社団法人ITセキュリティセンター）	10	（ニ）安全性・信頼性の高い暗号モジュールの利活用推進（内閣官房、経済産業省及び全府省庁） 下記項目を追加。 C）経済産業省において、独立行政法人情報処理推進機構（IPA）を通じ、「暗号モジュール試験及び認証制度（JCMVP）」を適用する製品分野の検討及び情報提供を行う。 （理由）「ITセキュリティ評価及び認証制度」と同様に「暗号モジュール試験及び認証制度（JCMVP）」を適用する製品分野を明確化して統一管理基準の適用を促進すべきである。	ご指摘の「暗号モジュール試験及び認証制度（JCMVP）」を適用する製品分野の検討及び情報提供を行うことに関し、記載については原案のとおりとさせていただきます。ご指摘の内容については、（ニ）a)に記載のある、独立行政法人情報処理推進機構（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中で、進めさせていただきます。
1	7	法人・団体 （一般社団法人ITセキュリティセンター）	32	（シ）情報システム調達時等における情報セキュリティの確保の支援（経済産業省） 上記項目は【情報セキュリティガバナンスの確立】のタイトルに相応しくない内容が含まれているため、別の場所に移すべきである。 B）NISTとの共同認証 C）製品毎のプロテクション・プロファイルの整備 （理由） b）NISTとの共同認証は暗号制度において重要事項であるが、ガバナンスとは直接関係を持たない。 C）製品毎のプロテクション・プロファイルの作成は日本の産業界において重要事項であるが、ガバナンスに直接結びつくわけではない。	各々ガバナンスに直接結びつくものではありませんが、「情報システム調達時等における情報セキュリティの確保の支援」に該当する施策であり、原案のとおりとさせていただきます。
1	8	法人・団体 （一般社団法人ITセキュリティセンター）	76	（ソ）Common Criteria (ISO/IEC15408)における国際協調（経済産業省） （コメント） 現在CCRA配下での評価認証制度が大きく変わろうとしています。特に国際共通プロテクション・プロファイルの開発及び情報収集は日本のIT業界の振興に重要な意味を持つため、推進を宜しくお願い致します。	ご指摘の内容については、今後の施策の推進にあたっての参考とさせていただきます。
2	1	法人・団体 （イー・アクセス㈱）	50	⑤ サイバー空間の犯罪対策 P.50【事後追跡可能性の確保】 （サ）ログの保存の在り方（警察庁及び総務省） サイバー攻撃に対する対策を強化、促進することは、近年のサイバー空間を取り巻くリスクの深刻化が加速している状況を踏まえ、大変重要なことであることは認識しています。 一方で、「通信履歴等に関するログの保存の在り方について」の方策を検討するにあたっては、法制度の整理及び通信事業者における負担、個人情報保護の観点等、課題が多岐にわたるため、「可能な範囲で速やかに一定の結論を得る」としても、関係事業者等の個々の状況や利用者への影響及び意見も踏まえた上で十分に慎重な議論を行ってバランスの取れた結論を得ていただきたいと考えます。 事後追跡可能性を確保するためには、通信履歴から個人を特定する必要があるため、利用者の保護がどのように確保されるかが大きな課題になるため。 加えて、ログの保存期間、保存する対象範囲等の規模が大きくなればなる程、通信事業者の設備や運用に多大な費用等負担が新たに発生し事業を圧迫する可能性があるため。	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。
3	1	法人・団体 （国際公共政策研究センター）	全体	最終版完成後、その英語版および一般が使えるスライドを作成しそのファイルを公表頂きたい。 国際連携推進のためには、他国に日本の情勢、基本的な考え方、政府の体制などを周知することも重要であり、英語版の公表はそのために必須である。また一般が使えるスライドを公表することにより、民間の関係者が海外に行った際の日本の活動の紹介において一助となる。	ご指摘の英語版等の作成については、必要な範囲で作成し、公表する予定です。
3	2	法人・団体 （国際公共政策研究センター）	3	″（ア）業務で扱う情報の機密性の要求度等に応じた対策の重点実施のための枠組みの構築″ NISC に、他省庁のサイバーセキュリティに関する予算や人員配置の権限を集中させるべきである。 国家的なサイバーセキュリティ対策の効率的な実現のためには、その予算や人員配置の権限を一つの組織に集中させることが必要である。縦割り組織的な対応では整合性の取れたサイバーセキュリティ政策を実現することはできない。また、NISCに権限を集中させることにより、予算の重複使用が防止できる。	NISCは2015年度を目途にサイバーセキュリティセンター（仮称）への改組を計画しているところです。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。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
3	3	法人・団体（国際公共政策研究センター）	5	″(カ) 政府機関におけるスマートフォン等の情報セキュリティ対策の強化（内閣官房)″ スマートフォン等のデバイスについては政府機関統一で適切に管理する技術的な仕組みを導入するべき。 スマートデバイスのセキュリティ対策では、手順書を作成や基準を見直しだけでは不十分。個人任せではセキュリティ事故が発生したことにも気づかないケースも想定される。MDM (Mobile Device Management) や SIEM (Security Information and Event management) 等の仕組みにより、実効的なサービスや仕組みを導入して、利用者に意識させずに自動で一定レベルのセキュリティが確保されるようにするべきである。	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。
3	4	法人・団体（国際公共政策研究センター）	18	″（チ）優秀な外部人材の活用″ 優秀な外部人材の確保のため、国家公務員の報酬体系を超えた報酬制度を検討していくことについても言及すべきである。 本当に必要とされる優秀な人材を確保するためには、現行の国家公務員の報酬体系では不十分である。	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。
3	5	法人・団体（国際公共政策研究センター）	24	″(シ) 情報通信分野における事業者との官民連携の推進 (総務省)″ 「情報通信分野：通信」セプターとの関係を明確にすべきである。 すでに Telecom-ISAC Japan の会長が「情報通信分野：通信」セプターの代表者ではあるが、その両者が情報連携を進めるのか、またそうであればどのように進めていくかが明確ではない。	総務省では、電気通信事業の所管省庁として、事業者間における情報共有を目的とするセプターのみならず、情報セキュリティ対策の実施主体であるISPの事業者団体と連携し、対策を推進していくことが重要であると考えていることから、原案のとおりとさせていただきます。
3	6	法人・団体（国際公共政策研究センター）	40, 41	″(ト) コンピュータセキュリティ早期警戒体制の強化 (経済産業省)″ ″(ニ) サイバー攻撃事前防止・早期対策に向けた取組の推進 (総務省)″ この二つの取組の間の関係、特に協力関係について明確にすべきである。 両者とも早期にサイバー攻撃などを認知するための取組と理解する。その両者間に密接かつ迅速な協力関係があれば、それぞれ単独よりもより早く正確な攻撃の認知が可能になる。	前者は、実際に発生したインシデントや攻撃手法、ソフトウエア等について発見された脆弱性等の情報を、グローバルなCSIRT間連携や国内の関係者との協力を通じて、中立的な立場で、具体的な対策をとることができる主体に提供し、現に発生している問題への対処につなげることを主な目的としています。後者はグローバルに収集した詳細な通信情報に基づく研究開発によってサイバー攻撃の予知技術を確立することを目的としています。このように両者は異なりますが、サイバー攻撃の解析機能の高度化に向けて、「サイバー攻撃解析協議会」等の場を通じ、協力して行く予定であり、原案のとおりとさせていただきます。
3	7	法人・団体（国際公共政策研究センター）	46	″(ヨ) IPv4 アドレスの枯渇に伴う諸課題への対応推進 (総務省)″ IPv4 アドレスの枯渇により、IPv4 アドレスを共同利用する必要があるという論理を示すべきである。 題名と内容との間に論理のギャップがあり、分かりにくくなっている。	IPv4アドレスの枯渇に伴い、通信事業者等は、新規にIPv4アドレスの割当てを受けることが困難となるため、IPv4の後継規格であるIPv6の導入を急ぐとともに、IPv4アドレスを複数のユーザで共同利用する環境を整備することが重要であるという認識において記載しているものであり、原案のとおりとさせていただきます。
3	8	法人・団体（国際公共政策研究センター）	48	″c) サイバー空間に関する観測機能の強化を図るとともに、サイバーフォースセンターの技術力向上等を…″ 「サイバーフォースセンター」が何であるかの説明を加えるべきである。 「サイバーフォースセンター」が説明なく突然出てきて、他との関係性や取組の内容が不明確になっている。	ご指摘を踏まえ、脚注を追加させていただきます。
3	9	法人・団体（国際公共政策研究センター）	50	″（サ）ログの保存の在り方″ 通信記録の保存については民間事業者にとって過度な負担とならないようにする。国際捜査への協力も考慮し、国際的基準に適合したものとする 民間事業者の競争力確保のため、過度な規制は避けるべきである。システムの一部を国が負担することも検討されたい。	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。
