「サイバーセキュリティ戦略(案)」に対する意見募集の結果の概要

資料 1-2

■ 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5月21日(火)～6月4日(火)

■ 意見総数: 174件 【内訳:22企業・団体から延べ130件、24個人から延べ44件】

(1)賛同意見 全10件

(2)修正意見 全58件

・ 戦略の構成、基本的考え方等に修正を求める意見はなし。

・ 表現の適正化、考え方の追加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16件)。戦略内の他の箇所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42件)。

(3)政策展開に係る意見 全105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

(4)その他 全1件

趣旨不明等の意見については、その旨理由を付して採用しない旨回答

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

● 各主体のCSIRT間の連携や国際的なCSIRT間連携の強化等に賛同する。(p17)

● 国における収集したインシデント情報や攻撃手法の分析結果等について、重要インフラ事業者等の関係機関と共有するための仕組みも整備することに賛同する。(p26)

● 中小企業に関しては、大企業が持つ人材やスキルとの格差が大きいのが現状であり、「中小企業に寄り添った情報提供・相談体制の整備」は官民協業で取り組む高優先度のものと考える。(p29)

（2）修正意見

● 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。（p29,13行目、下記のとおり修正）

> ･･･我が国の国際的な競争力の源として･･･企業や教育・研究機関において、サイバー攻撃に関するインシデント等の認知・解析機能を強化し、インシデント情報の共有促進を図る。また、企業等の海外進出先における情報セキュリティ対策を促進する。

● 国際標準化活動は、企業等に大きく依存するところ、企業等の利益管理の視点からは十分な資源・予算の投入は困難であることから、政府によるイニシアティブの発揮と支援の必要性について加えるべきである。（p35,6行目、下記のとおり修正）

> ･･･国際標準化や評価・認証の国際的な相互承認枠組み作りに関して、積極的に参画・働きかけを進めるとともに、関係する民間部門への支援や国内の評価・認証機能の整備も進めていくことが必要である

● 一般家庭や若年層のリテラシーを向上に関する取組を加えるべきである。（p38,下から13行目、下記のとおり修正）

> 高齢者層における情報セキュリティ対策も今後一層重要となるため、情報セキュリティに関するサポーター等の育成・活用など高齢者に対するきめ細やかなフォローを行うための環境を整備する。また、一般家庭や若年層に対する知識や情報の提供に係る取組を促進する。

（3）政策展開に係る意見

- インシデントの解析機能の向上については、重要な課題であり、総論としては賛成であるが、解析を重視するあまり、「通信の秘密」、「プライバシー」等への影響を軽視しないよう慎重に検討することを希望する。（p17）
- サイバーセキュリティ産業の育成、サイバーセキュリティ分野において国際競争力を持つ企業・ベンチャー企業の育成は、大変重要であり、国として積極的な支援を行う仕組みを是非構築していただきたい。（p21）
- 重要インフラ事業者においても多様なサービスやシステムを保有していると考えられることから、サービス等の特性に応じて優先順位や対処レベル等の整理を行うべきと考える。（p28）
- 情報家電・医療機器等の組込みソフトウェアの脆弱性対応に関する制度化が検討されているが、過度な規制によりイノベーションを阻害しないよう、配慮願いたい。（p31）
- 犯罪の立証に十分な通信ログを取得するのは非常に困難であると考える。取得をするのであれば「どのように利用するのか」「どの範囲まで取得させるのか」という問題を整理した上で議論すべきと考える。（p32）
- ログの保存を義務化することについては、通信の秘密と密接にかかわる分野なので、慎重に議論を行っていただきたい。（p32）
- サイバー攻撃を受けた際に、どの段階から、どの部分を警察庁から防衛省に移すのかなど、2組織間の役割分担を明確にし、またその際の対応の連続性を確保する。（p33）
- 情報セキュリティ人材の育成にあたっては、技術的知識やスキルだけではなく、高い職業倫理感、および、責任感を付与するような教育が必要である。（p36）

46者　　174件

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 ((ISC)2 Japan Chapter)	36	情報セキュリティのスキル標準や能力・知識の明確化、コミュニティを活用した交流では、民間のノウハウや活動を活用すべきである。 政府が情報セキュリティ人材育成の推進のため、積極的に環境や制度を整えることは歓迎する。 しかしながら、既に民間分野・学術分野では情報セキュリティの取組は進んでおり、資格制度や多くのコミュニティが存在する。 不足する16万人あまりの人材を早期に育成するためには、政府はあらたに同様のことはせず、これらのノウハウ活用や連携強化を積極的に行うべきである	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。
1	2	法人・団体 ((ISC)2 Japan Chapter)	26	政府機関等の情報セキュリティの取組として、Continuous MonitoringやStrong Authenticationなど具体的な取組とスケジュールを示すべきである。 米国OMBでは2009年に、これまで行ってきた情報セキュリティ対策では十分な効果がないことを認め方針を見直している。 新たな取組として「Trusted Internet Connections（TIC）」「Continuous Monitoring」「Strong Authentication」が追加されている。 日本政府においてもこれらを参考にして同様の取組を行うべきである。特に未着手であろうContinuous Monitoring、Strong Authenticationについては早々に着手すべきである	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。
2	1	法人・団体 （インターナップ・ジャパン㈱）	21	現在日本では、サイバーセキュリティーとい うとハッキングによる情報の盗取やなりすましによる詐欺ばかりに意識が向いているが、欧米においては、企業の経営に多大なる脅威を与え、健全な経済の成り立ちに対する悪質なテロ行為であるDDoSアタックこそがサイバーセキュリティーの主眼であり、対策も進ん でいる。 しかるに日本では、攻撃数自体は増加しているにも関わらず、企業が公表したがらない傾向があり、問題が表面化していないために対策が遅れている。政府としても早急に意識の喚起と対策の構築 を行うべきである。	2（3）の「③企業（略）の役割」において、「サイバー攻撃に関する情報共有など業界団体等による集団的な対策に取り組むこと」を期待するとしているところです。ご指摘の内容について、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。

46者　　174件

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	1	法人・団体 （ウィズ・テクノロジー㈱）	－	育成プログラム等、育成のための施策だけにとどまらず、情報セキュリティに関する専門家を一定数雇用した企業に対する税制上の優遇措置や資格保有者に対する待遇改善など、人材の活用促進の施策が必要不可欠である。 既に情報セキュリティに関わる人材育成については、2006年「情報セキュリティ政策会議」（議長：内閣官房長官）の下に設置された「人材育成・資格制度体系化専門委員会」（委員長：西尾章治郎 大阪大学大学院教授（文部科学省科学官））から公表された「人材育成・資格制度体系化専門委員会報告書」など、相当の検討が行われ、様々な施策が実施されてきた。しかし人材不足の現実は十分に改善の方向に向かっているとは言いがたい。この問題の根幹は育成する側の体制やプログラム作りのみを行い、「育成される側」の視点に基づいた施策が欠けているという点にある。端的に説明するならば、高度なスキルを習得しても、雇ってくれる組織がなければ、また相応の良い待遇が見込めなければ、才能ある人材であっても情報セキュリティの専門家になろうというモチベーションが生まれないということである。 これは現在多くの法科大学院が定員割れ・司法試験合格率低下を引き起こし、また多くの司法試験合格者に就職先がないという問題や、大学院における博士号取得者の増加とその就職難に関する問題と基本的に同じ構図であり、いたずらに育成だけを行っても、結局スキルや資格を取得した多くの人が、その後の職に困るという状況を引き起こすだけである。 したがってこの社会構造を変えない限り、多くの優秀な人材が情報セキュリティ分野において専門家になろうとはしないと考えられるし、結果として人材不足は解決できない。また雇用と人材の流動性が高まっている昨今では、優秀な人材ほど、多くの就職先があり、好待遇が期待できる分野へと移動していってしまうと考えられる。 米国において情報セキュリティ関連技術者は、他の分野のIT関連技術者と比較して平均1万ドル程度年収が高いという調査報告もある。また企業が採用においてセキュリティ関連資格を条件としている場合などもあり、専門家としての高度なスキルと経験を身につければ、相応の仕事と待遇が得やすい社会構造が成り立っている。 この問題を解決するためには情報セキュリティに関する専門家を一定数雇用した企業に対する税制上の優遇措置や資格保有者に対する待遇改善など、多くの視点から、育成された情報セキュリティ専門家が雇用と好待遇を得やすい社会構造を生み出す必要がある。	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。
4	1	法人・団体 （NRIセキュアテクノロジーズ㈱）	11	「それぞれの戦略に基づく取組については、概ね計画通り実現されてきたといえる。」という記述について、脚注で根拠を提示すべき。 年次計画である情報セキュリティ20XXについては、情報セキュリティ政策の評価等の実施方針（第3版）で方向性が定められており、複数年度にまたがる戦略の政策評価についても一定の手続きにのっとって公開をすべきである。 http://www.nisc.go.jp/conference/seisaku/dai32/pdf/32shiryou0601.pdf	毎年度実施している情報セキュリティ政策の評価等を根拠に記載しているところであり、ご指摘の内容をふまえ、脚注に、根拠として、年次計画に関する評価等を記載させていただきます。また、本戦略に基づく年次計画の評価等についても、今後実施の上、公開させて頂く予定です。
4	2	法人・団体 （NRIセキュアテクノロジーズ㈱）	17	意思決定のプロセスや予算等リソース配分の執行責任者の明確化などを具体的に記述すべき。 「強靭な」サイバー空間の構築やサイバー攻撃等に対する防御力・回復力の強化の ためには、複数の主体が相互に連携しながら進める必要があるが、実効的にこれを行うには、施策の責任の所在の明確化やリソース配分を明確にしておくことが重要である。	ご指摘の内容については、P17③に「適時適切な資源配分」として記載されていることから、原案のとおりとさせていただきます。

46者　　174件

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
4	3	法人・団体 （NRIセキュアテクノロジーズ㈱）	34	情報セキュリティ産業の育成や活性化についての記述が少ないため、これらの施策について以下のような記述を、①産業活性化の第1パラグラフ以降に追記すべき。 「そのためには、各種セキュリティ対策に対する税制度上の優遇といった制度面・金銭面での施策を通じて、これら情報セキュリティ産業の育成に配慮すべきである。」 本来あるべき姿として、ITシステムなどにセキュリティ対策を実装した情報セキュリティインフラが存在すべきであり、これらを支えるのが情報セキュリティ産業であるが、本戦略におけるインセンティブが低いため、これらの業界が他の先進的な国に追いつき・追い越すのは困難だと思われる。そのため、情報セキュリティインフラをベースとしてビジネスを営む企業のセキュリティ対策が進まないばかりか、企業のユーザである国民が、高度な情報セキュリティによって安心・安全なインターネットを遍く享受するのは難しいと思われる。	ご指摘の内容については、P29③に「情報セキュリティ投資を促進するインセンティブの検討」として記載されていることから、原案のとおりとさせていただきます。
4	4	法人・団体 （NRIセキュアテクノロジーズ㈱）	20	最終パラグラフを次のように修正すべき: 「新たな制度整備、先端的な技術開発、実証実験、高度な人材の育成やリテラシーの向上等、さまざまな施策を有機的に接続するための戦略を検討し、積極的に実施してゆくことが必要である。」 高度な人材の育成について検討する場合、そもそもグローバルな分野で高度な情報セキュリティ人材とはどのようなものか、そのような人材のスキルセットはどのようなもので、トレーニングやOJTの仕組みにはどのようなものが考えられるのか。といった密接に連携する課題を検討したうえで、整備しなければならない制度の検討や、今後必要と目される技術の開発・実証実験などを企画するといったアプローチでなければ、それぞれが有機的に影響を与える政策とはならないため。	ご指摘の内容を実施することが必要であるとの認識の下で記載しており、原案のとおりとさせていただきます。
4	5	法人・団体 （NRIセキュアテクノロジーズ㈱）	27	セプターカウンシルの今後のあり方や、緊急事態発生時の体制について検討するという内容を追記すべき。 セプターカウンシルにおいて、参加する企業の健全な情報セキュリティインフラとそれに基づく分析情報を交換しなければ、単なるインシデントの情報交換だけにとどまり、組織を有効に活用しているとは言い難い。そのためにも、セプターカウンシルの中で、目指すべき方向性について議論をすべきものと考えます。 また、サイバー攻撃事態に認定された時点で、官邸に別途設置される連絡室/対策室に情報が集約されるように切り替わる仕組みは有事・平時の危機管理計画であり、情報集約経路の切り替えに伴う混乱や情報の欠落等、サイバー攻撃事態に対して適切な運用計画とは考えられません。サイバー攻撃事態に関する連絡室/対策室の設置については、セプターを通じて一本化された情報を採用するなど、状況に応じて報告経路を変えるようなことがないようにすべきだと考えます。	ご指摘の内容については、新たな行動計画の策定に当たっての参考とさせていただきます。

46者　　174件

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
4	6	法人・団体 （NRIセキュアテクノロジーズ㈱）	29	「CSIRTの構築を促進し、CSIRT間の連携対応能力の強化等を図る」という記述について、次のように修正すべき。 「CSIRTの構築を促進し（同等のサービス提供を受けることを含む）、CSIRT間の連携対応能力の強化等を図る」 中小企業においては、専従の情報セキュリティ担当者を設置することは困難な状況であり、情報システム部門や総務などと兼務することで対策に取り組んでいる。そのような組織においては、ISPや情報セキュリティ専業の事業者による遠隔でのセキュリティ管理サービス（MSS）の導入が、費用対効果に優れている場合もあり、そのような選択をする企業が総じてセキュリティ対策ができていないと評価されるおそれがある	ご指摘の内容については、CSIRTの構築の中に含まれており、また、例えば、３（１）③において「情報セキュリティが確保された共同利用システムへの移行促進」と記載されているところであり、原案のとおりとさせていただきます。
4	7	法人・団体 （NRIセキュアテクノロジーズ㈱）	27	ローテーションといった既存の人事制度だけではなく、高度な専門性を持つ有識者の固定配置と組み合わせる、といった内容を追記すべき。 理由は以下の3つ ①期間専従することによる専門性の強化 ②担当者間との信頼関係の構築・維持の強化 ③および専門家としての処遇によるモチベーションの向上 このような人事制度の枠組みに、民間の情報セキュリティ専業企業の職員や、CSIRT等からの出向者を人事交流させ、サイバーセキュリティにおいて我が国を守るという一つの使命の下に連帯感を強化することが重要である	ご指摘の内容については、例えば、３（２）③において「政府機関が率先して、情報セキュリティ人材の外部登用を行う」と記載されているところであり、原案のとおりとさせていただきます。また、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。
4	8	法人・団体 （NRIセキュアテクノロジーズ㈱）	27	「各府省等のCSIRT要員及びCYMAT要員の育成等を強化する。」という記述について、スキルセットの明確化やそれに基づく選抜方法の検討について包括的に検討することを追記すべき。 スキルセットの明確化やそれに基づく育成方法・選抜方法が明らかになっていない状況で、実効的な要員の育成等を検討することは出口なき人材育成策となる可能性がある。	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。

46者　　174件

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
4	9	法人・団体 （NRIセキュアテクノロジーズ㈱）	37	検討のみではなく特に政府職員は率先して知識の拡充と実践的育成の受講とスキルの可視化まで行うことを含め、次のように追記すべき: 政府機関職員で情報管理に係る職務に就く全ての職員は、適切な情報セキュリティ教育を受けると共にスキルを可視化するべく、有効と考えられる国際的に通用する情報セキュリティ資格の取得を義務付ける。また、更にスキルを維持向上する為に、継続してスキルアップ出来る継続教育予算の拡充を図るなど、情報セキュリティ資格保有者への「有資格者手当て」等、インセンティブを検討し、知識、技能向上の意欲を向上させる施策を立案・実施すべきである。 第一次情報セキュリティ基本計画の策定時から「国際的に通用する人材の育成」が掲げられているにも関わらず実際に育成は行われていない。人材育成は重要な課題であり近年、毎年毎年検討を実施しているが、目に見える具体的な成果は出ていないのが現状である。 この現状を打破し、「世界を率先する」サイバー空間を構築しグローバルな戦略空間における貢献力・展開力の強化する為には、不足する情報セキュリティ人材の育成が不可欠であり、それはIPAの調査からも明らかであり、米国政府機関では政府職員が率先して情報セキュリティ資格を保有しスキルを可視化することで、人事評価への活用や適切なローテーションを実施している。（参考、米国国防総省 DoD Directive 8570.1M）更に民間納入事者にも同様の資格取得を求め、情報セキュリティを「共通言語」として活用することにより、システムの安定運用、セキュリティレベルの向上、調達コストの低減等を図っている。 我が国独自の先進的な教育プログラムや国際的に通用する国家資格が無い以上、民間の教育プログラムや資格を活用しまずは米国に追いつくことが必要であり、追いついた後に、我が国の国家資格のあり方を検討すべきである。	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。
4	10	法人・団体 （NRIセキュアテクノロジーズ㈱）	38	リテラシー向上の施策だけではなく、リテラシー向上のための施策でアプローチできない層に対して、さらに踏み込んだ施策（通信回線の一時遮断やネットワーク上での隔離といった対応方針等）も検討することを追記すべき。 元々リテラシーが低く、かつサイバー攻撃についての関心も薄い層に対しては、いくら判りやすいコンテンツを整備して提供しても、まったく流通せずに読まれない可能性が予想される。そのような場合、システム的に何らかのブロックをかける（検疫ネットワークのようなところに隔離し、コンテンツを読了しなければ外部接続できない　など）といった方向性とするのか、今の段階から検討すべきだと考える。 米国においては、重大なインシデントが発生した場合の通信遮断について議論（Protecting Cyberspace as a National Asset Act http://thomas.loc.gov/cgi-bin/query/z?c111:S.3480:）されており、我が国においても深刻なサイバー攻撃事態発生時に取りうる選択肢の一つとして検討しておくことは重要である。	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。

46者　　174件

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
4	11	法人・団体 （NRIセキュアテクノロジーズ㈱）	39	国際連携のあり方や方向性について、具体的な成果と今後の方向性を追記すべき。 ASEAN方面については、NISC主導で政策会議やワークショップ等を実施しており、ARF以上にASEAN各国とは密な関係を構築してきているはずである。また、重要インフラ分野におけるMeridian ProcessやOECDなどは、各国の政府機関担当者や第一線の研究者等が集まる会合であり、我が国もこれまでに同会議において講演をしたり、プログラム委員を務めるなど、まさに顔の見える形で積極的に参加をしてきているものと考える	ご指摘の内容については、4にある「国際分野における総合的な対応を推進するための方針」（なお、これについては政府全体の成長戦略との整合性を図るため、「サイバーセキュリティに関する国際戦略」に修正させていただきます。）の検討に当たっての参考とさせていただきます。
4	12	法人・団体 （NRIセキュアテクノロジーズ㈱）	42	海外組織との折衝に長じた職員の採用を検討することを、第2パラグラフ以降で追記すべき。 「各国CSIRTの構築支援や、セキュリティマネジメントのノウハウ支援、」とあるが、ASEAN各国においては、CSIRT組織そのものの熟成度もまちまちであるため、その国の実情に応じたきめ細やかなフォローを実施する必要がある。 また、インフラ構築支援として入り込んでいる中国・韓国の動向にも配意しながら、我が国のプレステージを発揮できるような場を確保など、技術だけでは務まらないミッションを扱う必要がある。そのためには、海外情勢に通じ、かつ各国との交渉に長けた外務省の協力が不可欠であり、NISCの機能拡大をするにあたって、外務省やJICA職員も受け入れることが重要だと考える。	ご指摘の内容については、例えば、3（1）①において「政府における平常時及び緊急時の対応力を強化するとともに、国際連携を促進するため、人材の確保・育成に取組むことが必要である」としており、原案のとおりとさせて頂きます。
5	1	法人・団体 （ 国際公共政策研究センター）	－	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。	ご指摘の英語版及びスライドについては、今後作成し、NISCウェブページ等により公開する予定としております。
5	2	法人・団体 （ 国際公共政策研究センター）	25	「国際規格」、「国際約束」の範囲内だけに限定することなく、立場を同一とする国々と相対あるいは小グループで秩序を作っていくことについても言及すべきである。 守るべき国際ルールは守るとしても、今後急速に環境が変わってくる中、国際ルールのない状況も想定される。その際、包括的な国際ルールを決めるのに時間がかかることや、利害関係の対立から、国際ルールがすぐに定まらない状況も考えられる。必要に応じて立場を同一とする国々と秩序を作ることから初めることにより、国際秩序の確立に寄与することも大事である。	コモンクライテリア等の国際規格に基づく適合性評価制度の活用について記載しています。ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
5	3	法人・団体 （ 国際公共政策研究センター）	27	各インフラについて全て同じレベルで対応するのではなく、優先順位を付けるべきである。リソースが限られている中、10 分野すべてを同レベルで守ることは困難である。例えば国民の経済や生活にとって何が重要であるかという基準で優先順位を付けてはいかがか。 Richard Clarke の著書 ″Cyber War″ でも提案されており、イスラエルなどでも優先順位を 与えて対応しているようである。	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。なお、現在、重要インフラとは位置づけられていないが、その情報システムの障害が国民生活等に多大な影響を及ぼす恐れのある分野について、今後、当該インフラにおける情報システムの位置付けを踏まえ、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こととしております。

46者　　174件

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（国際公共政策研究センター）	29	CSIRT の構築に関しては、一律に推進するのではなく、国からのサポートを行ったり、ある分野では複数企業共同によるCSIRT を設置するなど、企業の負担を減らす仕組みが必要である。 中小企業が1社で CSIRT を備えることは困難である。また、大企業にとってもCSIRTを構築するために社内で コンプライアンスの仕組みを作る必要などがあり大変な負担となる。	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。
5	5	法人・団体（国際公共政策研究センター）	32	警察庁や防衛省の日常の業務からは独立した中核的研究拠点（Center of Excellence） を設立し、研究開発、新たな脅威の研究・対応、産官学連携、専門人材の交流、海外連携などの役割を課す。 例えば、イスラエルは Center of Excellenceに専門家チームを作り、専門家を育成している。また、NATO はエストニアの Tallinn に Cyber Defense Center of Excellence を設置している。Europol はハーグに European Center for CyberCrime (EC3) を設置した。 これらの実質的な役割は各国の法執行機関のための CoE である。我が国でも、CoE に専門人材を集中させ、研究開発、新たな及び将来の脅威の研究・対応、専門人材の育成、専門家同士の交流、外部専門人材の教育、海外との連携、などの機能を持たせることが必要である。この機関は、実際の法執行機関などの日常業務から切り離すことにより、研究などに専念することが可能となる。また、大学など学術界からの参加や、民間との人材の交流も可能となり、民間のレベルの底上げ、民間への人材提供、またセキュリティ専門家のキャリアパスの提供という役割も果たすことができる。	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。
5	6	法人・団体（国際公共政策研究センター）	33	サイバー攻撃を受けた際に、どの段階から、どの部分を警察庁から防衛省に移すのかなど 2 組織間の役割分担を明確にし、またその際の対応の連続性の確保をする。一方、インフラ事業者など民間との協力体制を構築し、それぞれの役割、責任を明確にする。 サイバー攻撃には境界がなく（Borderless）、どこまでが犯罪でどこからが戦争行為かについての判断は非常に難しい。そのため、警察庁と防衛省の役割や責任分担を普段から明確にしておき、インシデント発生時の迅速な対応を確保することが必要である。一方、民間事業者との協働については、普段から警察庁や防衛省がインフラ企業と密接な情報交換、演習などを行っていなければ、インシデント発生時に迅速な対応はできない。普段は何も接触もない官庁がインシデント発生時に 突然介入してきても、現場を混乱させるだけである。	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。
5	7	法人・団体（国際公共政策研究センター）	34	アンチウィルスソフトや検索エンジンに関してどのように進めていくかを明確にする。 アンチウィルスソフトや検索エンジンはサイバー攻撃の状況を把握するのに重要なツールであるが、今日本には実質的な開発を行っている企業がない。社会インフラの保護のために必要不可欠なものとして国策として推進していくのかなど、国の方針を示すべきである。	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。

46者　　174件

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	8	法人・団体（国際公共政策研究センター）	36	情報セキュリティ人材が組織に入ってからのキャリアパス、そして出口について言及すべきである。 この章では入口（人材の確保）を重視しているが、専門人材の組織内外でのキャリアパスや、出口の展望を示すことが将来に亘る人材の参加を支えることになる。	3（2）③において、情報セキュリティ人材は求められるスキルは対象となる人材の属性によっても大きく異なることから、スキル標準の改善・活用を通じ、必要とされる能力・知識を明確化することとしています。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。
5	9	法人・団体（国際公共政策研究センター）	41	各省庁のサイバーセキュリティの取り組みについて、英語による発信を組織的かつ包括的に行っていくべきである。 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、英語による組織的な情報発信はそのために必須である。	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。
5	10	法人・団体（国際公共政策研究センター）	42	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。縦割り組織てき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。	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（㈱シマンテック）	26	当該個所に「政府機関が取り扱う情報について、情報の種類と重要度に応じた扱い方の共通化・標準化を行うとともに、重要情報の保護を目的とした法制度の整備も進めていく。」の一文を追加挿入。 政府機関の情報について、各省庁で種類と重要度の格付けを含めて取り扱い方法がまちまちであることは、潜在的なセキュリティ・リスクを増大させる。また、適切な法規制は、国の安全、延いては、国民の安全を守るために必要である。	政府機関については、国家機密等に関する情報及び情報システムの重要度に応じた情報セキュリティ対策の重点化を行うため、標的型攻撃等への対処に関するリスク評価手法の確立等を図ることとしており、原案のとおりとさせて頂きます。
6	2	法人・団体（㈱シマンテック）	26	「また、運用・保守の段階における情報セキュリティレベル低下を防ぐために、セキュリティが確保された設定の適用が自動的に行われるようなシステム・ライフサイクルの適用を検討する。」の一文を追加挿入。 運用・保守の段階において、セキュリティに対する考慮が欠落していたために知らず知らずのうちにセキュリティレベルが低下するということが散見されている。また、作業員のミス等によってセキュていぃレベルが低下することも同様に散見されている。これらの事態を防ぐために、運用・保守の段階においてもセキュリティレベルを保つことを前提とした作業環境を実現すべきであり、また、作業ミスを防ぐためにできるだけ自動化することが望ましい。	政府機関については、2（3）①の「国の役割」として、情報セキュリティ対策を実施する主体として、その取組によって他の主体における取組を先導することが求められるとしており、原案のとおりとさせていただきます。

46者　　174件

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 (㈱シマンテック)	37	「～検討を行う。」の後に、「また、官民のインターンシップなど実務経験をさせる場を設けることも検討する。」の一文を追加挿入。 官民のいずれの場でも、即戦力となるには実務経験が不可欠である。従って、教育課程を終えた後に、政府機関などで実務経験をさせる場を設けることで、教育された人材の有効活用につながる。	ご指摘の内容については、3(2)③において、「政府機関が率先して、情報セキュリティ人材の外部登用を行う」などを記載しているところであり、原案のとおりとさせて頂きます。
6	4	法人・団体 (㈱シマンテック)	21	各々の行に記述された「～が期待される」を「～を検討および実施すべきである」に変更。 サイバー攻撃対策は喫緊の課題であり、民間企業においても社会に対する責任を自覚した上で早急に対策に取り組んでいただかねばならないため、「期待する」のではなく「検討と実施を促す」べきである。	本戦略は、民間企業に義務を課す性質のものではないことから、原案のとおりとさせていただきます。
6	5	法人・団体 (㈱シマンテック)	20	「～が期待される。」の一文の後に「そして、こんにちの企業や教育・研究機関において、他企業や機関への業務委託や協業が進んでいる現状を鑑みて、サプライチェーン・リスクも考慮し、対策にあたっては委託先や協業先と連携することが期待される。」の一文を追加挿入。 企業や教育・研究機関において、業務の外部委託や外部との協業が増えており、また、そのような委託先や協業先からの情報漏えいが少なからず報告されている。情報セキュリティは「最も弱い鎖の輪」から破られるものであることを鑑みると、協業先や委託先においても自身と同レベルの情報セキュリティ対策が必要である。	ご趣旨を踏まえ、修正させていただきます。
6	6	法人・団体 (㈱シマンテック)	23	「おいては、」の後に「世界最先端の製品・技術・情報を導入しつつ日本独自のセキュリティ機能を開発することによって世界最高レベルのセキュリティを実現するとともに、」を追加挿入。 国産製品や技術の開発が重要であることは言うまでもないが、現在、そこに在る脅威に対抗するためには世界最先端の製品・技術・情報がセキュリティ対策の土台として不可欠である。そして、それらを導入した上で実現した世界最高レベルのセキュリティを更に高めるための事として技術開発を位置付けるべきである。	ご趣旨を踏まえ、修正させていただきます。

46者　　174件

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	7	法人・団体 (㈱シマンテック)	42	「支援する。」の後に、「また、グローバルに監視サービスや情報収集を行っている民間企業や団体との連携も必要に応じて行う。」の一文を追加挿入。 グローバルにビジネスを転換するセキュリティ企業の中には、一国の政府機関や捜査機関よりも幅広い情報収集を行っているものも少なくない。また、グローバルなメンバーを擁する専門家団体においても、分野を限れば、同様の傾向も見られる。国境を容易に超えるサイバー犯罪への対策をより実効性の有るものにするために、これらの情報や知見を活用すべきである。	2(2)④において、マルチステークホルダーがそれぞれの社会的立場に応じた役割を発揮しながら、国際連携や官民連携をはじめとして相互に連携し、共助することが必要になっていると記載しています。ご指摘の趣旨については、この基本的な考え方に含まれるものと考えています。
6	8	法人・団体 (㈱シマンテック)	32	「活用を図る。」の一文の後に「また、国境を容易に超えるサイバー犯罪の性質を考慮し、グローバルにビジネスを展開する企業や、グローバルなメンバーを擁する専門家団体が保持する情報屋知見にも注目し、積極的な活用を図る。」の一文を追加挿入。 グローバルにビジネスを転換するセキュリティ企業の中には、一国の政府機関や捜査機関よりも幅広い情報収集を行っているものも少なくない。また、グローバルなメンバーを擁する専門家団体においても、分野を限れば、同様の傾向も見られる。国境を容易に超えるサイバー犯罪への対策をより実効性の有るものにするために、これらの情報や知見を活用すべきである。	2(2)④において、マルチステークホルダーがそれぞれの社会的立場に応じた役割を発揮しながら、国際連携や官民連携をはじめとして相互に連携し、共助することが必要になっていると記載しています。ご指摘の趣旨については、この基本的な考え方に含まれるものと考えています。
6	9	法人・団体 (㈱シマンテック)	38	「～する。」の後に「また、サイバー犯罪の危険性や対応の喫緊性を鑑み、情報セキュリティに関しては、情報教育の中核としてNISCが主導してカリキュラムの作成と実施を行うことが望ましい。」の一文を追加挿入。 未成年者がサイバー犯罪に巻き込まれるケースは年々増えており、それを防ぐために、初等教育の段階から情報教育の中核として情報セキュリティ教育を位置付けることが必要である。また、学習指導要領の改訂に伴うカリキュラムの変更には数年を要するため、官邸主導での迅速な対応を行う旨を明記すべきである。	ご指摘のカリキュラムの作成と実施については、教育機関において行うものであるため、原案のとおりとさせて頂きます。なお、初等中等教育段階においては、情報セキュリティを含む情報モラルに関する教育の積極的な推進等が図られているところであり、ご指摘の内容について、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。
6	10	法人・団体 (㈱シマンテック)	22	「～期待される。」の後に「特に、昨年度以降は中小企業への攻撃が増加していること(シマンテックインターネット脅威レポート 第18号より)を踏まえ、重要インフラ事業者や先端的な技術を有する事業者と同等の脅威にさらされていることを自覚した上で対策に取り組むことを検討・実施すべきである。」の一文を追加挿入。 シマンテックインターネット脅威レポート 第18号 (http://www.symantec.com/ja/jp/security_response/publications/threatreport.jsp)に示されているように、昨年度より、中小企業が、重要インフラ事業者や先端的な技術を有する事業者へ侵入する「入口」として攻撃される事案が増加している。また、当該の中小企業は、研究開発や製造の分野における協力企業だけではなく、事務の委託先や用度品の供給元までもが狙われることもある。従って、全ての中小企業は、現在、重要インフラ事業者や先端的な技術を有する事業者と同等の脅威にさらされていることを自覚して、対策に取り組まなくてはならない。	本戦略は、民間企業に義務を課す性質のものではないことから、原案のとおりとさせていただきます。

46者　　174件

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	11	法人・団体 （㈱シマンテック）	33	「～強化する。」の一文の後に「また、全国統一的にサイバー犯罪を専門に取り扱う警察組織の創設を検討する。」の一文を追加挿入。 サイバー犯罪は、都道府県の境界を越えて行われることが大半であり、その際に、現在の都道府県毎に独立した警察組織の一部門としての位置付けでは迅速で網羅的な対応が難しい。諸外国の例を見ても、全国統一的な組織にすることが望ましい。	都道府県の境界を越えて行われるサイバー犯罪の特性を踏まえて、警察では、都道府県警察間での共同捜査・合同捜査を推進するとともに、インターネット・ホットラインセンターから通報を受けた違法情報について、警視庁において発信地の解明までの照会、差押え、証拠保全等の初期捜査を行う「全国協働捜査方式」を導入するなど、現在の警察の枠組みを維持しつつ、効率的かつ合理的な捜査に努めているところであり、原案のとおりとさせていただきます。御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。
6	12	法人・団体 （㈱シマンテック）	35	「国際標準化」の文言の後に「活動におけるイニシアティブとリーダーシップを発揮することを積極的に支援するとともに」を追加挿入。 国際標準化において我が国発の技術を入れ込んでいくことや意見を反映させることは、国際競争力や国際貢献の観点から極めて重要である。一方、国際標準化活動におけるイニシアティブやリーダーシップの発揮には、国際会議への参加、技術文書等の作成や国際間の調整、各国委員等との人的交流等、人的・経済的負担が極めて大きい。そのための活動は民間企業等に大きく依存するところであるが、企業等の利益管理の視点からはそこへの十分な資源・予算の投入は困難であり、国際標準化活動に携わる人たちは様々な制約のもとで大きな苦労や犠牲を払いつつ活動しているのが実情である。 我が国の国際競争力、国際的なステータスの確保、国際貢献の視点からは、この面に関する政府の積極的な関与や財政的支援が不可欠である。そのことを明示的に認識し、共有し、政策対象として位置づけられるべきである。	ご趣旨を踏まえ、修文いたします。
6	13	法人・団体 （㈱シマンテック）	39	「検討を進める」と「。」の間に「とともに我が国からも望ましい適用の形態を提唱する」を追加挿入。 国際法の適用は、その適用の在り方が主要国の意見で決められているというのが現状である。しかし、その適用の影響は非常に大きい。従って、我が国としての立場を明確にして意見を表明することで、「決まったことに従う」のではなく「従いやすいこと、および、従うと我が国にとって有利となる形に決める」ことが重要である。	ご指摘の内容については、例えば、P39において「国際的なルールづくりへの積極的な参画」として記載しているところであり、原案のとおりとさせていただきます。
6	14	法人・団体 （㈱シマンテック）	41	「検討する」と「。」の間に「とともに主導的な立場で国際ルールの在り方を提唱する。」を追加挿入。 国際ルールは国際法と同様に、その在り方が主要国の意見で決められているというのが現状である。しかし、その適用の影響は非常に大きい。従って、我が国としての立場を明確にして意見を表明することで、「決まったことに従う」のではなく「従いやすいこと、および、従うと我が国にとって有利となる形に決める」ことが重要である。	ご指摘の内容については、例えば、P39において「国際的なルールづくりへの積極的な参画」として記載しているところであり、原案のとおりとさせていただきます。