3	10	法人・団体（国際公共政策研究センター）	53	″(コ) 国家レベルのサイバー攻撃への対応の強化 (内閣官房、警察庁、総務省、外務省、経済産業省、防衛省及び関係府省庁) 平時および非常時における関係機関の役割の整理・明確化を行うことは非常に重要である。平時から非常時に役割の移行が起こる場合に、引き継ぎなどが短時間で混乱なく行えるように時間的な流れについても整理・明確化を行うべきである。 サイバー攻撃は境界が曖昧で、平時と非常時に線引きをするのが難しい。非常時になる前から引き継ぎなどが短時間で混乱なく行えるように、情報収集などの準備を怠りなく行っておく必要がある。	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。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
3	11	法人・団体 （国際公共政策研究センター）	54～61	p.54 よりの ″① 産業活性化″、p.57 よりの ″② 研究開発″ ① と ② にどちらにリストするかを整理すべきである。 ① の項目で ② に再掲されているものが多い。研究開発は大きな意味で産業活性化に含まれると考えるが、研究開発を別項目にしたなら、分かりやすさの点からも、研究開発は ″② 研究開発″ にリストするべきである。	ご指摘のとおり、研究開発は産業活性化に含まれるものとして整理していますので、原案のとおりとさせていただきます。
4	1	法人・団体 （世須羅グローバル㈱）	－	・サイバー攻撃をする不正アクセスの接続されている現在のデジタル情報信号に対して、同時に ・サイバー攻撃を受ける側から1または複数の継続かつ連続されるアナログ情報信号によるサイバー攻撃のリアルタイムの破壊情報信号を出力する。 ・サイバー攻撃をする逆撃退の不正アドレス壊滅同時防止手段を構築する。 アナログ情報手段は継続かつ連続される情報信号として利用した後は消えるため、デジタル情報信号データとして残らない仕組みが可能。 ・世界中の情報機関が如何にデジタル信号を開発しても世界中の全てのデジタル信号は100%解析される。 ・デジタル情報信号によるサイバー攻撃を防止する対策方法は全て不可能。 世界PCT特許申請出願予定。	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	法人・団体 （ソフトバンクBB㈱ ソフトバンクテレコム㈱ ソフトバンクモバイル㈱）	16, 24	P.16 ① 政府機関等における対策 2）サイバー攻撃への対処態勢の充実・強化 【CYMATとCSIRT等との連携強化や訓練等による対処態勢の構築・強化】 （ク）「新たなサイバー攻撃に対する情報セキュリティ防御モデル」の検討及び演習の実施 総務省において、サイバー攻撃の解析及び防御モデルの検討を行い、官民参加型の実践的な防御演習を行う。（総務省） （ケ）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（内閣官房及び関係府省庁）（P.27再掲） 内閣官房において、関係府省庁と協力し、大規模サイバー攻撃事態等の発生を想定した関係者による対処訓練を実施し、当該結果を踏まえた検討を行うこと等により、大規模サイバー攻撃事態等が発生した際に、「緊急事態に対する政府の初動対処体制について（2003年11月21日閣議決定）」、「大規模サイバー攻撃事態等への初動対処について（2010年3月19日内閣危機管理監決裁）」等に基づき官民が連携して的確な対応を行うことができる態勢を整備する。また、上記訓練は次年度以降も継続して実施する。 P.24 ② 重要インフラ事業者等における対策 【重要インフラ障害に対する連携対応能力の強化】 （ス）分野横断的演習の実施（内閣官房及び重要インフラ所管省庁） 内閣官房において、重要インフラ所管省庁、重要インフラ事業者等、セプター等の協力を得て、具体的なIT障害発生を想定した演習シナリオの作成とそれに基づく分野横断的な演習を実施し、各事業者等のBCPの改訂等に資する課題を抽出する。 （セ）個別分野におけるサイバー演習（総務省及び経済産業省） 経済産業省において、重要インフラの制御系の情報セキュリティ対策のため、今後、実際にサイバー攻撃が発生することを前提としたサイバー演習を実施し、制御システムのセキュリティ評価及びセキュリティ対策に関する知見を蓄積し、我が国の制御システムのセキュリティ対策に繋げる。 サイバー演習等を実施する際には、事業者に過度の負荷・負担を強いることがないよう配慮をすることが必要と考えます。 安全に関する重要情報の収集及び高度な解析を実施すること、また、その収集情報や解析情報及び結果・対策等を関係する事業者等への共有し、事業者の対策に活用することは非常に重要と考えます。 それら情報を用いた演習等を通じ、重要インフラ事業者等におけるノウハウ蓄積を目的としたシナリオ作成及びその精度向上のため、PDCAサイクルを実施していくことは、事業者における相当な負荷・負担が必要となることも想定されます。	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。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
5	2	ソフトバンクBB㈱ ソフトバンクテレコム㈱ ソフトバンクモバイル㈱	21	P.21 ② 重要インフラ事業者等における対策 【新たな「行動計画」の策定】（ア）新たな「行動計画」の策定（内閣官房及び重要インフラ所管省庁） 内閣官房において、重要インフラ所管省庁と協力し、重要インフラの防護を強化するため、重要インフラ事業者等及び政府機関との間における情報共有の仕組みや重要インフラの範囲及びそれぞれの性格に応じた対応の在り方等について検討を行うほか、「重要インフラの情報セキュリティ対策に係る第2次行動計画」の見直しを実施した上で、新たな「行動計画」を策定する。 （ウ）内閣官房において、重要インフラ所管省庁の協力を得つつ、「安全基準等」の整備浸透状況について以下の調査を行う 〈重要インフラ分野における調査〉 「安全基準等」の分析・検証及び改定等の実施状況、攻撃動向や情報システムに係る環境変化への対応状況の把握及び検証を行い、結果を公表する。 〈重要インフラ事業者等に対する調査〉 「安全基準等」の浸透状況に係る調査を行い、結果を公表する。また次年度の調査のための企画・準備を行う。 国の安全に関する重要な情報について、収集及び高度な解析を実施することは非常に重要です。また、その収集情報や解析情報及び結果・対策等を関係する事業者等への共有し、事業者の対策に活用することも非常に重要と考えます。 事業者間の情報共有においては、個人情報・秘密情報に配慮し、事業者が特定できないよう匿名化を実施・徹底して頂きたいと考えます。また、共有の形態については、事業者間で直接実施するのではなく、事業者以外の中立的な第三者を経由しての共有が望ましいと考えます。 事業者間で共有される情報には、各社の経営情報が含まれる可能性が高いため、事業者が特定できないよう匿名化が必須と考えます。	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	3	法人・団体（ソフトバンクBB㈱ ソフトバンクテレコム㈱ ソフトバンクモバイル㈱）	46, 50	P.46 ③ 企業・研究機関等における対策 【インシデントの認知・解析機能の向上】 (ノ) 情報セキュリティ目的の通信解析の可能性等関連制度の柔軟な運用（総務省） 総務省において、情報セキュリティを目的とした通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方について、可能な範囲で速やかに一定の結論を得るよう、サイバー攻撃等の実態、これに対する現行の取組状況等の実態把握に努めるとともに、情報セキュリティを目的とした通信解析における課題の洗い出し等を行う。 P.50 ⑤ サイバー空間の犯罪対策 【事後追跡可能性の確保】 (サ) ログの保存の在り方（警察庁及び総務省） 警察庁及び総務省において、相互に連携しつつ、サイバー犯罪に対する事後追跡可能性を確保するため、可能な範囲で速やかに一定の結論を得るよう、関係事業者における通信履歴等に関するログの保存の在り方やデジタルフォレンジックに関する取組を促進するための方策について検討する。 特に、通信履歴の保存については、通信の秘密との関係、セキュリティ上有効な通信履歴の種類、保存する通信事業者等における負担、海外でのログ保存期間、一般利用者としての国民の多様な意見等を勘案した上で、サイバー犯罪における捜査への利用の在り方についての検討を行う。 「通信履歴の保存」については、「通信履歴の保存」の必要性及び有効性を慎重に議論する必要があると考えます。具体的には、今回の議論は匿名統計化をされたデータの扱いとは異なることから、事前に十分な法的議論を経る必要があると考えます。よって、「事前に法的な議論をオープンな環境で実施した上で」の加筆を求めます。 また、「通信履歴の保存」が必要と判断された場合においても、法令等の改正やガイドライン等の整備といったステップを踏む必要があると考えます。 更に、実施する場合においても、「通信履歴の保存」は、通信事業者に多大なコスト負担・運用負荷がかかることから、対象範囲・対象期間等の条件については、事業者に過度の負担となることのないよう配慮が必要と考えます。 今回の議論における通信履歴に関しては、サイバー攻撃等への対処として、個人を特定することが想定されます。これは、憲法及び電気通信事業法にて保障されている通信の秘密を侵す可能性が非常に高いものと考えます。 よって、検討を実施するに当たり、「通信履歴の保存」の必要性及び有効性を慎重に議論する必要があると考えます。また、「通信履歴の保存」が必要と判断された場合においても、法改正及び基準等のガイドライン等の整備のステップを踏む必要があると考えます。 また、「通信履歴の保存」は、通信事業者に多大なコスト負担・運用負荷がかかることから、通信事業者の意見を十分にヒアリング・把握したうえで検討頂きたいと考えます。 加えて、全ての通信履歴の保存を行うのではなく、サービス等の特性に準じて優先順位の整理を行い、必要と考えられるものを保存すると	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。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
5	4	法人・団体 （ソフトバンクBB㈱ ソフトバンクテレコム㈱ ソフトバンクモバイル㈱）	37	④ サイバー空間の衛生 【普及啓発】 (コ) 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） c) 総務省及び文部科学省において、各府省庁と協力し、保護者、教職員及び児童生徒を対象に、子どもたちのインターネットの安心・安全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、通信関係団体等と連携しながら全国規模で実施する。 d) 総務省において、各府省庁と協力し、スマートフォン等が急速に普及していることを踏まえ、利用者に対して、スマートフォン等の情報セキュリティ対策について総合的な普及・啓発を推進する。 普及・啓発活動を実施してくことは非常に重要なことであり事業者も日々努力をしていますが、事業者に過度の負荷・負担を強いることがないよう配慮をすることが必要と考えます。 全国規模や総合的な普及・啓発活動を継続的に実施していくためには、事業者における相当な負荷・負担が必要となることも想定されます。	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。
5	5	ソフトバンクBB㈱ ソフトバンクテレコム㈱ ソフトバンクモバイル㈱	68	(カ) スマートフォン等におけるフィルタリングの在り方の検討（総務省及び経済産業省） 総務省及び経済産業省において、スマートフォン等に対応したフィルタリングの改善に向け、関係事業者との調整に取り組む。 (キ) スマートフォン時代における利用者情報保護に関する取り組みの推進（総務省） 総務省において、「スマートフォンプライバシーイニシアティブ」（「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」提言）に示された「スマートフォン利用者情報取扱指針」に基づき、業界ガイドライン及びアプリケーションのプライバシー・ポリシーの作成促進及び利用者に対する情報提供・周知啓発等、総合的な利用者保護に関する取組みを推進するとともに、スマートフォンのアプリについて、一般利用者がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みを構築する。 一般利用者がリスクを認知し、利用などの判断を自ら行うことが可能な仕組みを構築することは重要なことと理解しますが、スマートフォンのアプリについては、一般社団法人電気通信事業者協会主導で、事業者対応基準（アプリケーション提供サイト運営事業者向けガイドライン）が策定・運用されています。複数の仕組みが導入・運用された場合は、一般利用者の混乱も想定されることから、どの仕組みを推進していくのか等の整理が必要と考えます。 アプリケーション提供サイト運営事業者向けガイドラインは、アプリケーション提供サイトを運営する携帯電話事業者が、プライバシー及び情報セキュリティの観点から適切でないアプリケーションを提供サイトから排除し、アプリケーション提供サイトを適正に運用すること、利用者への周知・啓発を行うことを目的としています。	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。
6	1	法人・団体 （日本アイ・ビー・エム㈱）	6	（シ） システムの共同利用や統合管理によるセキュリティ対策の強化に向けた取組 （内閣官房） ご趣旨に賛同します。情報システムのログを総合的に分析することで、過去の問題を迅速に検索したり、その知見・経験を活かして現在の状況を分析する際の判断基準として、セキュリティログやサーバーログは極めて貴重な情報です。 多くの攻撃がターゲット化され、毎回未知なる攻撃方法が使われる現在、その一つ一つをセキュリティセンサーで検出したり対応する手法は限界に近づいていると考えます。このため、様々なログから情報を突合させるビッグデータ処理とともに、脅威を明確に規定して、その脅威に対する知見を持つ相関分析エンジンを利用することが重要と考えます。	ご指摘の内容については、今後の施策の推進に当たっての参考とさせていただきます。
6	2	法人・団体 （日本アイ・ビー・エム㈱）	7	(タ) 政府機関システムに企画・設計段階から情報セキュリティ対策が適切に組み込まれるための方策（内閣官房、総務省及び全府省庁） ご趣旨に賛同いたします。システムの企画・設計の段階から情報セキュリティ対策を組み込む「セキュア・バイ・デザイン」の考え方が非常に大事であると考えます。セキュリティ要件を明確化し、要件が確実に満たされることを検証するためには、「セキュリティ要件対策マニュアル」に加えて、要件定義に先立つ脅威分析、必要十分なテスト計画と実施、技術者の教育など、セキュアなシステム構築をエンド・ツゥ・エンドで支えるための仕組みが必要です。また、オープンソースや既存製品を含めたサプライチェーン全体を保護するための取り組みについても、国際的な協業の中で促進・標準化していく必要があると考えます。 システムの企画・設計の段階から情報セキュリティの適切な対応措置を組み込むためには、要件定義だけではなく、システムの企画、開発から運用に至るまでの「エンド・ツゥ・エンド」でベスト・プラクティスや標準を採用することが必要です。システムが複雑化し、また、エコシステムを前提にしたシステム開発・調達が行われるようになった今日、より広い視点に立って、どのようにセキュリティを確保していくか、またどのように持続可能な仕組みを構築するかが大事となっており、セキュア・バイ・デザインのアプローチは非常に有効な手段になると考えます。	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。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
6	3	法人・団体 （日本アイ・ ビー・エム㈱）	10	（ニ）安全性・信頼性の高い暗号モジュールの利用推進（内閣官房、経済産業省及び全府省庁） ご趣旨に賛同します。政府機関のような「国の最高機密」を扱う機関において、安全性・信頼性の高い暗 号モジュールの利用を促進することは極めて重要です。その際、サイバー攻撃がグローバルに行われる現状に鑑み、FIPS 140-2（国際標準規格ISO/IEC 19790:2006 暗号モジュール）のような「最高のセキュリティレベル（レベル4）」の認定を受けたテクノロジーを活用すべきと考えます。 国民や政府の重要情報を守るためにも、世界最高レベルの暗号モジュール利用は重要と考えます。	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。
6	4	法人・団体 （日本アイ・ ビー・エム㈱）	14	P.14 （ア）政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）の運用による緊急対応力の向上（内閣官房及び全府省庁） c）内閣官房において、・・・監視対象先におけるサイバー攻撃等のインシデント情報の効果的な収集及び高度な解析を行うための技術の採用・・・や人員の配置等について検討し、結論を得る。 ご趣旨に賛同します。上記箇所にある「効果的な収集及び高度な解析を行うための技術の採用」は極めて重要です。この分野では既に多くの市販製品が利用可能であり、民間企業の知見、技術を効果的に活用することが有効と考えます。 昨今の巧妙化するサイバー攻撃に対して、一つ一つのセキュリティセンサーによる検出や対応は限界に近づいています。効果的な対策に必須となる事象やログの高度な解析に向けて、様々な情報を突合させるビッグデータ処理とともに、脅威を明確に規定して、その脅威に対する知見を持つ相関分析エンジンを利用することが重要と考えます。	ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
6	5	法人・団体 （日本アイ・ ビー・エム㈱）	39, 53	（1）【インシデントの認知・解析機能の向上】 （チ）サイバー攻撃の予兆の早期把握と情報収集・分析の強化（警察庁及び法務省） （ツ）サイバー攻撃事案の実態解明に係る情報収集・分析など（警察庁） （2）【国家レベルのサイバー攻撃への対応の強化】 ・・・サイバー攻撃に関するインシデントの認知、インシデント情報等の収集・共有や高度な解析及びわが国に甚大な被害が生じるサイバー攻撃が発生した場合の対処の在り方等について・・・ ご趣旨に賛同します。正確な状況判断と的確なカウンターインテリジェンスを実施するため、高度なITスキルとセキュリティ・スキルを有するサイバー空間に精通する人材と、実空間での状況を踏まえて高度な決断を下す人材を配置し、この両者が対等の立場でディスカッションできる仕組みが必要と考えます。 （1）国家レベルのサイバー攻撃はソーシャルエンジニアリングなどを駆使したサイバー空間にとどまりません。GSOCなどで検知されるサイバー空間での情報と、実空間で日々収集しているインテリジェンス（犯罪集団、テロ組織、、貨物や資金の動向、職員のプロファイルなど）を組み合わせて可視化する仕組みを構築することにより、発生しているインシデントの背景や動機、目的等の実態解明のスピードと精度を高めることができます。 （2）更に、サイバー空間からリアルタイムで得られるFacebookやTwitterなどのソーシャルネットワークの情報や各種センサー類から絶えず発せられるBigDataをも活用してインシデントの予兆を捉えることにより、わが国に甚大な被害が生じる前に、通信事業者やISPなどの重要インフラを担う関係機関と連携して迅速に対応することが可能となると考えます。	ご指摘の内容については、今後の施策の検討及び推進に当たっての参考とさせていただきます。