46者　　174件

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	15	法人・団体（㈱シマンテック）	34	「～行う。」の一文の後に、「また、従来の防衛、警察、民間の安全対策組織との連携を統合運用・一体運用を前提に検討する。」の一文を追加挿入。 サイバー攻撃が実世界に影響を及ぼしている現状を踏まえると、従来の防衛、警察との連携は必須であるとともに、制御システムへの攻撃を鑑みると従来の安全対策組織との連携も必要である。	非常時における関係機関の役割については、ご指摘の内容を前提にするか否かにかかわらず、整理するものと考えておりますので、原案のとおりとさせて頂きます。
6	16	法人・団体（㈱シマンテック）	42	「NISCについては、」の後に「トップを政府CISOと位置付けて、」の文言を追加挿入。 諸外国の事例を鑑みても、政府CIOと同様に、情報セキュティを統括する政府CISOが必要である。	現在においても、内閣官房情報セキュリティセンター長については、政府CISOと位置付けられているところであり、原案のとおりとさせていただきます。
6	17	法人・団体（㈱シマンテック）	36	「半導体素子」の後に「や通信プロトコル、符号化・暗号化の方式」の文言を追加。情報セキュリティはハードウェアの身で成立するものではなく、ソフトウェアに拠る部分も多い。また、これらの基盤技術を自国で開発して、それを国際標準とすることが、我が国のセキュリティの強化につながり、延いては産業競争力の強化にもつながる。	ご指摘の内容については、P.34において、「匿名化・暗号技術、多種多量のデータについてソフトウェアによりネットワーク全体を制御する技術（略）に関する研究開発」等を記載しているところであり、原案のとおりとさせていただきます。
6	18	法人・団体（㈱シマンテック）	20	「具体的には、」の後に「クラウドコンピューティングやホスティングサービスを提供するデータセンター、」をの文言を挿入。 クラウド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。現状の定義では「情報通信」にはクラウドやデータセンターが含まれていないと理解しており、前後の文脈から、ここにそれを補うことで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と考える。 参考：http://www.ipa.go.jp/about/press/20120928.html	ご指摘のクラウドやデータセンターについては、情報システムや情報通信ネットワーク等により構成されるサイバー空間を構成するものと考えており、原案のとおりとさせて頂きます。
7	1	法人・団体（（一社）情報処理学会）	－	本戦略案に示された取組方針には大きな異論はなく、日本版NCFTAの設立等を通じて、セキュリティ戦略が前進することに期待致します。 しかし、個々の論点については、その表現の仕方も含めて検討の余地があるものと思われますので、以下のとおり意見を表明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。

46者　　174件

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	2	法人・団体 （(一社)情報処理学会）	16	「目指すべき社会像」の項を立て、セキュリティが自己目的化しないように情報セキュリティで守るべきものを明確にした点に共感を覚えるものです。但し、サイバー空間は文化を育み、多様な人と社会との間の相互理解を醸成し、時には匿名のつぶやきも受け止め、対抗言論を促す変化と包容力に富んだメディアですので、これらの点にも配慮した社会像の議論が望まれます。 また、セキュリティ戦略についてプロアクティブな取組姿勢を明示し、社会全体でリスクを機会に転換する攻めの姿勢を明らかにした点が評価できます。しかし、情報セキュリティの確保には、地道な啓発教育・技術開発の努力が必要であり、我が国の成長戦略（サイバーセキュリティ立国）の一つにすることができるかどうかはについては慎重な議論が必要と考えます。	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。
7	4	法人・団体 （(一社)情報処理学会）	17	総論としては賛成でき、インシデントの解析機能の向上は重要な課題ですが、解析を重視するあまり、「通信の秘密」「プライバシー」等への影響を軽視しないよう慎重に検討することを希望します。	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	5	法人・団体 （(一社)情報処理学会）	31	CCC については、2011年3月に終了した後、今後はどの様な形でこのような取り組みを継承してくのかの姿勢が不明瞭となっています。CCCに関するWebページ（https://www.ccc.go.jp/ccc/index.html ）では、ページ作成中のステータスのまま長く更新されておらず、一部機能（ハニーポット）を継承したとみられるCCC運営連絡会（一般財団法人日本データ通信協会 テレコム・アイザック推進会議・一般社団法人JPCERTコーディネーションセンター・独立行政法人情報処理推進機構）はみられるものの、例えば、その他の機能がどのように継承されたか分かりにくい状況となっています。CCCには一定の効果があったと考えられますが、その効果を検証し、有意義な機能については、発展的継承を行うなど、セキュリティへの取組に間隙が生じてはならないと考えます。	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	6	法人・団体 （(一社)情報処理学会）	32	通信履歴の保存については、サイバー犯罪条約の批准に際して議論されたことを踏まえて、丁寧な検討が必要と考えられます。現在、技術革新等を経て、セキュリティ上有効な通信履歴の範囲が拡大し、あるいは通信事業者等の負担軽減策に変化が認められるのであれば、新たな技術的知見等を踏まえて再検討する価値はあるものの、費用対効果の期待できない施策を強行することのないように十分な検討を重ねることを希望します。	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。

46者　　174件

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	7	法人・団体 （(一社)情報処理学会）	35	（1） リバースエンジニアリングと著作権法 　セキュリティ目的のプログラムのリバースエンジニアリングは、米国のフェアユース規定、英国のフェアディーリング規定等に照らし、現時点でも適法であると考えられます。しかし、現行著作権法第30条の4(技術の開発又は実用化のための試験の用に供するための利用)、第47条の7(情報解析のための複製等） 等の規定では、不十分な場合もあり、著作権法の適用明確化は重要な論点と考えられます。 　現行の権利制限規定(30～50条)は、対象となる行為が極めて個別具体的に限定される規定となっており、本戦略の目指すセキュリティ立国の阻害要因となることが懸念されます。 　ただし、リバースエンジアリングに伴う複製翻案等の行為が著作権侵害とならない場合をセキュリティ目的にのみ限定したのでは、その他公益性の高い著作物の利用態様について、利用者を委縮させることになるため、幅広く議論をすることが望ましいと考えられます。 （2） 個人情報の保護 　ビッグデータ解析などを阻む可能性がある規制の中には、個人情報保護法のように有益なものもあることから、規制によって実現しようとする権利利益等の保護との両立を図る視点が欠かせないものと考えます。	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。
7	8	法人・団体 （(一社)情報処理学会）	37	突出した能力を有する人材の確保にあたっては、突出した能力を伸び伸びと伸ばせる環境(try＆errorも一定程度許容する多様性を重視した教育)が必要ではないかと思われます。例えば、好奇心から行うソフトの違法ダウンロードに罰則を科すというようなことで補導される児童等がむやみに増えることは望ましくないものと考えます。	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	9	法人・団体 （(一社)情報処理学会）	－	(1)インターネット利用者の認証基盤の在り方への検討 　現在のインターネットでは、フリーのアカウントが多量に普及し，虚偽のアカウントの作成やそれらを使った不正行為についての問題が生じています。ビッグデータが注目されれば、それらの行為は今後より深刻になることも懸念されます。おりしも共通番号法が成立し、利用者の認証基盤についてはどの様な形が望ましいのか議論するタイミングではないかと思われます。 (2)デジタル機会均等を目指して 　ICTの利活用が困難な高齢者等は、よりセキュリティ上のリスクに晒されることが多くなることから、安全・安心にICTを活用できるという意味も含めたデジタル機会均等を再考することも必要と考えられます。	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。

46者　　174件

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（情報セキュリティ大学院大学）	19	「積極的に行う」となっているが、「人材レベルに応じた中長期的戦略と実行計画のもと着実に実施する」のように踏み込んだ表現とすべきである。 セキュリティ人材の育成といっても、技術レベルの異なる人材像に対する幅広い育成が求められており、対象とする人材レベルごとに必要とされる教育内容や手法が異なる。人材レベルに応じた中長期的戦略と具体的な実行計画が必要であり、着実な実施が求められるため。	ご指摘の内容については、本戦略を踏まえて改訂予定の「情報セキュリティ人材育成プログラム」の中で、明確化する予定となっています。
8	2	法人・団体（情報セキュリティ大学院大学）	23	「目指すものとする」となっているが、「目指し、そのために必要な具体策と予算措置を講じる」のように踏み込んだ記述とすべきである。 目標値は掲げられているが、目標達成に必要な具体策や予算措置については触れ られておらず、その実効性に疑問が残る。人材育成は、中長期的な戦略のもと着実に実施されることが重要であり、国が具体的な実行計画を示し、安定的な支援・先導を行うことが求められている。	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頂きます。
8	3	法人・団体（情報セキュリティ大学院大学）	23	単なる「見直し」と「計画等を策定」ではなく、「「情報セキュリティ人材育成プログラム」及び「情報セキュリティ普及啓発プログラム」等を強化して実行し、その評価を通してプログラムを見直し、更に強化した計画等を策定する。」とすべきである。 「情報セキュリティ人材育成プログラム」は2011年からの3年間を対象としているが、人材育成は一朝一夕では為しえず中長期的課題であるため、その視点も盛り込まれおり、様々な重要な取組みについて述べられている。今、必要なことは「プログラムの見直し」ではなく、「人材育成プログラムの実行と強化」である。まずきちんと実行されているかをチェックし、実行されていない重要な取組みについては即時実行した上で、プログラムの評価・改善を行うべきである。	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頂きます。
8	3	法人・団体（(一社)情報処理学会）	17	リスクの甚大化、拡散化及びグローバル化は、戦略案がまさに指摘する通りといえます。しかし、「これまでの戦略で講じてきた様々な取組の延長」では本当に十分に対応できないのか、これまでの取組で何が足りないのか、具体的に評価し、検証結果を踏まえて戦略を個別具体的に立案することが必要ではないでしょうか。	本戦略は、これまでの年次計画の評価や現状等を踏まえ、今後の大きな方向性としてとりまとめたものです。より具体的な評価や検証についきましては、今後の年次計画の策定やその評価等により実施していくこととしております。
8	4	法人・団体（情報セキュリティ大学院大学）	36	「検討を行う」となっているが、情報セキュリティ人材が払底している現状を鑑みると、「具体策を至急実施する」のようにすべきである。 情報セキュリティ人材の育成に関する検討については既に相当数の蓄積があり、新たな検討を行う必要性よりも既存の検討における提言を確実に実行する必要性のほうが高いため。また情報セキュリティ対策を講じるために種々のプログラムを立てたり、政府内に専門組織や協議会を作ったりする取り組みはあるが、それに従事する人材そのものが不足しており、その取り組みが空洞化する懸念が強くあるため。	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頂きます。

46者　　174件

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	5	法人・団体（情報セキュリティ大学院大学）	32	単に「強化する」となっているが、「新たな予算によって強化する」のように記述すべきである。 サイバー空間の犯罪対策の強化体制は、新規（追加）予算で実施すべきである。内部での予算の振分のみでは、検察や警察分野における組織内部での優先度の評価に従った調整により、実質的に必要な額より予算額が大幅に少なくなる懸念があるため。	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頂きます。
8	6	法人・団体（情報セキュリティ大学院大学）	33	単に「強化する」となっているが、「新たな予算によって強化する」のように記述すべきである。 サイバー空間の防衛強化については、新規（追加）予算で実施すべきである。内部での予算・人員の振分のみでは、自衛隊における組織内部での優先度の評価に従った調整により、実質的に必要な額より予算額が大幅に少なくなる懸念があるため。	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頂きます。
8	7	法人・団体（情報セキュリティ大学院大学）	36	「海外の専門的な大学院等」と海外に限定した記述となっているが、国内も対象とするよう「国内外の」とすべきである。 グローバルに活躍できる人材育成のために、海外の専門的な大学院等への留学を支援することは重要なことではあるが、国内にも高度セキュリティ人材を育成できる専門的な大学院等があり、そちらの大学院においてもグローバルに活躍する教育者による指導や国際的な学会への参加等により、グローバルに活躍できる人材の育成することは可能であるため。	ご指摘の内容については、「実践的な教育プログラム等に関する大学等専門教育課程の充実化」等と記載しており、原案のとおりとさせていただきます。
9	1	法人・団体（（一社）新経済連盟）	31	「今後、マルウェアを配布する等の悪性サイト情報を蓄積するデータベースを構築し、悪性サイトにアクセスしようとする一般利用者に対する注意喚起等を、ISP等により実施するための仕組みを構築し、悪性サイトの検知機能の強化などデータベースの機能の高度化を推進する」とあります。当該仕組みの構築に当たっては、各事業者の既存のシステムの自由度を妨げないあり方を確保すべきであり、その観点からISP等事業者の意見を十分取り入れる枠組みが重要です。	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。
9	2	法人・団体（（一社）新経済連盟）	32	「サイバー犯罪に対する事後追跡可能性を確保するため、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について検討する」との記述があります。これに関しては、事業者に過度の負担を課す可能性があるとともに、自由な情報流通への妨げになるおそれがあるため、その具体的な導入には慎重な議論が求められるべきです。	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。

46者　　174件

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
9	3	法人・団体 （（一社）新経済連盟）	33	「サイバー攻撃の主体の特定に資する平素からの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。共有や高度な解析等に関する関係機関の役割の明確化及び体制等の強化とともに、それらの機関間の連携を強化する」とあります。これについては、サイバー攻撃対策との名目で国民の自由な情報アクセスへの不当な介入。制限や委縮効果を生じることがないようバランスを取ることが必要不可欠です	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。
10	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㈱）	18	本項目においては、「各主体の役割」が規定されていますが、対処すべき対策や想定される攻撃等は「サービス」や「重要度」、「社会に対する責任」等によって変わってくるものと理解しています。従って、主体ごとに一つのルールを適用するのではなく、保護する対象に応じた適正な対処が可能となるよう、優先順位や対処レベル等の整理を行うべきと考えます。 また、情報通信産業は、今後多くの新規事業者の参入も期待される分野であることから、過度な負荷・コスト負担を強いることのないよう配慮が必要と考えます。 ブロードバンド環境が普及している日本においては、多様な分野においてICTが活用されおり、今後も更なる発展が見込まれます。そのような環境下においては、情報システムや情報通信ネットワーク等のセキュリティを確保し、経済の発展、国民の安全・安心確保を実施してくことは非常に重要なことと理解しています。また、通信事業者として安心・安全のために日々努力をしているところです。 しかしながら、情報システムや情報通信ネットワーク等は、スマートデバイス、M2M・センサーネットワーク、クラウドコンピューティングサービス等と多種多様であり、その活用先も電子商取引、医療、教育、交通、社会インフラ管理、行政等の多様な分野に及びます。 その機能と分野によって対処すべき対策や想定される攻撃等は異なるものと考えられることから、その特性に応じ、適宜適切に対応することが重要と考えます。 サイバーセキュリティ戦略（案）に記載があるように、サイバー産業の活性化を行っていくには、新規事業者の参入が必要です。従って、事業者に過度の負荷・負担を強いることがないよう、例えば、最低限必要な基準等を策定し、追加処置はオプション方式とするような方法も一案と考えます。	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。
10	2	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㈱）	17	各主体のCSIRT間の連携や国際的なCSIRT間連携の強化等について賛同します。	各主体のCSIRT間の連携や国際的なCSIRT間連携の強化等に取り組んでまいります。

46者　　174件

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	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㈱）	26	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。併せて、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ついては、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。 例）事業者と利用機器、請負業務、費用等の特定や関係性がわからないようにすること	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	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㈱）	26	国における収集したインシデント情報や攻撃手法の分析結果等について、重要インフラ事業者等の関係機関と共有するための仕組みも整備することに賛同します。 前述した通り、情報共有に当たっては事業者が特定できないよう匿名化を実施徹底すべきと考えます。 事業者単位での対策では収集可能な情報数や対策に限界も考えられ、各種情報及び対策について、共有化を図ることは望ましいと考えます。 また、前述の通り匿名化は必須と考えます。	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。
10	5	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㈱）	28	前述の通り 、重要インフラ事業者においても多様なサービスやシステムを保有していると考えられることから、一様に「重要インフラ事業者等」のセキュリティ対策を検討するのでなく、サービス等の特性に準じて優先順位や対処レベル等の整理を行うべきと考えます。	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。

46者　　174件

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	6	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㈱）	28	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。 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。 但し、個人情報や通信の秘密については、違法性阻却事由となる基準を国が定めて頂くことが必要と考えます。 事業者判断で実施した場合、基準がまちまちとなり、収集情報が情報価値として低下する懸念があります	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。
10	7	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㈱）	28	標準化等を推進することで、対策・運用等の効率化が図ることは重要なことと理解しますが、評価・認証を導入することにより自由競争が阻害されることのないように考慮することが必要と考えます。 事業者は、各社の努力によりシステム構築や機器等の調達・運用を実施し、競争を実施しているところです。評価・認証基準を厳格化することで、競争原則が働かなくなる可能性を危惧します。	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。
10	8	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㈱）	29	有価証券報告書等に記載する「事業等のリスク」に、サイバー攻撃に対するインシデントの可能性等の記載を検討される場合は、有価証券報告書の所管である金融庁殿と協議の上、進めて頂きたいと考えます。 有価証券報告書の記載要領は、企業内容等の開示に関する内閣府令第三号様式にて定めているため、本様式の手当てが必要と考えます	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。
10	9	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㈱）	31	一般利用者に対する注意喚起については、事業者も日々努力をしていますが、注意喚起の仕組みに関しては、事業者のみではなく、官民一体となって推進していくことが必要と考えます。例えば、対処の判断基準等において、事業者判断が困難である場合、公的機関により判断を行う等の体制が考えられます。 また、国民全体のリテラシー向上が必須となることから、学校においての教育や高齢者においては、自治体の指導・案内等も必要と考えます。 事業者のみで推進を行う場合、対応判断等の基準に差分が発生し、利用者の理解度の差分や混乱が生じてしまう懸念等があります	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。

46者　　174件

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	10	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㈱）	32	前述の通り、情報共有に当たっては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、国民全体のリテラシー向上が必須となることから、学校においての教育や高齢者においては、自治体の指導・案内等も必要と考えます。	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。
10	11	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㈱）	31	「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。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の整備のステップを踏む必要があると考えます。 また、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。 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いう考え方が必要です。 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ると考えています。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。 従って、検討を実施するにあたり、「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し、把握した上で検討頂きたいと考えます。	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。
10	12	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㈱）	38	「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。

46者　　174件

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	法人・団体 （（一社）テレコムサービス協会）	31	原案の趣旨に賛同します。最新の通信技術の動向等を踏まえ、通信の秘密の保護を含む電気通信事業法など関係法令との整理などがこれを機会に行われることになると思いますが、その際には、解釈基準など明確にしていただくことを希望します。ISP等の電気通信事業者は、以前から「インターネットの安定的な運用に関する協議会」が策定した、「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」に基づき、サイバー攻撃等に対処し、情報セキュリティの確保に取り組んでいます。ただし、当該ガイドラインは、現にサイバー攻撃等が起きている場合と平時のそれぞれの事例別に、「通信の秘密の侵害に該当しうるのか否か、また、通信の秘密の侵害に該当したとしても、違法性が阻却されうるのか否かについて、基本的な考え方を整理すると共に、該当する事例を挙げることにより、電気通信事業者における大量通信等への対処の参考に資するもの」であるため、事例に該当しない場合には個別判断が余儀なくされています。本提案に基づき当該ガイドラインの事例を増やす等ガイドラインの内容を充実させ、より明確化された解釈基準を参照するなどして柔軟な運用を図ることにより、ISP等の電気通信事業者がより機動的にサイバー攻撃への対処に必要な通信解析等が実施できる範囲がより明確になれば、日本のインターネットセキュリティ環境の向上に資するものと考えます。 今日サイバー攻撃の手法は日々進化しますが、ISP事業者による通信解析が技術的には可能であっても電気通信事業法など関係法令との関係でグレーであるリスクを伴うため、機動的な通信解析を控えている可能性がありますが、ガイドラインの充実、このような対策に関する解釈が明確化されることにより、日本のインターネットセキュリティ環境の向上に資することができると考えております。	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。

46者　　174件

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	2	法人・団体 （(一社)テレコムサービス協会）	32	通信履歴等に関するログの保存の義務化ありきの検討については反対します。保存対象となるログの種類が増え、保存期間が長期化すればするほどについては、当然ながら事後追跡可能性は大きくなりますが、一方で、一般利用者としての国民のプライバシーや通信の秘密の確保をより危うくします。また、ログの保存にかかる設備の投資、維持及び保存したログのセキュリティの確保および必要な記録を抽出する作業にかかる事業者の負担も多大です。現在、事業者は、自身のサービスやそのセキュリティを確保するために必要な期間を定めログを保存していますが、その期間やログの種類により、どれほどの事後追跡可能性が不足しているのかについて科学的に分析・調査されているとは言えない状況です。 また、海外のログ保存制度の状況を参考とする場合にも、事後追跡可能性の確保と、国民の通信の秘密やプライバシー、事業者のコスト増についてどのようにバランスさせるべく制度設計しているのかについて詳細に調査する必要があると考えます。その上で、ログの保存の制度化を検討するということであれば、①憲法上の通信の秘密や表現の自由、電気通信事業法上の通信の秘密や国民のプライバシー侵害②事業者規制や刑事司法制度等、既存の法制度との整理が可能かどうか③必要なログの種類や保存する期間の拡大による事業者のコスト増およびその消費者への転嫁などが論点となりますので、関係者から多様な意見等を集約・勘案したうえ、慎重な議論が必要と考えます。 現在は、ログの保存については特に法的義務は存在しておらず、事業者が自己の業務に必要な範囲内で必要な限度において保存しています。犯罪捜査への協力を惜しむものではありませんが、事後追跡性の確保のために、事業者の業務に必要な範囲を超え犯罪捜査のために ログを保存することを義務化するのは、従来の法的枠組みとは全く異なるものとなります。事業者の負担増大もさることながら、憲法上の通信の秘密や表現の自由など憲法 上の論点および電気通信事業法上保護されている国民の通信の秘密やプライバシーが侵害されるリスクが増大することについて国民に受忍を強いるものですので、その効果の科学的分析の上で、慎重な議論と国民の理解が必要であると考えます。	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。
12	1	法人・団体 （(一社)電子情報技術産業協会）	－	セキュリティ対策は事業主体たる民間における常日頃の自主的な取り組みが基本となるため。国に対しては、官内体制の一本化・集約化を図りリソースを有効活用した上で、一企業では対処しきれない複雑化したサイバー攻撃に対抗できるよう、モニタリング・分析機能の強化を期待したい。	本戦略に掲げられている各施策を着実に推進してまいります。
12	2	法人・団体 （(一社)電子情報技術産業協会）	21	「必要に応じて」の意味が不明であり、また、第三者機関による評価・監査やマネジメント標準を取得していないことが事業者にとっては不利益材料となる場合もある。趣旨が明確になるように記述頂きたい。	ご指摘の箇所については、各々の主体の自主的な判断により標準を取得する等を意味するものです。なお、ご指摘をふまえ、当該箇所については削除させていただきます。

46者　　174件

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
12	3	法人・団体 ((一社)電子情報技術産業協会)	24	金融庁が金融機関に対して情報セキュリティ対策のガイドラインを策定し、これに対する適合化を義務づけているように、金融以外の企業に対しても重要インフラ取扱い等、一定レベルの対象に対しては、対策実施レベルの明確化と義務化が必要。	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	4	法人・団体 ((一社)電子情報技術産業協会)	27	CSIRT要員及びCYMAT要員の育成等の強化に加え、政府職員に対してはサイバー攻撃に対処するため、以下の情報セキュリティ教育が必要。 ・定期的な情報セキュリティ教育及び教育内容の理解度を確認するテストの実施。 ・各府省庁職員にとって最低限必要な情報セキュリティ知識については、全府省庁職員に対して共通なプログラムによる教育を実施。 情報漏洩等を未然に防ぐため、機密性の高い情報を扱う政府職員への教育が重要。	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。
12	5	法人・団体 ((一社)電子情報技術産業協会)	28	「重要インフラ事業者」、「現行10分野と同等にその情報システムの障害が国民生活及び社会経済活動に多大な影響を及ぼす恐れのある分野」、「サイバー空間関連事業者」について、具体的にどの業態が含まれるかを明確にするとともに、いたずらにその範囲を拡大し、仮にも負担を課すようなことは避けるべきである。また、複数の官庁が事業者に対して個別に説明を求めることは著しい負担となるため、インシデント報告の窓口を一つに定めるべきである。	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。
12	6	法人・団体 ((一社)電子情報技術産業協会)	29	企業におけるサイバーセキュリティに関わる投資について、それぞれの企業は自らの組織や製品・サービス開発・提供のために継続して対策を進めている。最近のサイバーセキュリティの変化を受けて、さらに関連の対策を講じる事が必要となる。 国、関係機関でのサイバーセキュリティ対策の情報を企業などにより具体的にかつタイムリーに提供することにより、企業などで効率的に対策が推進できるようにすることが必要。	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。
12	7	法人・団体 ((一社)電子情報技術産業協会)	31	情報家電・医療機器等の組込みソフトウェアの脆弱性対応に関する制度化の検討がされているが、過度な規制によりイノベーションを阻害しないよう、配慮願いたい。	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	8	法人・団体 ((一社)電子情報技術産業協会)	32	大半を占める海外からのサイバー攻撃者に対して、国際連携もさることながら罰則適用が可能となるようにすることが必要。	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。
12	9	法人・団体 ((一社)電子情報技術産業協会)	32	サイバー犯罪に対する法整備(国内法、国際法を含む)は急務として行って頂きたいが、被害者となった事業体・企業に対しいて不利益を課すことのない内容とすべき。	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。

46者　　174件

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
12	10	法人・団体 （(一社)電子情報技術産業協会）	35	日本企業を優遇する趣旨の記述は、政府の公式な文書にはふさわしくないと考える。公平・公正な競争環境を整備するため、国としても国際的な枠組み作りに積極的に関与する、という姿勢を堅持すべき。 （原案） 「国際標準化や評価・認証、情報セキュリティ監査の重要性が増してくると考えられる。このため、国際貿易において日本企業が有利になるよう、国際標準化や評価・認証の国際的な相互承認枠組み作りに関して、積極的に参画・働きかけを進めるとともに、」 （修正意見） 「国際標準化や評価・認証、情報セキュリティ監査の重要性が増してくると考えられる。このため、国際貿易において日本企業が不利益を被ることのないよう、国を挙げて国際標準化や評価・認証の国際的な相互承認等の枠組み作りに積極的に参画・働きかけるとともに、」	ご趣旨を踏まえ修文させて頂きます。
12	11	法人・団体 （(一社)電子情報技術産業協会）	37	国民全体へのリテラシー向上への取り組みについて、サイバー空間が個人、家庭、職場、公共施設など、実空間における日常生活や社会経済活動等のあらゆる活動により深く浸透していく。国民一人一人がより良い活用を通じて、利点を教授できるように、リテラシー向上への地道な活動を国が中心となり推進すべき。	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。
13	1	法人・団体 （日本アイ・ビー・エム㈱）	25	ご趣旨に賛同します。 政府共通プラットフォームのクラウド化等を通じたサイバー攻撃や大規模災害に強い政府情報システム基盤構築に向けて、直ちに利用可能で先進的なプラットフォーム・テクノロジー、クラウド基盤構築テクノロジー、知見、経験が必要と考えます。 先進的な製品テクノロジーには、直ぐに利用可能なものも少なくありません。これら製品を、政府の知見、経験と組み合わせることにより、最新のサイバー攻撃や大規模災害にも網羅的に対応できるほか、これら攻撃にも強い政府情報システム基盤構築に役立つと考えます	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。

46者　　174件

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
13	2	法人・団体 （日本アイ・ ビー・エム㈱）	26	ご趣旨に賛同します。 「サイバー攻撃への対処態勢の充実・強化」におきましては、国内の知見はもとより、グローバルレベルの知見をご活用されると共に、その充実・強化の深さやスピードアップも極めて重要です。 インシデントの分析、監視、共有に加えて、さらなる対応手順の整備が必要と考えます。また、GSOCの持つべき機能として、監視対象のリアルタイム（即時）、短時間での解析を可能とする機能とともに、迅速に対応できる体制作りも必要と思われます。 サイバーセキュリティに迅速に対応するために、既に利用可能な世界最高水準のサイバー・セキュリティ運用サービスおよびそれを支えるSOCテクノロジー、知見、経験が利用でき、これらはGSOCの抜本的強化に役立つと考えます。 セキュリティ・インシデントに対しては、単に分析、監視、共有のみならず、対応策（時系列の分析、侵入ルート分析、感染範囲分析、データ流出分析、事後対策、対応手順、対応体制)の策定、およびその定期的な運用訓練実施、さらに継続的拡充が必要です。 サイバー攻撃は、周到に用意され、長い時間をかけて処理が行われるものもあります。高度な分析をできる限りリアルタイム（即時）で行うことで、侵入の痕跡、あるいは攻撃の予兆を検知し、迅速に意思決定を行うことで、被害を最小化し、後の対策に繋げることができると考えます	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。
13	3	法人・団体 （日本アイ・ ビー・エム㈱）	29	ご趣旨に賛同します。 中小企業に関しては、大企業が持つ人材やスキルとの格差が大きいのが現状であり、ここに指摘されている「情報提供・相談体制の整備」は官民協業で取り組む高優先度のものと考えます。 また、セキュリティ投資に関しても大企業の規模には至らないため、税制面のみならず公的な投資による技術的な対策を何らかの形で行うことも必要と考えます。その意味で「情報セキュリティが確保された共同利用システムへの移行促進等」は是非実現されるべき項目かと思います。 サイバーの世界では、企業の大小は関係なく、むしろ対策が甘いシステムから狙われ、踏み台等の攻撃の道具になるケースも多く見られます。その結果、関連の大企業や公的機関も攻撃の被害を受けるということも想定され、国家的な被害が大きくなることが予想されます。	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。

46者　　174件

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
13	4	法人・団体 （日本アイ・ ビー・エム㈱）	31	ご趣旨に賛同します。 組み込みソフトウェアに関しては、障害はもとより、マルウェア混入による異常作動や乗っ取りなど社会への甚大な影響が想定されるため、このような対象は喫緊の課題となりつつあると思います。 現在では開発段階でのバグや脆弱性への対応を進めていますが、ネットワーク接続の機器やパーソナルデータを取り扱う機器（組み込みソフトウェア）にフォーカスした対処も必要です。 現行サイバーの攻撃対象がサーバーなどのシステム機器に特化したものになっていますが、今後は車の制御系やネットワークに接続した家電（電子レンジやエアコン）などもその対象となることが予想されます。これらの機器は制御情報のみならずパーソナルデータ（車の位置情報など）をもつ可能性もあり、データ破壊やデータ流出の両方のリスクが懸念されます	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。
13	5	法人・団体 （日本アイ・ ビー・エム㈱）	32	ご趣旨に賛同します。 政府としての対応に加え、グローバルリスクの観点から、国内外の信頼のおける研究機関、民間事業者の知見を活用することが肝要であると思われます。 サイバー空間は、国土や組織を超えて存在するものであり、特にグローバルな見地からの戦略や施策が大事になります。平時からの信頼関係に基づいて、国および国をまたがる対処態勢を強化することが必要であると考えます	ご指摘の内容については、今後の施策の推進に当たっての参考とさせていただきます。
13	6	法人・団体 （日本アイ・ ビー・エム㈱）	32	ご趣旨に賛同します。 ログは確固たる証拠となるものであり、ログが正確に保存されている限り、問題の特定につながるため、保存期間や取得べき対象ログに関するガイドが必要かと考えます。 特にログの保存期間について、民間企業の過度な負担にならないようにご配慮いただたくお願いいたします。例えば、国際犯罪条約での通信ログの保存が3ヶ月ということになっております。保存期間が伸びることは、膨大な通信ログを保管するためのスペース等が必要となることを意味し、各社の様々なシステムの運用コスト負担の増大に繋がります。 様々なセキュリティ防壁と構築したにも関わらず、問題の漏えいや、不正アクセスの影響を受ける今日、最終的な問題の痕跡および特定にはログによる判断がかかせないものと考えております。 特に、通信の履歴を通して改ざんすることのできない情報を確保することで、問題特定の解決につながるものと考えております	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。