6	6	法人・団体 （日本アイ・ ビー・エム㈱）	48,49	（イ） 悪質・巧妙化するサイバー犯罪の取締りのための態勢の強化 （警察庁） （ク） 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 （警察庁） ご趣旨に賛同します。不正アクセス、不正プログラムは我が国においても急速に拡大し、かつ巧妙化しています。これらを検出するためのアプリケーションや仕組み、セキュリティ機材の整備は急務であると考えます。 不正アクセス、不正プログラムは、情報漏洩はもとより、社会インフラにも甚大な被害・影響を及ぼす危険性があります。例えば、リスク回避に奔走する市民による集中的な預金の引き出しといった社会的問題や、水道・ガス・電気等の社会インフラが混乱するなど、甚大な影響を受けるリスクが考えられます。	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。
6	7	法人・団体 （日本アイ・ ビー・エム㈱）	50	（サ） ログの保存の在り方 （警察庁及び総務省） ご趣旨に賛同します。サイバー犯罪の解決に向けて、ログの解析による事後追跡の可能性を担保する必要があると考えます。とくに単なる通信履歴としてのアプリケーションのログに加え、レイヤ7に該当するネットワークログ（Flow）による監査証跡が必要と考えます。また、問題発生時において企業側でログが取得できていないケースも多いことから、取得しておくべきログおよび取得期間についての法令整備等も必要と考えます。 ネットワークのログは侵入者が決して消すことのできない証拠となります。通信履歴をとらえることで通信の方向性や振る舞いを知ることができますし、サイバー犯罪の解決のためにデジタルフォレンジックの技術が極めて有効であると考えます。	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。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
6	8	法人・団体（日本アイ・ビー・エム㈱）	57	（ウ）標準型攻撃の対策技術に関する研究開発（総務省） ・・・マルウェアに感染したコンピュータからの情報流出に対処する技術の研究開発を行う。 ご趣旨に賛同します。新種のサイバー攻撃、ゼロディ・アタック等を考慮した場合、情報流出を防止するための技術は非常に重要です。またこの分野では既に多くの市販製品が利用可能であり、民間企業の知見、技術を効果的に活用することが有効と考えます。	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。
7	1	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	4	（ウ）「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」の推進（内閣官房及び関係府省庁） 政府における電子署名関連アプリケーションの開発と国民への情報提供時に電子署名が活用されることを提案する。 「オンライン手続におけるリスク評価及び電子署名・認証ガ イドライン」の推進（内閣官房及び関係府省庁）においても、電子署名を政府機関においてより積極的に活用するための施策を推進すべきであり、政府機関等における電子署名関連アプリケーションの開発により注力すべきであると考える。 また、昨今、紙面を賑わしているネット選挙など広く国民全体に影響する情報提供環境においては、送信者の詐称の検証を可能とする環境が求められることから、行政機関自らが電子署名を利用することで、安心、安全な利用環境を率先して示して頂きたい。特に、一般利用者に対しては、送信者や情報提供先などが意図した相手であることが容易に理解可能な表示方法（ユーザインターフェース）が必要であり、これらについて一定の基準が示されることが望ましい。	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。
7	2	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	24	(ス) 分野横断的演習の実施（内閣官房及び重要インフラ所管省庁） 及び　(セ) 個別分野におけるサイバー演習（総務省及び経済産業省） 分野横断的演習ならびに個別分野におけるサイバー演習の対象として、大規模データセンターを取り上げることを提言する。 クラウドサービスやデータセンターサービスが社会経済の随所で利用され、それらを提供するデータセンターやその機能は社会インフラとなっている。またパブリッククラウドサービスの緊急時対応の情報基盤としての有用性も認識されているところである。現状の重要インフラ事業者の定義では、第一種通信事業者による一部のものを除き、大規模データセンターは含まれていないと解釈されるが、多くの社会経済システムの運営が大規模データセンターに依存している現状を考えると、大規模データセンターを明示的に重要インフラ（またはそれに準ずる）産業と位置付けるべきであると考えられ、ここで実施を計画する分野横断的演習ならびに個別分野におけるサイバー演習の対象として取り上げるべきであると考える。 参考：　http://www.ipa.go.jp/about/press/20120928.html また、昨年発生した大規模データセンターにおける停電事故も参考にすべきである。	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。
7	3	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	25	(ソ) サイバー攻撃（インシデント）対応調整支援（経済産業省） サイバー攻撃によるインシデント対応に際しては、民間事業者等の有する能力やノウハウを積極的に活用することを施策として盛り込むことを提案する。 サイバー攻撃によるインシデント対応に関しては、民間事業者等も知識・経験・ノウハウ・スキルを有しており、JPCERTコーディネーションセンターだけでなく、民間事業者等の活用も視野に入れるべきである。JPCERTコーディネーションセンターだけに頼ることは、知識・経験・ノウハウ・スキルの偏在を招く可能性があり、また事態対処能力を単独の組織のみに頼ることは、有事に備えて確保すべき対応能力の稼働率等効率性の面でも問題がある。JPCERTコーディネーションセンターの国際的連携・調整能力は活かしつつ、民間の能力も適宜活用することにより、効率と我が国としての対応力の拡大・確保を実現すべきと考える。	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。
7	4	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	31	(オ) 技術・営業秘密保護に関する官民フォーラムなどの場の準備 （内閣官房及び経済産業省） 営業秘密保護は特に日本企業の海外進出先における情報漏えい・流出リスクが深刻化している現状があり、その点に対する対策も検討対象とするよう提言する。 一般に日本企業の進出先国・経済においては、日本国内に比較して情報セキュリティ対策のための製品・技術・サービスの提供が限られ、知識・経験・リテラシのレベルが必ずしも十分でない状況がある。このような環境における情報保護は、国内以上に慎重かつ周到に取り組まれる必要がある。本項による情報共有・検討に際して、そうした点に対する目配りが行われることを希望する。	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。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
7	5	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	32	(サ) 企業における電子署名利活用の普及促進（総務省、法務省及び経済産業省） 企業における電子署名の利活用の普及促進策の検討・実施に際しては、その用途・目的に応じて適切なサービス品目を選択するための基準が示され、また民間事業者による具体的な電子証明書の提供サービスがどの基準に合致しているかが紹介・周知されることを提案する。 企業における電子署名の利活用の必要性を一般論として説明するだけではその利用イメージや費用対策効果の理解を得られにくいと考える。実際の利用イメージやコスト対効果の具体的事例（成功事例を含む）等を示すことによって利用企業等の理解を得ることが必要であり効果的である。 企業における電子署名の利用においては、本来その用途に応じて適切なサービスが選択されるべきであるが、その選択のための客観的な基準が示されていないことが普及のハードルの一つとなっている。この基準と、各民間事業者から提供される個々のサービスがどのような	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。