46者　　174件

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
13	7	法人・団体 （日本アイ・ビー・エム㈱）	34	ご趣旨に賛同します。 サイバー空間の構築においては、空間を構成する要素を定義し、それらに対する脅威やリスクを共通に定義することで、研究者や技術者が共通の問題意識や対策を持つことが必要であると考えます。その中でも、サイバー空間におけるデータは、保護すべき基本的な要素であり、データ保護に対する対策やそれに伴う標準化が大事です。 リスクベースの考え方と呼応して、コンテクストに依存して変わり得るデータの価値を捉えることで、現実的な制約条件がある環境においても、必要十分な対策が適用されている状況を作り出すことが重要だと考えます。	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。
14	1	法人・団体 （（一社）日本インターネットプロバイダー協会）	31	原案の趣旨に賛同します。最新の通信技術の動向等を踏まえ、通信の秘密の保護を含む電気通信事業法など関係法令との整理などがこれを機会に行われることになると思いますが、その際には、解釈基準など明確にしていただくことを希望します。ISP等の電気通信事業者は、以前から「インターネットの安定的な運用に関する協議会」が策定した、「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」に基づき、サイバー攻撃等に対処し、情報セキュリティの確保に取り組んでいます。ただし、当該ガイドラインは、現にサイバー攻撃等が起きている場合と平時のそれぞれの事例別に、「通信の秘密の侵害に該当しうるのか否か、また、通信の秘密の侵害に該当したとしても、違法性が阻却されうるのか否かについて、基本的な考え方を整理すると共に、該当する事例を挙げることにより、電気通信事業者における大量通信等への対処の参考に資するもの」であるため、事例に該当しない場合には個別判断が余儀なくされています。本提案に基づき当該ガイドラインの事例を増やす等ガイドラインの内容を充実させ、より明確化された解釈基準を参照するなどして柔軟な運用を図ることにより、ISP等の電気通信事業者がより機動的にサイバー攻撃への対処に必要な通信解析等が実施できる範囲がより明確になれば、日本のインターネットセキュリティ環境の向上に資するものと考えます。 今日サイバー攻撃の手法は日々進化しますが、ISP事業者による通信解析が技術的には可能であっても電気通信事業法など関係法令との関係でグレーであるリスクを伴うため、機動的な通信解析を控えている可能性がありますが、ガイドラインの充実、このような対策に関する解釈が明確化されることにより、日本のインターネットセキュリティ環境の向上に資することができると考えております。	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。

46者　　174件

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	2	法人・団体 （（一社）日本インターネットプロバイダー協会）	32	通信履歴等に関するログの保存の義務化ありきの検討については反対します。保存対象となるログの種類が増え、保存期間が長期化すればするほどについては、当然ながら事後追跡可能性は大きくなりますが、一方で、一般利用者としての国民のプライバシーや通信の秘密の確保をより危うくします。また、ログの保存にかかる設備の投資、維持及び保存したログのセキュリティの確保および必要な記録を抽出する作業にかかる事業者の負担も多大です。現在、事業者は、自身のサービスやそのセキュリティを確保するために必要な期間を定めログを保存していますが、その期間やログの種類により、どれほどの事後追跡可能性が不足しているのかについて科学的に分析・調査されているとは言えない状況です。また、海外のログ保存制度の状況を参考とする場合にも、事後追跡可能性の確保と、国民の通信の秘密やプライバシー、事業者のコスト増についてどのようにバランスさせるべく制度設計しているのかについて詳細に調査する必要があると考えます。その上で、ログの保存の制度化を検討するということであれば、①憲法上の通信の秘密や表現の自由、電気通信事業法上の通信の秘密や国民のプライバシー侵害②事業者規制や刑事司法制度等、既存の法制度との整理が可能かどうか③必要なログの種類や保存する期間の拡大による事業者のコスト増およびその消費者への転嫁などが論点となりますので、関係者から多様な意見等を集約・勘案したうえ、慎重な議論が必要と考えます。 現在は、ログの保存については特に法的義務は存在しておらず、事業者が自己の業務に必要な範囲内で必要な限度において保存しています。犯罪捜査への協力を惜しむものではありませんが、事後追跡性の確保のために、事業者の業務に必要な範囲を超え犯罪捜査のために ログを保存することを義務化するのは、従来の法的枠組みとは全く異なるものとなります。 事業者の負担増大もさることながら、憲法上の通信の秘密や表現の自由など憲法上の論点および電気通信事業法上の保護されている国民の通信の秘密やプライバシーが侵害されるリスクが増大することについて国民に受忍を強いるものですので、その効果の科学的分析の上で、慎重な議論と国民の理解が必要であると考えます	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。
15	1	法人・団体 （（一社）日本士業協会）	30	自助努力しろで終わらせず、そのための啓蒙が必要 私自身が対策をとったり相談を受けたサイバー犯罪の手口やマルウェア等の挙動を見ると、Windowsからのメッセージを装ったり、ワクチンソフトを装ったりしてユーザを騙すものが大変多い。一般ユーザは画面をそのまま鵜呑みにして促されるままカード番号を入力してしまったりしている。あるいは踏み台、いや他人を攻撃する砲台にされられている。もちろん騙されたとは思っていないし、自分が他人を攻撃しているとも思っていない。 これはIT知識がないためというより、そもそも自分で自分の認識が認識できていないためと思う。ではどうしたらよいのか、自分が目で見たものをよく認識し、自分の頭で考えてみる、というマインドを持つための訓練が必要なように思われる。自助努力してね、では自分が被害者にあっていることすら認識できていない人の行動は全く変わらないと思う。	ご指摘の内容については、３（１）④により、普及啓発を図ることとしており、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。

46者　　174件

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
16	1	法人・団体 （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）	34	サイバー空間における電子的本人認証手段の重要性については言うまでもありません。たとえマルウェアやハッキングによる攻撃を根絶できたとしても、本人認証手段が脆弱であればサイバー空間が安全になったとは言えません。解読不能の暗号方式を開発しても、権限のない第三者にパスワードを推測され復号モジュールにアクセスされれば機密の漏えいが発生します。 この電子的本人認証に関してはこれまで様々な提案が行なわれてきました。『パスワードは8桁以上とし、英字・数字・特殊文字をそれぞれ1文字以上使い、意味のある語は避け、90日以内に一度変更のこと』といった、一見セキュリティを向上させるように見えても実際は一般国民にとっては無理難題に近いような運用の推奨や、「メモに記載して賢く秘匿する」「賢く使い回す」「2要素認証を利用する」「ID連携やパスワードマネジャーを利用する」「生体認証を利用する」といった対策案がよく知られています。 これらはそれぞれ特定の利用者ないし特定の利用環境においては非常に有効な方策であると考えられます。ただ、一人の人間が覚えていられるパスワードは平均3個強であるという人間の現実（注）に由来する脆弱性を抱え続けているため、何時でも、どこでも、どんな端末でも、どんな環境でも、災害時等には着の身着のままであっても、といった多様な要件を満たす包括的な解決策にはなりえていません。この根源的課題に立ち返って記憶しやすい本人認証手段の開発を図るべきと考えます。	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。
16	1	法人・団体 （（一社）日本データ通信協会テレコム・アイザック推進会議）	31	原案の趣旨に賛同します。最新の通信技術の動向等を踏まえ、通信の秘密の保護を含む電気通信事業法など関係法令との整理などがこれを機会に行われることになると思いますが、その際には、解釈基準など明確にしていただくことを希望します。 ISP等の電気通信事業者は、以前から「インターネットの安定的な運用に関する協議会」が策定した、「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」に基づき、サイバー攻撃等に対処し、情報セキュリティの確保に取り組んでいます。ただし、当該ガイドラインは、現にサイバー攻撃等が起きている場合と平時のそれぞれの事例別に、「通信の秘密の侵害に該当しうるのか否か、また、通信の秘密の侵害に該当したとしても、違法性が阻却されうるのか否かについて、基本的な考え方を整理すると共に、該当する事例を挙げることにより、電気通信事業者における大量通信等への対処の参考に資するもの」であるため、事例に該当しない場合には個別判断が余儀なくされています。本提案に基づき当該ガイドラインの事例を増やす等ガイドラインの内容を充実させ、より明確化された解釈基準を参照するなどして柔軟な運用を図ることにより、ISP等の電気通信事業者がより機動的にサイバー攻撃への対処に必要な通信解析等が実施できる範囲がより明確になれば、日本のインターネットセキュリティ環境の向上に資するものと考えます 今日サイバー攻撃の手法は日々進化しますが、ISP事業者による通信解析が技術的には可能であっても電気通信事業法など関係法令との関係でグレーであるリスクを伴うため、機動的な通信解析を控えている可能性がありますが、ガイドラインの充実、このような対策に関する解釈が明確化されることにより、日本のインターネットセキュリティ環境の向上に資することができると考えております。	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。

46者　　174件

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
16	2	法人・団体 （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）	18	自律的な取り組みを国民に要求するに当たっては高齢者も若年者も自らの身を自ら守ることが容易にできるような防衛手段が欠かせません。老若を問わずすべての国民が自分に合った電子的本人認証手段を選択できる仕組みを国や社会が提供しておくことが望ましいと考えます。 近年になり認知心理学や脳神経科学等の発達により人間のパスワード記憶容量を拡張拡大する方法があることが知られてきました。この新手法に関しては日本セキュリティ・マネジメント学会（会長：佐々木良一東京電機大学教授）では創立25周年事業の一環として2011年9月に本人認証・パスワード問題に関する『社会への提言』を発表しています。当本人認証検討会が起案を行なったもので、「文字によるパスワードが脆弱であることを踏まえ、本人にとって再認しやすい画像などを活用した電子的本人認証手法を広く利用すること」を提言し、以下のサイトに掲示しています。 http://www.jssm.net/jssm/anniver25_03.pdf この提言の趣旨に添った研究開発の強化を提言いたします。 注：　野村総研調査報告 http://www.nri.co.jp/news/2009/090611.html http://www.nri.co.jp/news/2012/120208.html （「生活者がインターネットのサービスを利用する際、「確実に記憶することができる」と思っているログインIDとパスワードの組合せの数は、2008年度と2011年度のいずれも、平均3.1個程度でした。また、IDとパスワードを使ってログインするサイト数の平均も、2008年度の19.2個に対して、2011年度は19.4個と大きな変化は見られませんでした。」と報告されている。）	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。

46者　　174件

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
16	2	法人・団体 （（一社）日本データ通信協会テレコム・アイザック推進会議）	32	通信履歴等に関するログの保存の義務化ありきの検討については反対します。保存対象となるログの種類が増え、保存期間が長期化すればするほどについては、当然ながら事後追跡可能性は大きくなりますが、一方で、一般利用者としての国民のプライバシーや通信の秘密の確保をより危うくします。また、ログの保存にかかる設備の投資、維持及び保存したログのセキュリティの確保および必要な記録を抽出する作業にかかる事業者の負担も多大です。現在、事業者は、自身のサービスやそのセキュリティを確保するために必要な期間を定めログを保存していますが、その期間やログの種類により、どれほどの事後追跡可能性が不足しているのかについて科学的に分析・調査されているとは言えない状況です。また、海外のログ保存制度の状況を参考とする場合にも、事後追跡可能性の確保と、国民の通信の秘密やプライバシー、事業者のコスト増についてどのようにバランスさせるべく制度設計しているのかについて詳細に調査する必要があると考えます。その上で、ログの保存の制度化を検討するということであれば、①憲法上の通信の秘密や表現の自由、電気通信事業法上の通信の秘密や国民のプライバシー侵害②事業者規制や刑事司法制度等、既存の法制度との整理が可能かどうか③必要なログの種類や保存する期間の拡大による事業者のコスト増およびその消費者への転嫁などが論点となりますので、関係者から多様な意見等を集約・勘案したうえ、慎重な議論が必要と考えます。 現在は、ログの保存については特に法的義務は存在しておらず、事業者が自己の業務に必要な範囲内で必要な限度において保存しています。犯罪捜査への協力を惜しむものではありませんが、事後追跡性の確保のために、事業者の業務に必要な範囲を超え犯罪捜査のために ログを保存することを義務化するのは、従来の法的枠組みとは全く異なるものとなります。事業者の負担増大もさることながら、憲法上の通信の秘密や表現の自由など憲法上の論点および電気通信事業法上の保護されている国民の通信の秘密やプライバシーが侵害されるリスクが増大することについて国民に受忍を強いるものですので、その効果の科学的分析の上で、慎重な議論と国民の理解が必要であると考えます	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。
17	1	法人・団体 （NPO日本ネットワークセキュリティ協会　社会活動部会）	10	文章の趣旨がより明確に伝わる文章表現に改良する。一例としては、 「サイバー攻撃はその手法の入手が容易であり、国家のみならず多様な主体が隠蔽や偽装等を行うことに加え、世界中から実行することが可能である。サイバー攻撃は、攻撃主体が存在する国・空間から我が国に直接行われることもあれば、他国に係るサイバー空間を経由して行われたり、更には我が国に係るサイバー空間を踏み台にして他国等に対して行われたりすることもあり得る状況となっている。また、サイバー攻撃を武力攻撃等と同等の攻撃とみなすかについては国際的に定説がない状況であるが、武力攻撃等に匹敵する脅威を持つサイバー攻撃が、我が国に対して、あるいは我が国を経由して行われる可能性も否定できない状況となっている。」などが考えられる。 現状の文章は文意がつかみにくい表現が見受けられるので、趣旨がより明確になるよう用語を補う等の改良を行うことが望ましいと考える。	ご趣旨を踏まえ、修文いたします。

46者　　174件

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
17	2	法人・団体（NPO日本ネットワークセキュリティ協会　社会活動部会）	12	「リスクの甚大化」を「脅威の甚大化」に変更する。 前後の文脈から、ここにおける用語は「リスク」より「脅威」が該当すると思われる。	環境の変化において、「甚大化するリスク」、「拡散するリスク」、「グローバルリスク」が顕著に進行していると表現していることから、ここでも同様の表現とします。
17	3	法人・団体（NPO日本ネットワークセキュリティ協会　社会活動部会）	16	「イノベーション、経済成長、社会的課題の解決」の後に「や、新ビジネスの開発など文化的・経済的付加価値の創出」を追加挿入する。 サイバー空間への自由かつ低コストのアクセスの恩恵としてネット企業等経済活性化に結びつく要素が大きく、またクールジャパンなど文化的発信にも役立っている。「イノベーション、経済成長」にこれらが含意されるとも解釈できるが、このような効果を明示的に示すことでサイバー空間の価値をより的確に表現できると考える。	ご指摘のとおり含まれており、原案のとおりとさせていただきます。
17	4	法人・団体（NPO日本ネットワークセキュリティ協会　社会活動部会）	18	「CSIRT間連携の強化」の後に「、情報システムの脆弱性の予防・早期発見・対処のための連携体制の整備強化」を追加挿入する。 サイバー攻撃はしばしばICTの脆弱性を衝くものであり、ここで述べられている受動的対応に加え、予防的・能動的対応である脆弱性への対処の項目を加えることが、この項の趣旨に照らして望ましいと考える。	ご趣旨を踏まえ、修文いたします。
17	5	法人・団体（NPO日本ネットワークセキュリティ協会　社会活動部会）	18	「ア感染」の後に「、それらが付け入る欠陥となっている脆弱性の発生」を追加挿入する。 上記（3）に同じ。なお、文脈上この個所への挿入が適当でない場合は、別途同趣旨の文章が補われることが望ましいと考える。	ご趣旨を踏まえ、修文いたします。
17	6	法人・団体（NPO日本ネットワークセキュリティ協会　社会活動部会）	20	「具体的には、」の後に「クラウドコンピューティングやホスティングサービスを提供するデータセンター、」を追加挿入する。 クラウド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。現状の定義では「情報通信」にはクラウドやデータセンターが含まれていないと理解しており、前後の文脈から、ここにそれを補うことで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と考える。参考： http://www.ipa.go.jp/about/press/20120928.html	ご指摘のクラウドやデータセンターについては、情報システムや情報通信ネットワーク等により構成されるサイバー空間を構成するものと考えており、原案のとおりとさせて頂きます。

46者　　174件

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
17	7	法人・団体（NPO日本ネットワークセキュリティ協会　社会活動部会）	22	「一般利用者等が使用する」の後に「パソコンや」を追加挿入 現状において他の主体に被害が及ぶサイバー攻撃の対象としてはパソコンがより重要であり、スマートフォン等のみに焦点が当たることを避ける意味でパソコンへの言及が必要である。	ご趣旨を踏まえ、修文いたします。
17	8	法人・団体（NPO日本ネットワークセキュリティ協会　社会活動部会）	23	「高度な技術や製品の開発や」の後に「高い能力を持った情報セキュリティ人材の育成、」を追加挿入する。 その上の行でも指摘されている通り、情報セキュリティ人材の不足も深刻な課題であり、技術や製品の開発と併せて人材育成にも言及することが、この項の目的に照らして望ましいと考える。	ご趣旨を踏まえ、修文いたします。
17	9	法人・団体（NPO日本ネットワークセキュリティ協会　社会活動部会）	25	「サプライチェーン・リスク」を「ITサプライ・リスク」に変更する。 「サプライチェーン・リスク」という用語については、ここで示されている「既知脆弱性への未対応、危殆化された技術の利用やマルウェアを埋め込まれる等」を指すという共通認識は形成されていないと考えられる。特にサプライチェーンという用語は製造業における部品・中間製品の供給連鎖構造という意味で解釈されることが一般的であると考えられ、その面のリスクという誤解が生じる恐れがあるのではないかという危惧を感じる。そこで、この項の文脈に沿った別の表現を考えたところ「ITサプライ・リスク」という用語が該当すると思われたので提案する次第である。なお、P26、P28にも同じ用語が使われているので、これらも合わせて変更されるよう提言する。	ご指摘の用語については、情報システムの設計、製造、設置等の段階においてマルウェアを埋め込まれること等をも含めて想定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。
17	10	法人・団体（NPO日本ネットワークセキュリティ協会　社会活動部会）	28	「策定・変更状況」の後に「の把握・評価」を追加挿入する。 文脈から「の把握・評価」またはそれに相当する述語が省かれていると考えられるため。	ご趣旨を踏まえ、修文いたします。

46者　　174件

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
17	11	法人・団体（NPO日本ネットワークセキュリティ協会　社会活動部会）	29	海外での企業活動における情報セキュリティ対策に言及する。文章の一案として「日本企業等の海外における企業活動は我が国経済の重要な一角を形成している。一般に一部先進国を除き進出先経済では、情報セキュリティに関する知識、経験、対策品やサービスの供給が国内に比べて不十分である。そのような中で日本の競争力の源泉である技術情報・ノウハウ等を活用して企業活動をすることは、情報の流出・盗用等のリスクに常にさらされることとなり、我が国経済にとっての潜在的脅威となっている。これに対し、海外進出先における情報セキュリティ対策が十全に行われるための環境整備や対策実施のための支援について必要な方策を検討し、充実を図る。」 等が考えられる。 上記文例に書いたとおり、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も、政府の積極的な支援や環境整備への取組が必要である。別の項で国際連携からの言及はされているが、国益保護の視点からの海外進出企業の情報防衛の視点も極めて重要であると考える。 よって本提案を行うものである。	ご趣旨を踏まえ、修文いたします。
17	12	法人・団体（NPO日本ネットワークセキュリティ協会　社会活動部会）	29	「ガイドライン・ツールの整備やクラウド技術を活用し、情報セキュリティが確保」を「ガイドライン・ツールの整備、クラウド技術の活用等により情報セキュリティが確保」に変更する。 この個所における文意を考えると、このように記述するほうが意味が正確に伝わると考える。なお文章の構成と流れから「情報セキュリティが確保された共同利用システム」はクラウド技術を活用して実現されたものとの趣旨であると理解した。	ご趣旨を踏まえ、修文いたします。
17	13	法人・団体（NPO日本ネットワークセキュリティ協会　社会活動部会）	30	「開催している。」の後に「また官民協力によるインターネット安全教室の開催等、一般利用者に対する日常的な普及啓発活動が多面的に展開されているところである。」の一文を追加する。 現在、インターネット安全教室だけでなく、総務省、警察庁、IPAにおいても一般利用者向けの普及啓発施策を展開しており、成果を上げている。そういった施策を継続展開することは有意義であると考えられ、そのことを明示する意味で、ここに上記のような一文を補うことを提案する	ご指摘の普及啓発施策については、本戦略に基づき、具体的な施策をとりまとめた年次計画において記載することととしているため、原案のとおりとさせていただきます。

46者　　174件

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
17	14	法人・団体 （NPO日本ネットワークセキュリティ協会　社会活動部会）	35	国際標準化活動におけるイニシアティブの発揮とそのための支援の必要性に言及する。文章の一案として 「我が国発の技術を国際標準として展開することは、国際競争力確保、国益や国際的発言力の確保、国際貢献の視点から重要である。そのために国際的標準化活動へのより積極的参加が望まれる。国際標準とすべき技術開発は民間の研究開発によるものが大きく、その国際標準化には民間の力の活用が欠かせない一方、その活動のための人的・経済的負担は大きい。この面での支援や環境整備のための政策・施策を充実させることにより、我が国が国際標準化の面でも一層のリーダーシップを発揮できる姿を目指す。」といった内容が考えられる。 国際標準化において我が国発の技術を入れ込んでいくことや意見を反映させることは、国際競争力や国際貢献の観点から極めて重要である。一方、国際標準化活動におけるイニシアティブやリーダーシップの発揮には、国際会議への参加、技術文書等の作成や国際間の調整、各国委員等との人的交流等、人的・経済的負担が極めて大きい。そのための活動は民間企業等に大きく依存するところであるが、企業等の利益管理の視点からはそこへの十分な資源・予算の投入は困難であり、国際標準化活動に携わる人たちは様々な制約のもとで大きな苦労や犠牲を払いつつ活動しているのが実情である。我が国の国際競争力の維持、国際的なステータスの確保、国際貢献の視点からは、この面に関する政府の積極的な関与や財政的支援が不可欠である。そのことを明示的に認識し、共有し、政策対象として位置づけられることを希望することから、この提案を行う	ご趣旨を踏まえ、修文いたします。
17	15	法人・団体 （NPO日本ネットワークセキュリティ協会　社会活動部会）	38	一般家庭や若年層への手当てに言及する一文（段落）を追加挿入する。 文案の一例として、 「これら施策に加え、職域や教育機関を通じての普及啓発の情報が届きにくい一般家庭や若年層に対する手当も重要である。既に一定の成果を上げていることを踏まえ、民間のボランタリな活力も活用しつつ、地域社会等を通じてリテラシーの浸透や新しいサイバーリスクに関する知識・情報の提供への取組を継続する。」などが考えられる。 一般家庭は主婦や高齢者が多く属する一方、特にサイバー関係の情報の提供手段が限られ、エアポケットになりやすい領域である。また児童生徒の情報セキュリティ教育のためにも一般家庭のリテラシー向上は重要である。この面では既に種々取組がおこなわれて成果を上げているが、増大するサイバー脅威やネット利用犯罪の危険を考えると、更なる継続、繰り返し教育が重要であり、そのための手当を政策として確認しておくことが不可欠であると考える	ご趣旨を踏まえ、修文いたします。

46者　　174件

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
18	1	法人・団体 (NetAgent Inc.)	21	重要インフラ事業者や先端的な技術を有する事業者等と契約関係にあることなどにより我が国の重要な情報やシステムを取り扱っている事業者（中小企業）は、その中小企業がセキュリティホールにならないように、本来運営事業者と同等程度の情報セキュリティ対策を負うべきであると言えます。一方、中小企業は、大企業に比べ、資金的な余裕はなく、情報セキュリティ対策はどうしても後手に回りがちであると言えます。そこで、国として、そのような中小企業に助成金制度などを用いて、情報セキュリティ対策の支援を積極的に行っていくべきであると考えます。	中小企業等における対策については、3（1）③において、情報セキュリティ投資を促進する税制等のインセンティブの検討を行うこととしており、ご指摘の内容について、今後の施策の検討にあたっての参考とさせて頂きます。
18	2	法人・団体 (NetAgent Inc.)	21	サイバーセキュリティ産業の育成、サイバーセキュリティ分野において国際競争力を持つ企業・ベンチャー企業の育成は、たいへん重要であり、国として積極的な支援を行う仕組みをぜひ構築していただきたいと考えます。また、サイバーセキュリティ分野におけるベンチャー企業、中小企業が海外市場へ進出する際、その進出、市場開拓を後押しするような助成金制度などの支援プログラムを用意する必要があると考えます。	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。
19	1	法人・団体 （富士通㈱）	－	今回の戦略案は、政府や民間企業へのサイバー攻撃の脅威が現実化していることから、経済や国民の安全・安定を図るため、またこの取組みを成長につなげるため、たいへん時宜を得たものと考えます。戦略として決定し、政府の各府省庁や民間企業がそれぞれの役割を全うし、各取組みが着実に実行されることを望みます	本戦略に掲げられている各施策を着実に推進してまいります。
19	1	法人・団体 （ヤフー㈱）	28	・国が集約すべきものと競争に委ねるものを峻別する必要があることに留意いただきたい。 ・報告に関して「セキュリティリスクへの対応を最優先にしつつ対応する」旨、加筆いただきたい。 ・基本的には競争原理の下でセキュリティベンダーが切磋琢磨していく分野と思料しますので、その競争がもたらす効用を阻害しない範囲で、国が関与すべきであると考えます。 ・インシデント発生時の限られた人的リソースを報告それ自体に費やすことによって、被害の拡大を招来しないようにする必要があると考えます。	重要インフラ事業者等からの所管省庁等への情報連絡については、「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」において、サイバー攻撃をはじめとする意図的要因によるIT障害や、非意図的要因によるIT障害、災害や疾病によるIT障害が発生した場合等とされており、原案のとおりとさせていただきます。
19	2	法人・団体 （富士通㈱）	24	CSIRT要員及びCYMAT要員の育成に加え、政府職員のサイバー教育について以下の内容を追記するのが望ましいと考えます。 ・定期的な情報セキュリティ教育及び研修内容の理解度を確認するテストの実施などの情報セキュリティ教育の徹底・強化 ・各府省庁の職員にとって最低限必要な情報セキュリティに知識については、恒常的に全府省庁員に対して共通なプログラムを実施するような横断的な取組み 情報漏洩等を未然に防ぐため、機密性の高い情報を扱う政府職員への教育が重要と考えるため。	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。

46者　　174件

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
19	3	法人・団体 （富士通㈱）	35	研究開発については、官民協議の上で優先事項を決定し、各主体の知見を効果的に活かせる役割分担のもとで実施することが望ましいと考えます。また、研究開発に関して盛り込むべき対象として、戦略案に例示されたものに追加して生体情報を活用した認証技術の研究開発を促進することを希望いたします。 サイバー空間に関わる主体や防護対象となる情報システム等が多岐に渡り、政府機関や企業等の関係機関が情報共有を図りつつ、実施すべき研究開発を決定することが重要と考えるため。 遠隔操作ウイルスによる不正ログインの事例等により、サイバー空間上の本人確認技術に関する研究開発の強化が望まれている。生体情報を活用した認証は、利用者本人を特定するという特性から端末のウイルス感染による認証情報流出への対策として有効なものであり、また、スマートフォンの認証方式としても、利活用が期待されるものであるため。	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。
20	2	法人・団体 （ヤフー㈱）	32	ログの保存を義務化することについては、通信の秘密と密接にかかわる分野でありますので、慎重な議論を行っていただきたい。 仮にログを犯罪捜査のために保存するとの結論に至ったとしても、どのくらいの期間、どういったサービスのどういった情報について保存をしておくのか、詳細な議論・定義を行っていただきたい。 国民（利用者）や対象となる事業者が混乱しないように、慎重な議論が必要と思料します。	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。
20	3	法人・団体 （ヤフー㈱）	41	早期に拡大を図っていただき、具体的な目標を掲げて連携の強化をお願いしたい。 インターネットに関する施策を検討する際は、常に、問題点の統計的分析とエンフォースメントの実行可能性をベースにした議論が為される必要があります。この点、これまでの事件捜査において追跡を断念せざるを得なかった理由は、国内でのログ保存の問題だけではなく、協力関係のない外国から加害行為が行われていることに起因する場合も相当割合存在すると思料されますので、同時または先行して国際連携を強化すべきと考えます。	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。

46者　　174件

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
21	1	法人・団体 （㈱ラック）	－	一般利用者に対する啓発活動のポイントは「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。上記を踏まえた、我が国のサイバーセキュリティ戦略における基本価値観の樹立と共有が肝要である。 提案として我が身を守るサイバーセキュリティの観点は重要で実施すべきことであるが、この目線では我が国は後進国であることを認識しなければならない。欧米に対して技術面、制度面から追いつけ追い越せの観点を持つだけではなく、我が国が諸外国に対して主導的な立場を獲得することも、合わせて重要である。 仮に自分の情報は盗られても、他人の情報や他国の情報は確実に守るといった、「公（おおやけ）」に対する意識は我が国が誇るべき考え方である。その点をサイバーセ キュリティ政策推進に生かしていただきたい。	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。
21	2	法人・団体 （㈱ラック）	30	この我が国「公（おおやけ）」に対する意識を持つことに対しての強みを考慮し、セキュリティ戦略に活かす方策として、一般利用者等のセキュリティ意識の醸成が重要と考える。 そのため、このセキュリティ認識の醸成については、一部のセキュリティに関連する産官学の取り組みに限定せず、Webサイトやマスメディアなどを通して、一般利用者等がしっかりと興味を持ち、理解、行動できるよう、例えば、一般利用者等に訴求力のあるキャラクター等を活用したキャンペーンやWebサイトによる積極的な告知などを行う取組が必要だと考える。 リスクが深刻化する中、一般利用者等の自助努力による取組のみでは対応が困難であることは、本戦略にても触れられている通りである。セキュリティに係る情報は一般利用者等まで情報が伝わらないことが多い。普及啓発により一般利用者等がよりセキュリティを身近に意識でき、安全なサイバー空間を維持することが可能な取組を検討していただきたい	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。
21	3	法人・団体 （㈱ラック）	32	警察庁が報告した「サイバー犯罪対処能?の強化等に向けた緊急プログラム」に則りおとり捜査の積極的活用を見据えた捜査手法等の強化や外国捜査機関等との情報共有の強化、国際捜査の推進等の国際連携の推進の強化など、従来の手法に囚われず、グローバルリスクに対する強化を本戦略に盛り込むべきと考える。 また一般利用者等をサイバー犯罪から保護するためには、相談窓口の充実も必要不可欠であるため、相談者が利用しやすい体制の整備についても盛り込むべきと考える。 サイバー犯罪は高度化・国際化の傾向が強く今後数年で、大きな被害が発生する可能性があると考える。そのためには、捜査員の技術力向上に係る施策だけではなく、外国捜査機関との連携やおとり捜査等の手法を含め、法制度等の整備等、捜査力強化に向けた取組を検討していただきたい。 また、今後増加するサイバー犯罪の認知件数も増加すると思われ、それに応じた相談窓口の整備も急務と考える	本戦略には、主に、政府機関、民間企業等の関係機関が連携して推進すべき施策が記載されております。 「サイバー犯罪対処能力の強化等に向けた緊急プログラム」（平成25年1月16日サイバー空間の脅威に対する総合対策委員会決定）に掲げられている施策については、「サイバー犯罪対処能力の強化」に係る取組として推進してまいります。

46者　　174件

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
21	4	法人・団体 （㈱ラック）	40	サイバー攻撃に対処するため、日米安保体制を基軸とした米国との協力は重要である。一方で、ロシアやASEAN各国との情報連携等が可能な信頼関係の醸成が必要と考える。セキュリティに係る外交としては、現実の外交と歩調を合わせる形で、ロシア、ASEANとのパイプ強化を戦略案に盛り込むべきと考える。 サイバーセキュリティにおけるグローバル化により、世界各国から攻撃を受ける可能性が高まりつつあるなか、大きな勢力を持つ東欧やロシアの犯罪組織に対する情報は米国よりロシアが保持していると考える。またセキュリティ技術においても、ロシアの技術力強化を進めており、現実外交と合わせ、新たなパートナーシップに盛り込むべき可能性を有している国と考える。 一方で、ASEANについても、サイバー攻撃に関する情報連携が重要であり、日本の経験してきた取組等を共有することで、日本の存在を示すことが可能と考える。そのため、セキュリティの外交として、より踏み込んだ取組を検討していただきたい	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。
21	5	法人・団体 （㈱ラック）	40	国際展開については、ASEAN地域等における新興国のみならず、アフリカ等への支援も戦略に入れ込むべきと考える。それにより、ASEAN地域等のJPCERTが中心となった新興国への支援だけではなく、ODAを活用する資金・技術提供による協力をより発展させ、ASEAN、アフリカの地域における日本への信頼醸成、協力体制の整備を長期的な視野で構築すべきと考える。 国家間との信頼醸成や協力体制を整備するためには、長期的な視野で取組む必要がある。アフリカへの投資は10年先を見据える必要があり、今後多くの日本企業が進出することが予想され、セキュリティの問題が大きく取り上げられる可能性が考えられる。そのような情勢を考慮し、日本政府の信頼できるパートナーシップを長期的な視野で構築する必要があると考える。 前述したパートナーシップを構築するためには、ノウハウだけではなく、資金・技術援助も必要となることから、省庁横断的な取組としてODAなどの利用強化も見据え、取組を検討していただきたい	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。
22	1	個人	36	情報処理の促進に関する法律を改正して、情報処理技術者試験を必置資格としてはどうか。 情報セキュリティ関連試験検討WG報告書 平成16年11月 独立行政法人 情報処理推進機構 情報処理技術者試験センターで検討された情報セキュリティエントリーレベル2試験を新設してはどうか。 ［情報セキュリティエントリーレベル2試験］ ・情報処理技術者（開発側または利用側）として、情報技術、情報セキュリティに関する一定の知識・技能をもち、部門またはグループ内の情報セキュリティ環境の維持を推進する者。 ※エントリーレベル2の試験は、知識、経験を問う問題が多くなる。なお ITパスポート試験やその他区分の合格者は、2年以内であれば午前免除とする案もありうる。 （知識を問う午前問題をCBT方式のITパスポート試験などの合格で免除し、一般エンドユーザなどの受験者の負荷軽減を図ってほしい）	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。