7	6	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	32	(サ) 企業における電子署名利活用の普及促進（総務省、法務省及び経済産業省） 企業における電子署名の利活用の普及促進策の検討・実施に合わせて、2013年度以降も、電子署名に関する技術ならびに法に関する国際的視野に立った調査研究を、官民合同プロジェクトとして、継続実施されることを要望する。 企業活動がグローバル化する一方、適用可能範囲が国内に留まっていては電子署名の普及促進には大きな効果が期待できない。また国際的取引等において、国内で一般的な署名方式が通用せず、海外の方式に合わせることになる場合は、わが国の国際競争力や経済活動にとって阻害や負担要因となる。そのような中、欧州会議では電子署名に関する新規制（REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market）が2012年6月4日に採択される等、国際標準化が進展しつつある。このような動きに遅れず、国際動向を仔細に調査し、電子署名のグローバル展開に向けた方策を検討・推進することにより、本施策をより大きな効果に結びつける必要がある。	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。
7	7	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	33	(ソ) 企業の運営するウェブサイトの安全性向上（経済産業省） 本件実施に際しては、民間事業者によるサービス提供の機会を阻害しない範囲で実施されるよう希望する。 ウェブアプリケーションの脆弱性対策は情報漏えいならびにドライブバイダウンロード攻撃の防止のために重要である。そのためのウェブサイトの脆弱性検査やアクセスログの解析は民間事業者が事業として営むサービスのひとつである。そのようなサービスを経済的理由から利用できない零細事業者に対して、無償ツールを提供することで情報セキュリティ対策の向上を図る政策を否定するものではないが、本来民間のサービスを購入できる事業者までが無償ツールを利用することで済ませるようになれば、いわゆる民業圧迫となる恐れもある。 従い、無償ツールの提供に際して一定の条件付けを行うとか、無償ツールと有償サービスの情報を同時同等に提供して利用者が比較選択する機会を確保する等の措置を講じる等、民業圧迫とならない運用が行われるよう希望するものである。	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。
7	8	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	33	(タ) 内部者の不正行為によるセキュリティインシデント防止の検討（経済産業省） ガイドラインの策定と普及浸透に際しては、企業におけるガバナンスを不必要に侵害または圧迫する要素がないよう、また企業活動や企業で働く人の人権に対する制約要因となることのないよう、特段の配慮がなされることを希望する。 内部不正による情報セキュリティインシデントに関し、社会的対応が必要となるのは、個人情報の漏洩、反社会的勢力等の利得につながる場合、および国益を損ねる場合に限定されると考えられ、それ以外のケースは民間事業者等の自己責任の範囲と規定すべきと理解される。 一方、内部不正に対する防止策は、ともすると通常の業務プロセスを複雑化したり効率を著しく阻害したりするものになりかねない。また私的持ち物の検査等が過度に行われる場合はプライバシー等人権に関わる侵害に結びつく恐れも懸念される。従い、本件ガイドラインの策定やその普及、適用に際しては慎重な判断と運用が必要である。	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。
7	9	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	34	(ト) 大学に対する情報セキュリティに関する最新情報の提供（内閣官房、総務省、文部科学省及び経済産業省） 情報セキュリティに係る資格試験合格による単位認定の導入、資格に関する学習プログラムの導入、経営学修士課程等における情報セキュリティ関連講義の実施等に際しては、民間における知的・人的蓄積の活用を図るよう希望する。 情報セキュリティに関する技術・知識・経験・識見等は民間、それも主として情報セキュリティに関する製品やサービスを提供する事業者に集中して蓄積し、多くの事業者においては体系化されている一方、大学等教育機関においては必ずしも十分な蓄積があるとはいえない状況がある。大学における情報セキュリティに関する教育の実施に際しては、民間の持つそのような知的・人的蓄積を活用することが必要であり有効である。従い、本件施策の実施に際してはそのような民間の持つ能力や知的財産を、適正な対価の下に有効に活用することで成果を上げるような行政及び大学等の対応が望まれる。	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。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
7	10	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	36	(キ) 国際連携を活用した普及・啓発活動の実施（内閣官房及び関係府省庁） 及び (ク)「情報セキュリティ国際キャンペーン」の実施（内閣官房及び関係府省庁） 国際連携の推進に当って民間で情報セキュリティに取組む企業及び団体も加えた官民連携による交流が行われるよう、行政対応を希望する。 情報セキュリティ対策の実施主体や対策のための製品・サービスの提供主体の中心は民間である。このような国際交流は、特に日本企業の海外展開が進んでいる今日においては重要であり、政府間だけでなく官民一体となった交流、情報交換、知識・経験の共有が有効である。従い、このような国際交流の場を、ぜひ官民連携で進められるよう、実施推進主体による配慮・目配りを期待する。	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。
7	11	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	36	(ケ)「情報セキュリティ普及・啓発プログラム」の推進（内閣官房及び関係府省庁） 推進に当っては、民間の活力を活用する視点ならびにそのための費用面での対応を行う施策が十分盛り込まれるよう希望する。 情報セキュリティの一般への普及・啓発活動においては、インターネット安全教室を始め各省庁で展開する施策において民間のボランタリな活動団体等の活用が活発に行われ、末端までの浸透に大きく役立っているところであり、今後もそのような展開が行われることが重要である。その際、民間の力が持続するためにも、民間で必要な経費等への、特に業務や講師・インストラクター等に従事する人の人件費への手当が十分に行われることが必要である。したがって、その面への対応が十分に行われるよう希望する。	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。
7	12	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	41	(ニ) サイバー攻撃事前防止・早期対策に向けた取組の推進（総務省） 本項における各施策には、民間でサイバーセキュリティ対策に関する事業を営む企業等の参画や、それら企業等との情報共有を実施するための取組を含めるべきである。 企業・組織における情報セキュリティ対策はその実施主体の努力に加え、情報セキュリティ対策のための製品・システム・サービスを提供する事業者によって支えられており、その実力如何が日本のサイバーセキュリティ能力を左右すると言っても過言ではない。総務省における本項の取組は重要かつ有意義であるが、その成果が総務省及び一部関係機関のみに帰属することは日本全体の底上げを図る上では不十分である。従って、広く民間も含めた活動となるよう運営上の配慮を期待する。	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。
7	13	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	43	(ヘ) ソフトウェアや情報システムの安全な利用の推進及び脆弱性の発生を縮減するための対策の推進（経済産業省） e)項 ウェブサイトの脆弱性対策については民間事業者のサービス、コンサルテーション、教育の活用も行われるよう希望する。具体的には、独立行政法人情報処理推進機構(IPA)による普及啓発に際して、民間事業者によるサービスの情報も併せて提供されること、または民間事業者による情報提供の機会が確保されることなどが担保されるよう配慮されたい。 項番(7)でも記したように、情報セキュリティ対策における民間活力の活用は重要である。ウェブサイト運営者や製品開発者が自ら脆弱性について学び、脆弱性を作り込まないように努力することやそのための支援をIPA等が提供することは有意義であるが、それだけでは十分でなく、民間事業者の支援が加わって初めて十分なレベルの対策となる。そのためにも、ウェブサイト運営者や製品開発者が民間サービス等の存在を知り利用機会を得るための施策まで、組合せて実施すべきと考える。	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。
7	14	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	45	(メ) 情報システム等の安全性・信頼性等に関する利用者への品質説明力の強化（経済産業省） この項における第三者による利用者への品質説明力の強化という施策には、反対する。 情報システム等の開発者・提供者による説明責任を等閑に付す結果になる恐れがあるので。	ご指摘の「情報システム等の安全性・信頼性等に関する利用者への品質説明力の強化」の記載については、情報システム等の開発者・提供者による品質説明力強化への取組も含まれているため、原案のとおりとさせていただきます。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にさせていただきます。