46者　　174件

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
22	2	個人	37	情報処理の促進に関する法律を改正して、情報処理技術者試験を必置資格としてはどうか。 ITパスポート試験の期待する技術水準に下記を追記して、シラバスなども改定してはどうか。 ・上位者の指揮のもとに、情報セキュリティレベルを損なうことなく、担当する業務に係わる情報システムを利用できる。 ・情報セキュリティインシデントの発生あるいはその虞があるときに、情報セキュリティポリシーに基づいて、適切な判断と対処ができる。	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。
22	3	個人	37	情報セキュリティサポーターに関しては、ITパスポート試験の合格をその必要条件とすることで、ITリテラシーの底上げに繋げることができるのではないか。 ITは私たちの生活基盤の一つであると同時に、ビジネスの世界にも広く浸透し、「グローバル化」、「クラウド」、「スマートフォン・タブレット」、「SNS」など、急速に進化しています。もはや、ITなくしてビジネスは成立しない時代となっているため。 企業では、社内システムや顧客管理など、すべてIT化が当たり前の時代で、ITの知識を身につけていなければ、システムの仕組みがよく分からず、知らない間に企業機密や個人情報が漏えいしてしまった、ということもありえるため。 情報セキュリティに関する基礎知識が身につくことで、インターネット、電子メール、社内システムを利用する際に、機密情報の漏えいやウィルス感染など様々なリスクがあることを理解できるようになるため。	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。
23	1	個人	26	サイバー空間におけるカウンターインテリジェンス情報に関する情報の収集・分析・共有に係る取組を推進し、外国機関との連携を強化するなどして強固な情報保全体制を構築するためには、国家・政府のコミットによるセキュリティクリアランス制度の確立が必要となる。それに向けた姿勢を本文に盛り込むべきである。 現状は、主に民間企業側によるリスク・コスト負担への依存度が大きく、今後の国際的連携・協調を図る際の障害の一要素になるものと考えられる。	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頂きます。 なお、関係機関間の有機的な連携のための基盤として、サイバー攻撃に関するインシデント情報等の共有を促進することについては、4（1）において、「攻撃者等に対して秘密とすべき情報について、既存の仕組みも活用しつつ、共有する目的、共有される情報等の内容や共有する者の範囲等に応じた秘密の保持のための枠組みを整備する」としておりますので、原案のとおりとさせて頂きます。

46者　　174件

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
23	1	個人	24	大規模なサイバー攻撃事案発生時には、警察・自衛隊・民間組織が円滑に連携して対応できる体制作りが必要であり、それに基づく訓練等も実施すべきである。 我が国において大規模なサイバー攻撃が発生した場合、その被害は政府機関、民間の重要インフラなど官民をまたがった多くの組織で被害が発生することが予想される。一般的なテロ事案等では、「海外の国家・軍事組織による攻撃は自衛隊、それ以外のテロ組織等は警察」というような役割分担が存在する。また自衛隊が出動するためには自衛隊法に基づく手続きを経る必要があり、突然発現したサイバー攻撃の被害に対して即応することは難しい。（自衛隊法で定める治安出動として行うとしても、最低限都道府県知事の要請が必要）しかしサイバー攻撃を受けた初期段階では、それが国家レベルの（あるいは軍事的な行為の一部としての）攻撃であるのか、ハクティビストなど民間のテロ組織等によるものであるのかを明確に切り分けることは事実上不可能である。そのため、大規模なサイバー攻撃が発生した場合は軍事的な攻撃である可能性を視野に入れつつ、重要インフラ事業者および警察・自衛隊が連携して迅速な対応ができるような体制の確立が必要である。この体制が構築できれば、同時に情報の共有、専門的ノウハウなどの共有も必然的に図られるであろうし、我が国全体での人的資源の効率的活用をも実現できる可能性がある。実際に隣国である韓国では、2013年3月20日に発生した大規模なサイバー攻撃事案の発生時、民間事業者の担当部門である韓国インターネット振興院（KISA、Korea Internet＆Security Agency）が中心となりながらも、発生当日に民間や軍も参加した合同チームを結成し、翌日には被害と解析結果の概要を公表するという迅速な対応を実現している。このような海外の事例を見ながら、我が国においても、大規模なサイバー攻撃事案に対する民間・警察・自衛隊の連携の枠組みを構築する必要がある。	ご指摘の内容については、3（1）①及び②等に記載しています。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。
23	1	個人	16	論旨については賛成ですが、通信業に関わるものとして補足申し上げます。 「強靭な」という表現が目立ちますが、Internet及びそこで利用されているの特質として、「個々の装置の脆弱さを前提にして、自律分散的なアプローチを行い、網全体として安定動作させる」という特徴があります。ベストエホートと言われながら大きな震災時でも電子メールが届くのが良い例です。 一定の強靭さは必要と考えますが、こういった特徴を生かす形での対策をお考え頂ければと存じます。たとえば、受付窓口のような機能であれば、ネットワーク上で広域分散を行うようなアプローチがございます。一箇所が攻撃されてもまた別の所で受付けて役務を継続する。窓口部分がやられても、バックエンドは別のところにあって防御される。バックエンドも複数箇所にミラーリングされているというやり方です。この方法は人為的アタックだけでなく激甚災害の対策としても利用できる”Internetらしい”対処です。	ご指摘の内容については、2（2）の「①情報の自由な流通の確保」において、「開放性や相互運用性」の確保を記載しているところであり、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。

46者　　174件

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
23	2	個人	35	慎重な検討及び、十分な合意形成を行って頂きたいと考えます。 電気通信業に関わるものの立場から申しますと、犯罪の立証に十分な通信ログを取得するのは非常に困難であると考えます。取得をするのであれば「どのように利用するのか」「どの範囲まで取得させるのか」という問題を整理したうえで議論すべきと考えます。本問題に関しましては、「通信の媒介者」であるネットワークと「通信の当事者」であるサーバでも位置づけが異なっておりますが、その点を混同したような報道がされることもあり、そのレベルからの啓蒙活動が必要と考えます。 また、近年は学校や店舗等で無線アクセスポイントを設置したりしておりますが、こういった方々に同様の義務を課すのかも検討が必要です。この部分のログがないと「投函したポストは判明したが、投函者はわからずじまいだった」ということにもなりかねません。 （郵便との比較） 郵便との比較で申しますと、「送信元アドレスの詐称」というのは「ポストに投函した人が特定できない」というのと同程度の事象です。また、ネットワーク側に通信履歴があったとしても、ネットワークが読み取っているのは基本的にはIPの部分だけで、この記録ではダウンロードとアップロードの区別はできません。郵便に例えればこれらの記録は宛名部分であって実際に何を行っていたのかの立証には、中身が必要です。郵便の中身については郵便事業者が関知しないように通信の中身についてもネットワーク側は関知していません。中身については当事者に聞くしかないところも郵便と同等だと思われます。通信の秘密については郵便時代から様々な議論があって確立してきたものと存じます。その際に立ち返って考える必要があると考えます。	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。
24	1	個人	12	米国におけるサイバーセキュリティ政策の革新的動向として、最大のサイバー脅威であるAPT(Advanced Persistent Threat)攻撃に対する実効性のある対策としてのサイバー脅威及び脆弱性のリアルタイム状況認識を行う「セキュリティ常時監視」について明示的に説明すべきである。（サイバーセキュリティ政策のパラダイムシフト：静的な情報セキュリティ監査報告からリアルタイムなセキュリティ常時監視への移行） 米国行政管理予算局（OMB）は、2009年FISMA議会報告書において、「過去15年間に亘る国家サイバーセキュリティ政策は、増大するサイバー脅威に対応できなかった。」と述べている。OMBは、ゼロデイ脆弱性を含むAPT攻撃に対応するためにリアルタイムな情報システムのセキュリティ健全性の状況認識の可視化、すなわち常時監視を行うために、2010年4月にFISMAに関する新しいガイドラインを公表している。 国防総省（DoD）は、2011年1月にH.R.6523法の制定によりDoD情報システムへのセキュリティ常時監視の導入が義務化された。また、DoDは、2011年7月に発表した「サイバー空間における作戦のための国防総省戦略」において、イニシアティブの1つとして、「国防総省の情報ネットワークの保護のための新防衛概念の採用」を挙げており、その具体策の1つとしてセキュリティ常時監視に相当する「能動的サイバー防衛（active cyber defense）」を提言している。 一方、国土安全保障省（DHS）は、2011年11月に公表した「国土安全保障分野のためのサイバーセキュリティ戦略」において、サイバーエコシステムの1つとしてセキュリティ常時監視のための「セキュリティプロセス自動化」を挙げている。	ご指摘の箇所については、諸外国における国家戦略の概要を記載しているものであるため、原案のとおりとさせて頂きます。また、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。

46者　　174件

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
24	2	個人	12	リスクは、胸囲と資産の脆弱性の積で定義されるため、深刻化するリスクの要因としては、「情報通信技術の革新」による資産の脆弱性のだけでなく最大のサイバー脅威である「APT攻撃」に追加すべきである。また、これらの動的な脅威及び脆弱性伴うリスク変化に迅速かつ的確に対応できる社会システムとしては、従来の脅威に対する防護及びリアルタイム検知による状況認識能力に加えて新たなメカニズムとしての「脆弱性のリアルタイム検知による状況認識能力」が必要である。 最大のサイバー脅威であるAPT攻撃は、完全には防御できないため、リスクの変化を適時かつ的確に認識するために脅威及び脆弱性をリアルタイムに認識し、リスク低減を行い、それでも脆弱性攻撃が成功した場合には、迅速にインシデント対応及び回復する動的なセキュリティリスク管理プロセスが必要である。	例えば、1(1)②において「標的型攻撃」を記載しているところであり、原案のとおりとさせていただきます。
24	3	個人	12	リスクベースによる対応を強化するためには、政府機関、重要インフラ事業者等及び企業など各主体がサイバー空間の脅威に対する状況認識のための情報セキュリティ対策に加えて、従来、オフラインによる情報セキュリティ監査に基づき実施されてきたソフトウェア脆弱性、セキュリティ設定の脆弱性等の状況認識をリアルタイムに行う情報セキュリティ対策の革新が必要である。 ネットワーク速度の隠密性を有するAPT攻撃については、米国OMBが報告しているように紙ベースの情報セキュリティ監査報告書に基づく脆弱性対応では実効性のある対応ができないため、実効性のある情報セキュリティ対策としてセキュリティ常時監視の導入推進が必要である。因みに、我が国においても、政府機関及びISMS評価認証取得企業である防衛関連企業がAPT攻撃を受けても適時なサイバー攻撃の状況認識ができておらず、静的な情報セキュリティ監査では実効性がないことが明らかになっている。	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。
24	4	個人	12	NISCは、防衛省を除く政府機関の情報システムの脅威及び脆弱性の状況認識及びリスク評価を行うセキュリティ常時監視の新たな制度及び監視システムを整備する必要がある。 一方、防衛省は「サイバー空間の防衛」のために防衛省の情報システムのセキュリティ常時監視のための新たな制度及び監視システムを整備する必要がある。 米国においても、連邦政府機関の情報システム及びDoD情報システムのセキュリティ常時監視はそれぞれ国土安全保障省及び国防総省が行っている。 また、国土安全保障省は、2012年6月に次期セキュリティ常時監視である常時診断緩和(Continuous Diagnostic and Mitigation:CDM)並びに高度セキュリティ人材確保の困難性対応及び調達コスト削減のためのクラウドサービスとしてのCMaaS(Continuous Monitoring as a Service)の計画を発表している。CDM計画は、連邦政府機関、州政府及び地方自治体に対して既存常時監視能力の向上/自動化、重要セキュリティ関連情報の相関・分析、及び連邦政府機関及び連邦政府全体レベルでのリスクベース意思決定の高度化を目的としたものである。	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。

46者　　174件

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
24	5	個人	12	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対策としても、情報システムと同様に、静的な情報セキュリティ監査ではなくて、サイバー脅威及び脆弱性の状況認識を行う「セキュリティ常時監視」の段階的導入の推進のあり方について、具体的な検討スコープの1つとして追加する必要がある。 国土安全保障省（DHS）のICSJWGは、「制御システムサイバーセキュリティの業界横断的ロードマップ（第3版）」を2011年9月に発表し、開発目標の1つとしてセキュリティ管理策の常時監視の段階的開発を挙げている オバマ大統領は、サイバーセキュリティ強化の立法化が進まないため、2013年2月に重要インフラ防護の強化のための大統領令13636号（E013636）及び大統領指令21号（PPD-21）を発出している。前者は、重要インフラのサイバーリスク低減のためのフレームワークの策定を国立技術標準研究所（NIST）に命じている。 一方、後者は、重要インフラのサイバー脅威及び脆弱性に関するニアリアルタイム状況認識能力のデモ開発をGHSに命じている。また、国防総省は、重要インフラサービス調達要件に制御システムのセキュリティ常時監視要件の盛り込みを検討している	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。
25	1	個人	17	情報通信機器技術の向上により、無線LANルーターを代表部屋に設置すれば当該住居内の他部屋ではデジタル機器が無線化により、壁超えで3階離れていても接続されることで快適な生活環境ができる。しかし、賃貸マンションなど部屋が壁で仕切られた隣人・上下階の別人間で利用したい特定部屋の無線ルーターを指定すれば電波で接続され、通信情報を共有化できることになる。 各主体CSIRT連携とあるが、無線ルーターを介した共有化があった場合、更に頻繁に発生するようだと追跡調査など困難となる。無線LANルーターを介した情報通信共有化では、使用開始の無線LANルーター指定時に、所有者と同住居の居室間だけに限定した方が情報セキュリティ向上に繋がると考える。	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。
26	1	個人	16	管理や規制が緩すぎることはセキュリティー上のリスクが高まることから、管理や規制を適切に行う必要がありませんか。 世界ではデータ保護の法律があり、日本でも必要ではありませんか。具体的にはアメリカでは愛国者法があり国内の情報システムがテロ行為などを受けた際に裁判所の判決がひつようなく捜査権限を有しています。有事の際にはこのような柔軟な対応ができなければ、マイクロ秒単位で攻撃が行われるサイバー攻撃においては判断の遅れが致命的な被害の増大を招く恐れがあると考えられるため、法整備が必要ではないでしょうか。また本日（2013年6月4日）の産経新聞朝刊の3面によると華偽（ファーウェイ）が「中国人民解放軍のサイバー戦闘部隊のえるすぐりの人物に、特別な通信ネットワークを提供している」として、アメリカ・オーストラリア・カナダ政府が政府の通信ネットワークから華偽を除外する措置をとっています。日本も情報を共有してもらい、対策を検討してはいかがでしょうか。	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。

46者　　174件

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
26	2	個人	21	情報共有の国際的な範囲を示してはいかがでしょうか。 意見1のとおり華僑(ファーウェイ)等の国際的な情報共有が重要と考えられ、国内の企業や教育・研究機関による情報共有と協議に解釈されないよう、国際的に企業や教育・研究機関による情報共有と明示的に記載してはいかがでしょうか。	「サイバー攻撃に関する情報共有」という表現は、国際的な情報共有の意味を含むことから、原案のとおりとさせていただきます。
26	3	個人	24	クラウド化はサイバー攻撃に強い情報システム基盤の構築とは反対方向のため再検討してください。なお政府共通プラットフォームはNIST(米国国立標準技術研究所)の定義によるとクラウドに該当しませんので、用語を適切に使い分けてください。 クラウドは情報システムを委託先にゆだねることから自らが直接にセキュリティ対策をコントロールすることができません。またクラウドは委託先によってはサーバ設備が外国に設置される可能性が排除できないことから、意見1による愛国者法等によるデータの差し押さえリスクが生じます。これは経済産業省の「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」でも問題が指摘されています。 政府共通プラットフォームを推奨することは当然のことかもしれませんが、政府が民間のクラウドサービスを推奨していると誤解している者が私の周辺にも多くなっています。(政府が民間のクラウドサービスりように伴う被害を保証するのであればこの限りではありません。	政府共通プラットフォームは、民間のクラウドサービスを利用するものではなく、政府機関向けに導入された専用の情報システム基盤であり、クラウド技術を採用しています。 したがって、「政府共通プラットフォームによる政府情報システムのクラウド化」の意味するところは、民間のクラウドサービスの利活用とは異なるものになります。 ご意見いただいたクラウド利用における情報セキュリティ上の懸念点については、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。 なお、該当部分の記述は、政府として民間のクラウドサービスの利用を推奨するものではありません。
26	4	個人	24	人材の確保・育成方法の具体的手法が示されていますが、人材像についても具体的に記載してはいかがでしょうか。例えば、国家公務員による高度なサイバー対策技術を備えた要員を育成する必要がありませんか。 サイバー対策技術を一般競争入札で調達した場合、反日企業が落札する可能性を排除できません。想定されるサイバー攻撃に備えるための要員を競争入札したところ、サイバー攻撃を秘密裏に計画している企業が落札することがあってはなりません。 現在の企業は国際化が進んでおり、たとえ国内資本の企業であっても当該外国人が会社員として潜入している可能性が排除できないことから、サイバー対策要員は国家公務員である必要があると考えています	ご指摘の人材像については、本戦略を踏まえて改訂予定の「情報セキュリティ人材育成プログラム」の中で、明確化する予定となっています。