7	15	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	45	(モ) SOC事業者間等における情報共有の促進（内閣官房、総務省及び経済産業省） SOC事業者における人的・費用的負担に対する配慮がなされるよう希望する。 SOC機能において、他のSOCその他のインターネットトラフィックの監視観察解析機関等との情報共有は極めて大事で有効な施策であるが、民間事業者にとっては時として過剰な人的または費用的負担となる恐れがある。そのための手当てを行政施策において行うことにより、官民間の情報共有をより容易にし実効を上げるために、本件を希望する。	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。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
7	16	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	60	(チ) サイバー攻撃の解析・検知に関する研究開発（総務省） (ツ) 革新的な情報セキュリティ技術の研究開発基盤の構築（総務省）※再掲 (テ) サイバーセキュリティ研究開発拠点の構築（総務省） (ト) 制御システムセキュリティに関する研究開発（経済産業省） これらの項において実施される研究開発や研究開発のための基盤・拠点・設備等の利用には、可能かつ妥当な範囲において、民間事業者が参画しあるいは利用の機会を持てるための施策を取入れ実施されることを希望する。 サイバーセキュリティ対策の実践面を担う民間のセキュリティ事業者の技術やスキルの向上は、日本のサイバーセキュリティ対応能力を左右する重要な要素である。 国において先端的研究開発を進める意義は大きいが、それを民間とも共有し、また民間にも機会を提供することは、国の総合力の底上げに有効であり必要であると考える。 よって民間に先端研究開発への参画機会や情報入手機会を与えることを目指して本件を提案する。	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。
7	17	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	62	(ア) 情報セキュリティ人材育成プログラムの改訂（内閣官房） (イ) リカレント教育の促進（文部科学省） (ウ) 情報セキュリティに関する教育における産学連携の促進 （文部科学省及び経済産業省） (エ) 大学等における情報セキュリティに関する教育（内閣官房、総務省、文部科学省及び経済産業省） 情報セキュリティに関する高等教育に対して、専用の奨学金制度を導入することを提案する。 高等教育機関における情報セキュリティ教育はその内容の多様性と高度性から提供のためのコストも高く、教育を受ける者の負担も大きいことが予想される。 またキャリアパスモデルの浸透が今後の課題であることから就業機会や処遇の面での不安という要素も履修者の負担になると考えられる。アメリカにおいては、情報セキュリティコースに特化した奨学金制度を国が用意し、国の機関における一定期間の就業を条件に返済を免除する等の施策を実施して一定の成果を上げている。 （参考：http://www.ipa.go.jp/security/fy20/reports/industry-basic/index.html 報告書P76、調査結果概要P15） 日本においても目的別奨学金の導入は学生の誘致やリカレント教育に有効であると考えられることから、本件提案を行う。	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。
7	18	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	62	(ウ) 情報セキュリティに関する教育における産学連携の促進 （文部科学省及び経済産業省） (エ) 大学等における情報セキュリティに関する教育（内閣官房、総務省、文部科学省及び経済産業省） 情報セキュリティにおける高等教育機関の教材開発ならびに講師陣の充実には、民間に蓄積された知識・経験・ノウハウ・人材の活用を積極的に行うべきである。 情報セキュリティのための学科等を持つ大学等においても、教材の開発や講師陣の充実には苦労しているところ、民間には事業を営むために抱える蓄積があり、それを新たな人材の開発育成のために活用すべきである。具体的には特定教科の教材の開発を民間に委託するとか、民間の専門知識を有する人材を講師として非常勤（または常勤）派遣する等が考えられる。また今後定年を迎える年齢層の中にも専門的知識や経験を持つ人材が多く含まれることも考えられ、それら人材の活用も一策であると思われる。	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。
7	19	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	64	(ケ) 情報セキュリティに関する国家試験の改善（経済産業省） 情報セキュリティにおける資格認定者に対しては、その資格維持の条件として一定の継続的教育の履修を義務付ける。 情報セキュリティは変化と革新の激しい分野であり、ある時点で試験に合格した実績は、その後も継続的にその試験が求める知識や識見を維持し続けている保証にならない。海外の情報セキュリティ関連資格の多くは継続的教育の履修を義務付けており、日本における主要な資格もそのような制度を取り入れるべきと考える。 なお、継続教育の内容については、民間における教育コースを認定することや、情報セキュリティに関する業務に一定期間以上携わっている実績を認定することも考えられ、民間が提供する履修機会の有効活用や情報セキュリティ人材を実務で活用することに対するインセンティブにも資するものと考える。	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。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
7	20	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	64	(シ) 大学に対する情報セキュリティに関する最新情報の提供 （内閣官房、総務省、文部科学省及び経済産業省）※再掲 複数の教育機関による、研究機関における研究経験、民間等における実務経験及び標準開発活動等を組み合わせて単位を認定することで大学卒または大学院卒の資格を認定する仮想的情報セキュリティ大学・大学院制度の創設を提案する。 現在、情報セキュリティに関する高度教育の提供能力は限られており、専門課程を持つ大学等は少数である。一方、情報セキュリティの実務を担える人材の開発・充足は急務であり、教育機会の充実を待つ余裕はない。また多数多様な人材の育成には選択の機会の提供も重要である。従い、情報セキュリティ人材の知識スキル体系を定義し、それを満たす履修要素を設計して、各履修要素を満たす内容を、大学の講義、研究機関における研究、実務への就業等の中から認定するとこで、教育コースを形成する。受講者は、就業や修学等の複数の形態を併用し、自分の目的に合う履修機会を組み合わせることで必要な単位を満たし、卒業資格を得ることができる。 この仕組みは履修機会を提供する側にとっても、学生の確保、研究員や従業者の確保、学会や標準化機関での活動要員の確保等、メリットが大きい。つまり実務人材の不足を補いつつ、高度情報セキュリティ人材を養成していくことが可能となる仕組みである。 なお、この制度の運用はそのようなカリキュラム・制度の設計と対象履修機会の認定ができる能力を有する教育機関や民間企業もしくは団体に委託することで、実務能力を用意することなく可能であり、その面でも柔軟性と効率性の高い制度となると考えられる。 現在、サイバー大学や放送大学など複数の教育機会を組み合わせ、また電子多岐に履修することで単位認定して大学卒業資格を与える制度はあるが、さらに踏み込んで研究開発、標準化活動、実務への従事等に単位取得機会を拡大することで、人材不足を補いつつ高度教育を履修した情報セキュリティ人材の育成につなげることができると考える。	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。
7	21	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	54	①産業活性化 情報セキュリティ産業自体の活性化と能力向上を支援するために、1)研究開発支援施策の実施、2)ベンチャー企業育成・支援施策の重点的適用、3)需要喚起策としての情報セキュリティ投資減税等の実施、4)公的調達における国家安全保障の視点からの調達選抜の仕組みの導入、5)海外進出支援、等の施策が実施されることを期待する。 サイバーセキュリティ技術は国の安全保障にもかかわる技術であるので、自国における一定水準の技術力の確保は必須であり、そのためには研究開発機関における取組もさることながら、民間企業における技術力の向上・蓄積と、それを可能にするための産業活性化が不可欠である。しかるに、日本で自ら製品開発を行う情報セキュリティ事業者の事業規模は必ずしも大きくなく、その供給量も限定的である。 （http://www.jnsa.org/result/2013/surv_mrk/ 報告書P67,P76、 http://www.ipa.go.jp/security/fy23/reports/industry-prop/index.html） また、サイバー空間は陸海空宇宙に次ぐ第5の防衛領域との指摘もされるように、サイバーセキュリティにおける国家安全保障の視点は重要であり、公的調達に際しては必要に応じそのような判断基準を導入すべきである。従い、我が国を起点とする情報セキュリティ企業の育成と産業の活性化、またその鍵となる国産の先端的サイバーセキュリティ技術の涵養は、サイバーセキュリティ戦略の一つの軸をなすべき重要な課題と考える。よって本項の提案をする次第である。	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。
7	22	法人・団体（NIP日本ネットワークセキュリティ協会社会活動部会）	3	①政府機関等における対策 公的機関における調達に際して、サイバーセキュリティ分野においては技術評価を特に重視することが可能な評価の仕組みを取り入れることを提案する。 サイバーセキュリティにおいては、技術的特殊性から、高度な技術や経験やスキルが必要であり、それらが伴わない製品やサービス、特にサービスは利用価値が著しく低くなるばかりか、十分所期の目的を満たさないことが起こりかねない要素がある。一方で、そのような質の伴わない製品・サービスは価格が低く抑えられる傾向にあり、価格を重視する選考では、そのような低質の供給が選択される恐れがある。 一方、公的機関が調達に際して行う入札等の選抜においては、近年、費用効率の追求の視点が強く意識される中で価格点重視または価格点の比率を高める方向にあると見受けられる。そのような中、不十分な技術内容の提案が価格点で高得点を得ることで採用される可能性が高まっているが、これは上述のようにいわゆる「安物買いの銭失い」の結果に陥るリスクが高いと言える。 従い、サイバーセキュリティに関する調達、特に役務の調達に際しては、一定の予算枠の範囲内であれば技術評価を優先して採用できるような評価の仕組みを用いるべきであると考える。 （なお、本件は政策の記載順としては最初に登場する事項についてであるが、政策の内容でなく手続きにおける改善提案であることから末尾に記載した。）	ご指摘を踏まえ、追記させていただきます。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
8	1	法人・団体 （㈱ラック）	35	④サイバー空間の衛生 【普及啓発】 　啓発の一丁目一番地は「一般利用者等に当事者であることを気づいてもらうこと」である。一般利用者、家族、先生・教師、会社員、組織の長等毎に、無関係な人は存在しないことを出発点として、しっかり国民に伝えるべきである。 　またWebサイトやキャンペーン等を通した啓発活動が中心となって普及啓発を行う旨が記載されているが、当該Webサイト等へ訪問する者は、以前からセキュリティに興味を持っている層である。そのため、多くの一般利用者は上記Webサイトやキャンペーン等が開催されていることすら存在を知らずに日常生活を送っており、そのような層に対して啓発を行う方法について検討することが必要と考える。 　サイバー空間の衛生を強靭なものにするためには、攻撃者側が狙う一般利用者等のスマートフォンや端末等のセキュリティ確保が重要である。直接的な被害を受ける国民等の一般利用者等に対して適切な情報を速やかに提供することと、当事者意識を持たせることが重要と考える。特に大多数のセキュリティに対する関心を持たない層に対して、適切な対策をとることの重要性を認識させることは重要である。狙われやすい企業と連携した啓発活動等の積極的な施策に期待したい。	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。
8	2	法人・団体 （㈱ラック）	52, 53	P52 ⑥ サイバー空間の防衛【自衛隊等の態勢強化】 P53【国家レベルのサイバー攻撃へ対応強化】 　諸外国は、サイバー攻撃の脅威に対する対処を国の安全保障の観点から位置づけている。しかしながら日本にはそうした視点が不足しているように思われる。各国との協力を深めるためにも、自衛隊が適切の活動できるよう具体的な法律の整備を急ぐべきと考える。 　民間企業が外国政府等の関与が疑われる国家レベルのサイバー攻撃を受けた場合に、自衛隊のサイバー防衛隊はどこまでの責任範囲で対処できるのか、またその際の警察庁等の他の府省庁との連携や責任範囲は曖昧なままである。国民の生命財産を守るという観点で早急に整備をお願いしたい。	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。
8	3	法人・団体 （㈱ラック）	69, 72	P69 ① 外交【 基本的な価値観を共有する国等との多角パートナシップ構築・強化 】 P72 ② 国際展開【 ASEAN地域等と共に成長できる関係の構築 】 　米国、EU、韓国及びASEAN地域等との政府レベルでの連携が本取り組みにて強化されており、高く評価できる施策である。一方で当該地域に進出する民間企業においては、現地におけるセキュリティ情報を収集する経路が限られている。政府において海外連携にて収集した情報のうち、機密に当たらない情報については民間企業と共有する枠組みについて検討いただきたい。 　海外進出先における情報セキュリティ対策は日本企業の悩みの一つとなっており、国益を守る視点から、政府の積極的な支援や環境整備について加えるべきである。	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。
9	1	個人	－	言っていることが矛盾の極みである。 「サイバーセキュリティ」は、ありえない言葉である。 　情報に対してセキュリティ対策をするのであり、情報セキュリティが正しい言葉である。 サイバー空間とは、インターネットというオープン・ネットワーク空間であり、公道とか公海に相当するものである。 　従って、強靭なサイバー空間、活力あるサイバー空間、世界を率先するサイバー空間などという言葉が存在しない。 　公海と言える大平洋を強靭になど不可能である。 　入ってくる人を規制せず、自由に出入りできる世界がインターネット空間であり、それをサイバー空間と言うのである。 　そのオープン・ネットワークのセキュリティー性を上げようというのは、全く矛盾してしまう。 　大事な情報は、インターネットに接続してはならないというのがセキュリティー対策の基本である。 　指示を受けたからやるなどではない慎重な検討を希望するものです。	ご指摘の「サイバーセキュリティ」については、サイバー空間と実空間の融合・一体化と、サイバー空間を取り巻くリスクの深刻化という環境の変化を踏まえ、「サイバーセキュリティ戦略」（平成25年6月10日情報セキュリティ政策会議決定）の「はじめに」において「従来の『情報セキュリティ』確保のための取組はもとより、広くサイバー空間に係る取組を推進する必要性と取組姿勢を明確化するため、本戦略の名称は『サイバーセキュリティ戦略』とした」等と記載しているものであり、原案のとおりとさせていただきます。
10	1	個人	3	「サイバーセキュリティ戦略」のパブリックコメントで追加された最も優先度の高い「今までの取組とは異なる新しい対応」としての「脆弱性への対処」の文言を次のとおり追加されたい。 ・該当箇所：「サイバー攻撃に関するインシデントの認知・解析---」 ・修正案：「脆弱性への対処やサイバー攻撃に関するインシデントの認知・解析---」 　政府機関や企業の機密情報並びに重要インフラの制御システムを狙った執拗な標的型攻撃（APT攻撃）に対応するための実効性ある対策として、「サイバーセキュリティ戦略」のパブリックコメントに基づき「従来のサイバー脅威の状況認識に加えて脆弱性の状況認識」の必要性が認識され、「脆弱性への対処」の文言が追加されている。	ご指摘を踏まえ、修正させていただきます。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
10	2	個人	3	今そこにある危機である執拗な標的型攻撃（APT攻撃）に対応するためには、実効性のある基本的対策としてセキュリティ常時監視の導入が必須である。 セキュリティ常時監視の実現にあたっては、見直された政府統一基準（セキュリティ管理策）に基づくOS及びアプリケーション別のセキュリティチェックリストの整備並びに世界最高水準の製品の活用によるセキュリティ常時監視能力の整備及び高度セキュリティ人材不足の解決のためのクラウドサービス化を検討する必要がある。 （修正案） 内閣官房において、各府省庁のCISOがガバナンス機能を発揮し、機微な取扱いが必要な情報を扱う業務を特定して重要な情報資産を識別し、適時及び適切に当該資産を守るために政府統一基準に基づき組み込まれたセキュリティ管理策を継続的にチェックする枠組みを構築する。 APT攻撃に対する実効性のある基本的対策が具体的に提示されていない。現時点においても、SCAP等のデファクト標準に基づく世界最高水準のセキュリティ製品を活用すれば、外部センサ及び内部センサデータ収集レベルのセキュリティ常時監視能力の実現及び意思決定のためのリスク評価能力の開発が可能である。 APT攻撃は、DDoS攻撃のような従来型の予測や可視化の容易なサイバー攻撃と異なり、数ヶ月～数年に亘って標的に対する任務を完了するまで隠密裏に攻撃を継続するものであり、第三者による情報セキュリティ監査等によってインシデントが発見される事例がほとんどである。また、APT攻撃は、攻撃指示が出された場合、ネットワーク速度に基づく攻撃であり、攻撃の予測が困難である。このようなAPT攻撃に実効的に対応するためには、重要度の高い情報及び情報システムが危険にさらされているかどうか（脆弱性の有無）を情報セキュリティ監査のPDCAサイクルよりもより短い周期で認識する必要がある。このためには米国で進められている情報セキュリティ、サイバー脅威及び脆弱性の継続的な状況認識を行う「セキュリティ常時監視」と同様なメカニズムを整備する必要がある。	当該記述はリスク評価手法の検討としての取組を記載しているものであり、また、統一基準の見直しも検討しているところです。ご指摘の内容については、今後の施策の検討にあたっての参考とさせていただきます。