46者　　174件

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
26	5	個人	21	日本語による独自の基本ソフト（OS）の研究・開発を推奨してはいかがでしょうか。 ITは英語と切っても切り離せないことが抵抗感を生じさせている一因と感じています。 日本語のプログラムソースによる基本ソフト（OS）を作成することで抵抗感を排除し、人材育成の発展だけでなく、日本語以外の操作によるサイバー攻撃にたいする情報セキュリティが向上する可能性があると考えています。	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。
27	2	個人	33	サイバー空間の防衛は、現状、防衛白書の一部と見まがう印象をうける。全省庁的な取組として記載されるべきである。	3（1）⑥の冒頭において、「我が国全体としての対応の強化を図ることが重要である」としている等、全省庁的な取組として記載しておりますので、原案のとおりとさせて頂きます。
27	3	個人	36	我が国の社会経済活動及び国民生活あらゆる側面・場面において情報セキュリティ対策が必要であり、その基盤となる最も重要なものは、国民全般全域への啓蒙、教育等によるリテラシー向上と高度なセキュリティ関連技術を保有する人材の育成であることが読み取れる。 然らばIPAによる「ITパスポート試験」レベルの試験を大学入試センター試験の選択科目に加える等の実効的な具体策を検討し、その可能性・方向性を示すべきである。現状の「ITパスポート試験」は、社会常識の要素を含む情報セキュリティの基礎基盤能力を測るのに最も相応しい試験であり、この内容・レベルの試験を学校教育制度プロセスに組み込むことによって、国民全体の情報セキュリティリテラシーの底上げに確実に繋がると同時に、人材育成のファーストステップになるものと考えられる。	3（2）の「③人材育成」において、公的資格・能力評価の改善や新設の必要性も含め、多様な資格・能力評価制度の在り方など情報セキュリティ人材として求められるニーズの多様化に応じた検討を行うこととしています。ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
28	1	個人	32	違法な手段で業務妨害等の結果を生じさせるサイバー攻撃は「通信」とはいえず、憲法第21条第2項後段の保障の範囲外にあると解するべきである。 通信とは、特定人から特定人に対して意思を伝達するものを指す。サイバー攻撃・犯罪は、業務妨害等の本質的に反社会的な結果の発生を目的とする行為であって、特定人から特定人に対する意思の伝達を目的とする行為ではない。 他人のHPを改ざんし政治的な主張をするサイバー攻撃・犯罪もあるが、サイバー攻撃・犯罪に当たる行為と政治的な主張をするという行為は区別されるべきであり、両者が一つの行為で行われているからといってサイバー攻撃・犯罪が正当化されるわけではない。そもそも、不特定多数に対する政治的主張は通信の秘密として保護に値しない。 特定人が特定人に対する意思伝達としてサイバー攻撃・犯罪を行う場合も考えられるが、合理的必要性なく違法な手段で業務妨害等の結果を生じさせるものであって、通信として保証するに値しない。	ご指摘の内容については、今後の「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」等の施策の検討に当たっての参考とさせていただきます。

46者　　174件

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
29	1	個人	42	NISCの専門職員の増強を意図されていますが、各府省における要員の育成も重要だと考えます。各府省では2～3年で異動され、人材が育ちにくい環境ではないかと思えます。情報担当分野においては、最低でも5年程度は経験をつむのが望ましいと考えます。それが無理であれば、NISCから専門要員を各府省に常駐派遣するような方式を考えてはいかがでしょうか。	ご指摘の内容については、例えば、P.27に記載しており、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。
29	2	個人	30	「サイバー空間の衛生を確保する」ことの重要性に鑑み、「一般利用者等の自助努力による・・・取組を補強するため、他の主体による積極的なサポートが必要」との認識が示されています。非常に有用な観点であり賛同します。 サイバー空間の衛生を確保するための広範で日常的な取組の一環として、主として中小零細企業向けの「情報セキュリティ監査」の活用を促進することを提言します。 また、その物的保証（背中を押す）として、費用の一部を補助することを提言します。 既に、意識の高い企業や官公庁、自治体ではセキュリティ監査を実施していますが、中小零細企業では普及していません。 その大きな理由のひとつは費用がかかることです。また、「安かろう悪かろう」でも結局無駄になります。そこで、中小零細企業にとって手の届く魅力的な「情報セキュリティ監査制度」と費用面の補助があれば制度の活用が進み、サイバー空間の衛生レベルが着実に向上すると考えます。 そのとき、情報セキュリティ監査を実施する主体として、監査法人や情報セキュリティ専業企業だけでなく、NPO法人を活用すれば、一定の質を比較的安価に確保できる可能性があると考えます。 サイバー空間（あくまで公共のもの）の現状をたとえて言えば、人々が集う場が衛生管理されていないようなものであり、利用者が身を守るにはそれぞれの自己責任によるしかない状況です。 サイバー空間のどこかが不衛生な状態があれば、結局は大多数の国民が被害を受ける側になり、それを未然に防ぐのが、公衆衛生の果たすべき役割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。
30	1	個人	19	サイバー攻撃対策における国家機関の役割としては、サイバー演習における環境を構築し実施する「サイバーレンジ」が不可欠であると考えております。国家機関及び重要インフラ事業者等においては、全ての組織においてサイバーレンジを構築し、正しいセキュリティ対策の実施と教育を全組織の共通認識とすべきであると考えております。	サイバー攻撃に関する演習については、演習用テストベッドを利用した実践的な防御演習や自衛隊等における実践的なシミュレーション環境での訓練等の施策を進めることとしています。ご指摘の内容について、今後の施策の検討に当たっての参考とさせて頂きます。

46者　　174件

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
31	1	個人	36	「これらを活用する能力を有する優れた個人を発掘育成するための合宿研修や情報セキュリティ人材が実践的技能を競うコンテスト等を官民で連携し、実施する。」という記述について，異論があります． この記述を何の先入観もなく読んだ場合，「これまで何も行われておらず，これから取り組む」というように見えますが，すでに取り組んでいるものもあるはずです． 例えば，独立行政法人 情報処理推進機構（IPA）とセキュリティ・キャンプ実施協議会の共催による，セキュリティ・キャンプの取組がまさに発掘育成するための合宿研修であり，実践的技能を競うコンテストについては，例えばNPO日本ネットワーク・セキュリティ協会（JNSA）が実施しているセキュリティ・コンテスト（SECCON）がそれにあたります． すでに実施されている取組があることはきちんとご認識いただいた上で，さらにそれらの取組を発展させていくか，別の取組で補完／発展させていくかという選択が必要になるかと思います	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。
31	2	個人	36	「グローバルに活躍できる人材を育成等することが重要であるため、国際会議への参加や海外の専門的な大学院等への留学を支援するとともに、国内における国際会議の招致や開催を推進する。」という部分について，異論があります． 国際会議の承知や開催を推進については，大いにやっていただければと思いますが，「海外の専門的な大学院等への留学」という文言につきましては，順序を間違えていると考えます．この部分は，留学以前にまず「日本国内での専門的な大学院や専攻における教育や育成の充実」という部分を視野に入れるべきと考えます．もしくは，「日本国内の大学や大学院での取組拡充と支援」というものを考えるべきです．日本国内で取り組まれている情報セキュリティ関連の教育／研究プロジェクトはありますし，それらの取組やプロジェクトが，諸外国のそれと比較して大きく劣るとは考えていません．また，日本国内での教育や育成の充実を行うことで，CYRECの取組との連携を行いやすくなる（＝オールジャパンの層を厚くすることを期待できる）とも考えられます	ご指摘の内容については、「実践的な教育プログラム等に関する大学等専門教育課程の充実化」等と記載しており、原案のとおりとさせていただきます。
32	3	個人	36	「人材の発掘・育成を、採用・活用につなげていくことも必要である。そのため、政府機関が率先して、情報セキュリティ人材の外部登用を行う。」という部分について，異論があります． 政府機関が率先して人材の外部登用を行うのはもちろんですが，他の民間企業に対しても，情報セキュリティ人材の必要性を説いていただき，登用／雇用の門戸を開いていただくような文言を書き加えていただければと思います	人材育成については、政府機関のみならず、重要インフラ事業者等、一般企業等においても重要と考えています。そのために必要な人材育成の過程において、まず政府が率先して登用することが必要であるとともに、人材育成の観点から民間企業に対して政府が雇用を求めるものではないため、原案のとおりとさせていただきます。
33	1	個人	36	情報セキュリティ人材の育成にあたっては、技術的知識やスキルだけではなく、高い職業倫理感、および、責任感を付与するような教育が必要である。スキル標準や公的資格、能力評価においては、その観点での考慮、および、認定が不可欠であることを明記すべきである。	ご指摘の「高い職業倫理感」等については、情報セキュリティ人材の育成にあたって重要と考えております。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。

46者　　174件

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
34	1	個人	23	サイバー攻撃が現実空間にもたらす被害が漠然としている。大規模地震に関して予測しているような「定量的」なリスク分析・リスク評価を行ったほうが、広く国民にサイバー攻撃に対する危機感とその対策の必要性を訴えることができると考える。 万一サイバー攻撃を被った場合、 ・どの様な被害の発生が予想されるのか ・発生した被害はどの分野にまで波及するのか ・被害発生に伴う予想損失額 ・人命被害にまで波及した場合予想される予想死亡者数 について「サイバー空間版のハザードマップ」の作成を考慮することを提案する。	本戦略の「基本的な考え方」として、2(2)において「③リスクベースによる対応の強化」を掲げているところであり、例えば、政府機関においては、標的型攻撃等への対処に関するリスク評価手法の確立を図ることとしています。ご指摘の内容については、今後の施策の検討に当たっての参考とさせていただきます。
35	1	不明	－	参画する民間企業等に国籍条項を設けるべきである。	ご指摘の「参画する」の趣旨が不明確であるため、回答を控えさせていただきます。
36	1	不明	－	サイバーセキュリティ強化は大切だが、サイバーセキュリティ対策を強化してもリスクを0にすることは不可能である。マイナンバー法案のように、国民の個人情報を一つにまとめ、ネット上で手続きや申請を行う行為は危険である。 ネットを活用するにあたっては、情報の分散によってリスクも分散し、仮に何かが漏れた場合の損害を最小化するしかないと考える。	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。
36	2	不明	16	サイバー攻撃者を特定し、攻撃に対処するために有効だとしても、国民全体の個人情報を取得し、長期にわたって保存する行為はプライバシーの侵害行為だから辞めてほしい。	ご指摘の内容については、2(2)の「①情報の自由な流通の確保」において、「プライバシーの保護」等の確保を記載しているところです。ご指摘の内容については、今後の施策の推進に当たっての参考とさせていただきます。
36	3	不明	16	有害情報や違法情報の規制という名目で過度な規制が行われぬよう、包括規制ではなく個別対応してほしい。また、捜査や削除依頼などを担う機関をつくる場合は、暴走し越権行為を引き起こさないよう権限を絞ってほしい。	ご指摘の内容については、2(2)の①「情報の自由な流通の確保」において、管理や規制を過度に行うことなく、開放性や相互運用性を確保する旨を記載しているところです。ご指摘の内容については、今後の施策の推進に当たっての参考とさせていただきます。
36	4	不明	21	セキュリティ対策は国や機関に任せるだけではなく個人でもやらなければ意味が無いので、その対策もしっかりやってほしい。	ご指摘の内容については、2(3)の「④一般利用者(略)の役割」において、「自分の身は自分で守る」とともに、「他者に迷惑をかけない」という認識をもって対策に取り組むことが重要となっている等としております。

46者　　174件

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
37	1	不明	－	ソフトウェアの中の実行可能領域をROMで構成すれば、ハッキングは不可能となる。当然の理屈であるが、この単純な事実をサイバーセキュリティ政策の基礎にすることが必要である。 各デバイスには余計な情報は持たせず、厳重なセキュリティ対策がなされたサーバー側でプログラムの実行、データ保持を行うことで、ハッキングやウィルスに対抗すべきである。	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。
38	1	不明	－	セキュリティ強化は必須だが、同時に国民の税負担も考慮し、効率的なシステム運用をすべきである。	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。
39	1	不明	－	サイバーテロ対策を名目としてネット監視を強化することには、強く反対する。憲法第21条〔表現の自由〕の2「検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。」に違反していると考える。 サイバー攻撃の多い国からのアクセスを遮断すればよく、また、重要な機密、個人情報等が入ったサーバーおよびPCはスタンドアロンで運用すべきである。	前段のご指摘の内容については、今後の「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」等の施策の検討に当たっての参考とさせていただきます。 また、後段の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。
40	1	不明	17	情報技術の高度化の時代、完璧な防御はあり得ない。サイバーセキュリティ対策は限定的とし、国家機密等の重要情報はアナログ化すべきである。相手の裏をかくのが戦略の妙であり、日本にサイバー攻撃を仕掛けてくる国も、日本がこのご時世にアナログ化に走るとは予想していない。 例えば、機密情報の通信にFAXを利用すれば、誤送信対策だけで済み、国民の負担も少ない。 日本の自衛隊はサイバーセキュリティ強化以前にやるべきことが山積している。サイバーセキュリティに使う予算があるなら、シーレーンの強化、装備調達の人員補強、予備役の増員に使って欲しい。	ご指摘の内容については、今後の検討の参考とさせて頂きます。

46者　　174件

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
41	1	不明	－	インターネットに接続した世界で「安全なサイバー空間」を構築するのは矛盾しており、推進体制を「情報セキュリティセンター」から「サイバーセキュリティセンター」に名称変更するなどという構想も間違いである。 そもそもアメリカ生まれのインターネットは、一部が破壊されても別ルートで必ず伝達できるという「柔軟なネットワーク」であり、セキュリティ性は狙っていない。 最初は軍事用であったインターネットは、一般開放された瞬間に誰でも通行できる「公海」となった。公海には、海賊などが通行者を狙っており安全性などない。その対策は、通行者の自己防衛である。「間もなくInternet of Things と呼ばれる、あらゆるものがインターネットに接続される時代を迎える」などとは、セキュリティ犯罪者による洗脳的スローガンである。 また、高セキュリティ性確保の基本は「クローズドなプライベート・ネットワーク」であり、「インターネットに接続されない制御システムにおいても同様にリスクが高まっている」などもありえない。もし攻撃にあったと言うならば「インターネットに接続されている」ことを意味する。例えば、公衆無線LANサービスなどで無線LANを暗号化するという、一種のサイバー空間セキュリティー策はダメである。「情報セキュリティー対策」が大事であり、情報セキュリティセンター（NISC）で推進行動することが正しいと言えるのである。	サイバー空間については、我が国の成長力強化にとって不可欠であり、今後の一層拡大・浸透していくと考えております。その上で、サイバー空間を取り巻くリスクの深刻化に対応することが必要と考えております。また、ご指摘の名称変更につきましては、本戦略の名称をこれまでの「情報セキュリティ戦略」から「サイバーセキュリティ戦略」に改めること等を踏まえ、仮称として「サイバーセキュリティセンター」とさせて頂いておりますが、今後の国内外の環境変化等を踏まえ、具体的な改組にあたって検討する予定です。
42	1	不明	－	今後もサイバーセキュリティの重要性が高まるなか、各国公立大学でもサイバーセキュリティ関係の学科の設置が必要ではないか。	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。
43	1	不明	－	企業は自助努力によりISMSなどの認証規格を取得している。個人情報など重要な情報を扱う国の各省庁や自治体も、ISMS取得を義務づけるべきである。 リテラシーの向上を含めてセキュリティ対策を強化するのはPDCAが重要。役人は努力不足であり、人に言う前に自らが取り組むべきである。	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。
43	2	不明	－	セキュリティ対策技術は日進月歩で陳腐化が激しい。攻撃もどんどん進化するので、セキュリティ技術共有サイドのプレイヤーとの間で、技術に関する継続的な情報共有の場が必要である。	ご指摘の技術に関する情報共有については、例えば、政府において、警察庁と民間事業者等との間で、解析対象となる電子機器等の技術情報の共有を進めているところです。ご指摘の内容について、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。
45	1	不明	－	サイバーセキュリティー　戦略とありますが、ITの事、ほとんどわかりません。このような（案）を創っても上手く取り組めるのでしょうか？以前、政府は、老舗の企業のきちんと教育を受けた人間と、IT関連の人間をバーターするなど、とんでもない事を言っていました。一般の感覚では信じられない事です。多くの我慢をして積み上げてきた仕事を手放す事など、勝手に決められては、たまりません。	前段のご指摘の内容については、サイバーセキュリティに関する普及啓発等の施策の推進に当たっての参考とさせて頂きます。また、後段の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ないため、回答を控えさせていただきます。

46者　　174件

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
46	1	不明	24	パソコンやルーターなどのインターネット通信装置を含む中国製電子機器に製造段階から意図的にバックドア（通信盗聴ソフトウェア）や偽部品が組み込まれている疑いがあるとして米国政府は、全米から排除する方針を固め行動に移しつつある。日本国内でも低価格を武器に急速に浸透しており、中国で組み立てられたパソコンが防衛省で使用されていたり、警察内部の本人の認証システムまでもが中国製品という現状がある。特にインターネット通信をつかさどるルーターにバックドアが仕込まれた場合、既設のセキュリティ対策はほとんど無力化し、機密情報や知的財産、個人情報といった安全保障にかかわる重要情報が中国政府、中国人民解放軍の手に渡る可能性がある。一方、中国はセキュリティ上の理由で昨年（2012年）12月に米国製通信装置の排除をすでに完了している。このセキュリティ上の理由には、キルスイッチ（インターネットの遮断）も脅威とされている。 政府システムはもとより、民間通信事業者、金融機関等重要インフラ企業における中国製品の使用状況に関する実態調査を行い現状把握を行う必要がある。同時にバックドアが電子機器に組み込まれた場合に我が国の安全保障にどういった影響があるか、有識者の議論を経てその脅威に対する認識を政府ならびに国民の間で共有する必要がある。そのうえで電子機器の調達について政府方針を定め、情報セキュリティが担保される仕組みを構築する必要がある。ソースコードの開示を求めるとする意見が予想されるが、ソースコードと製品の対応が必ずしも保証されないこと、さらには製品出荷後の自動更新によるバックドアの生成リスクなど十分な議論が尽くされる必要がある。 米国ではマイクロチップなどの軍需用電子機器を中心に国内製造への転換を進めている。我が国も電子機器や通信装置の国産化を進めることで、情報セキュリティが担保されるだけでなく電子機器、通信機器メーカーの復活、情報セキュリティ製品の開発企業の創出につながり、幅広い雇用機会が期待できる。また、中国との交渉カードとしての利用も考えられる。	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。