10	3	個人	26	重要インフラの制御システムへのAPT攻撃に対する実効性のある基本的対策は、情報システムと同様にセキュリティ常時監視であり、経済産業省が「制御システムにおける動的なセキュリティリスク管理のためのセキュリティマネジメントシステムの適合性評価スキーム」の検討項目としてセキュリティ常時監視を盛り込むべきである。 （該当箇所） 「経済産業省において、独立行政法人情報処理振興機構---」 （修正案） 「経済産業省において、動的なセキュリティリスク管理の基本的考え方に基づき、独立行政法人情報処理推進機構---」 重要インフラの制御システムのセキュリティ管理策の標準化及び制御機器等の静的な評価認証については、日本として推進が行われているが、当該セキュリティ管理策の常時監視については、まだ検討対象にされていない。 米国では、2013年2月に出された大統領令（EO13636）に基づく「重要インフラセキュリティフレームワーク」の開発指示と同時に大統領決定21号（PDD-21）に基づく重要インフラの物理及びサイバーに関する脅威及び脆弱性のニアリアルタイムな状況認識能力デモ開発指示が国土安全保障省に出されている、	「制御システムのセキュリティマネジメントシステム適合性評価スキーム」は、各企業がセキュリティマネジメントに関する適切な管理策を選択し、当該管理策について導入、運用、監視、維持改善を継続するマネジメントシステムを評価・認証するものです。 各企業がリスク対応のためにとる管理策については、常時監視も選択肢の1つですが、最終的には個別のケースにより各企業が判断するものです。従って、当該本文には特定の管理策に関する記述はせず、原案のとおりとさせていただきます。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。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
11	1	個人	－	サイバーセキュリティには、「人」「機械」「普及」の3つのリスクがあると考えております。 1　人のリスク（法の遵守と道徳教育） 情報セキュリティの管理者は、公務員のような厳格なモラルが求められると思います。なぜなら、通信の内容、財産、個人情報など、役所でしか把握できないような内容も、職務上、知り得る機会があるからです。試験で資格を得る以外に、実務経験者となった後も数年おきの研修制度を設けるなど、常に健全かつ最先端の職識を持つ必要があると思います。また、情報の責任者が、その職責に反して情報漏洩や産業スパイなどの反社会的行為をした場合、取り締まる法整備や体制構築を強化する事も必要に思います。 2　機械のリスク（国産技術の振興と多国間連携） アメリカのNASAは、重要な機器には外国製の部品を使わないといった、製造段階でのハード面のリスク管理もしています。国家間でのサイバー防衛では、ソフト面だけではなくハード面のリスク管理も必要であり、まずは国産品、次に信頼できる同盟国品、そして代替できない場合に限り廉価な諸外国産を用いるなど、情報機器に使われている部品の信頼性を物理的な面以外に政治的にも評価して、セキュリティ向上を図る必要があると思います。レアメタルや機器に使用できる部品の、リサイクル率を向上することも大切に思います。また、国産のブラウザなどの基幹ソフトやワクチンソフトなど、ソフト面での国産普及を促進する施策も必要に思います。 また、天災や戦争による物理的損害や、サイバー攻撃によるプログラミングやデータの破壊といった、万が一の危機に備える為にも、例えば、情報復旧の為のバックアップ端末は国内の離れた場所に3箇所以上、定期的なバックアップ処理の義務化、遠隔操作の防衛の為に、オフラインへの物理的な遮断が手動で行える仕組みなどの対応策が必要に思います。また、国際規模のサイバー攻撃事例について、国家間で情報を共有して対策を協議するなど、外交を通じた多国間連携によるサイバー防衛策も大切に思います。天災など国内のみで防ぎきれない場合も考えられるので、将来的には、衛星や月にバックアップサーバーの施設を建設する計画を立てても良いと思います。 3　普及のリスク（安全の平等とサイバー攻撃の報告体制構築） パソコンとスマートフォン向けの無償ワクチンソフトを、国民へ国が無償で提供する。最低限の情報の安全が、貧富関係なく平等に得られるようにするために、市販されているワクチンソフトの最低限の機能を、国が無償提供しても良いと思います。 国がどんなに予算をかけてサイバー防衛体制を強化しても、普及の規模がもたらすサイバー犯罪の最新リスクをすべて取り締まることは難しいです。そこで、民間の情報関係の会社やパソコンに詳しい個人と協力できる体制を構築する必要もあります。例えば、保健所への感染症の報告のように、サイバー攻撃に関する報告を義務づけたり、インターネット上における何らかの悪い兆しを、報告や情報提供できる掲示板を設置するなどしてはどうか。	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。
12	1	個人	－	Torという匿名通信システムがあります。 しかし、このようなものは、犯罪やスパイ活動等以外に有益な使い道がないと思います。 したがって、サイバーセキュリティを確保するため、法律によりTorの使用等を禁止するべきだと思います。 この点、このような禁止は、通信の秘密との関係で問題があるとも考えられます。 しかし、我が国においては、このようなものを使用するまでもなく、サイバー空間における通信の秘密は、厳格に保障されていると思います。 確かに、捜査等のために適正な手続によりこれが制限されることはあります。 しかし、これは通常の通信であっても同じであって、これを理由にTorの禁止が憲法違反であるとはいえないと思います。 また、Torは、超法規的な反体制活動等のために有益であるとも考えられます。 しかし、超法規的な反体制活動等が正当であるような場合は、国家の法規範は、もはや　その正当性を失っていると思います。 このため、このような場合は、法律によってTorが禁止されているかどうかは、もはや無意味になってしまっていると思います。	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。
13	1	個人	8	いつも国のために働いていただいてありがとうございます。 私は日本が大好きです。 日本人が誇りをもって、幸せに暮らせるように願っております。 今回メールいたしましたのは「サイバーセキュリティ2013（案）」に関して意見を申し上げたかったからです。 8頁（ツ）「政府調達における情報セキュリティの確保（内閣官房及び経済産業省）」において、「「政府機関の情報セキュリティ対策のための統一基準」を遵守する」とあります。 これはこれで必要なことだと思いますが、仕様を満たしていれば中国や朝鮮の企業が落札できるということでしょうか？ それであれば、見つからないようにバックドア等のプログラムを仕込むことは簡単にできるでしょうし、情報の抜き取りが容易にできることが予想できます。 また、日本の企業のフリをした中国・朝鮮系の企業があるかもしれません。 会計検査や予算執行上難しいかもしれませんが、どの企業から調達するかも情報セキュリティ上重要になってくると思います。 日々新しい手技が開発される分野で大変だと思いますが、日本のセキュリティのため、よろしくお願いします。	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。

番号	枝番号	提出者	該当ページ	概要	御意見に対する考え方
14	1	不明	－	現在、企業や個人に関する情報のテンペスト(遠隔からのPC画像盗聴)での窃取など高度かつ悪質なサイバー攻撃が国内外で現実のものとなっています。 その他にもスパイウェア通信傍受や"電磁波攻撃"と呼ばれる新しいサイバーテロは、PCや電化製品にインフラから侵入し機器に負荷をかけ過電圧をもたらす事により、機器を損壊する攻撃として知られています。 また、人体にも多大な影響があり殺傷能力のある攻撃として全国で被害が多発しています。 中国や北朝鮮、韓国からのサイバーテロ、特に最近ではアメリカが中国・北朝鮮からのサイバー攻撃により甚大な被害が発生したとニュースになっています。 国内に於いては公明党の支持母体創価学会が、"中国を父・韓国を兄として戦って行く"とサイバーテロを匂わす発言をしていた事が問題となっております。 この電磁波攻撃には軍事的な人工衛星からのセンシングや、"パラメトリックスピーカーからの音声送信"等、目に見えない攻撃が行われている為、従来型の防衛では攻防にならないのではと危惧しております。そこで弊社は国民に安心と安全を提供すべく国民からの生の声をリサーチし、実態調査、サイバー犯罪対策、様々なセキュリティソリューションをご提供する事で、国家の安全保障・危機管理、国際的な競争力の維持・強化、国民の安全・安心の確保の為にご協力出来ればと存じております。 サイバー攻撃を国家安全保障上の重要課題と位置付け、今後増えるであろうクラウドに於ける具体的なセキュリティ取組、スマートフォン等の情報セキュリティ対策の強化、Javascriptの脆弱性対策、IPAとの連携の強化、官民が連携して的確な対応を行うことができる態勢整備は今後非常に重要な課題となると思われます。	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。
15	1	不明	－	反日左翼や国内外で反日姿勢を強める特定アジア3か国(中国、韓国、北朝鮮)に情報が漏洩しないように超法規的措置をもって関係者関係先の選別に努めてください。日本に帰化した上記3か国の者は当然排除です。	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。
16	1	不明	－	華為技術製ネットワーク機器を踏み台にした、ハッキングが、アメリカ、イギリスで問題になっています。 機器のバックドア情報が、ハッカー集団に渡っているようです。 政府、自治体、企業の採用制限の検討が必要ではないでしょうか？	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。