「サイバーセキュリティ2014（案）」に対する意見募集の結果の概要

資料 5-1

- 実 施 方 法： NISCのWebページ及び電子政府の総合窓口(e-gov)に掲載して公募
- 実 施 期 間： 2014年5月20日（火）～6月9日（月）
- 意 見 総 数： 114件 【内訳：15企業・団体から延べ92件、14個人等から延べ22件】

（1）賛同意見　全4件

（2）修正意見　全37件

- 全体の構成等に修正を求める意見はなし。
- 表現の明確化や適正化など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15件）。
- 戦略で言及しているなどの理由で原案どおりとする意見については、理由を付して回答（全22件）。

（3）政策展開に係る意見　全66件

- 今後の政策展開に係る意見については、当センターとしての考え方及び当該意見を今後の参考にする旨を回答。

（4）その他意見　全7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。

「サイバーセキュリティ2014（案）」に対する意見募集の結果について

意見募集期間：平成26年5月20日（火）から同年6月9日（月）まで

29者114件

番号	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
1	個人	1	1章	「ネットワーク」の安全性・信頼性の向上及び「成りすまし」による被害抑止する有効な手段として、生体認証を推進していただくことを望みます。安全・安心な社会生活を送れるようご検討ください。	政策展開に係る意見	認証方式に何が適しているかについては、システムや対象によって異なるものであるため、一律に生体認証を推進することはできないと考えます。御意見については、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。
2	匿名	1	1章	役所、学校、病院、その他インフラ施設で使用するパソコン及び関連機器などの「更新費用の積立」制度を義務化していただきたい。 OSのサポート終了によりパソコンを更新する場合、特定のバージョンでのOSでしか動作しないソフトウェアや特殊な機器（放送設備や制御装置）が使用できなくなります。パソコンなどは予算計上されやすいですが、機器などは耐用年数が長いことや承認者の理解能力が無い場合、予算化されていません。更新時に予算化するのではなく、使用開始と同時に積立を開始するように制度化していただきた	政策展開に係る意見	更新費用等を積立金として留保するかどうかは、各企業等の主体的判断にゆだねられるべきものと考えます。御意見については、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	個人	1	1-④ 1-⑤	「サイバーセキュリティ」という概念を「人権」という切り口からみると、これを「サイバー空間における人権侵害を防止すること。」と表現することができると思います。 本件計画案に「サイバー空間における人権侵害の防止」という項目を設け、個人情報等のプライバシーの保護、ネットバンキングやポイント等の財産権の保護、名誉棄損や侮辱の防止、人種、国籍等に基づく不当な差別的書込みの防止、サイバーいじめの防止、児童ポルノやリベンジポルノ等のアップロードの防止、いわゆる「忘れられる権利」の保護等を盛り込むべきだと思います。	政策展開に係る意見	サイバー空間における人権については、様々な考え方があります。御意見については、今後のサイバー空間に対する法整備等と整合をとりつつ、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	(株)ニーモニックセキュリティ	1	資料2「暗号モジュール試験及び認証制度」等	「暗号」に並列する形で「本人認証」ないし「パスワード」という独立の項目を起こし、本人認証ないしパスワードに関する注意事項を詳しく記述することを提案します。 本人認証を破られれば暗号化による防御は一瞬のうちに無効化されてしまいます。しかるに本ガイドラインでは「本人認証・個人認証」という項目は存在せず「パスワード」が簡単に言及されているだけです。然るべく注意を喚起されることを期待します。	修正意見（修正なし）	本文書は「サイバーセキュリティ戦略」に基づき、2014年度の各府省庁の施策を取りまとめた年次計画であり、暗号利用や認証に係るガイドラインではございません。御意見については、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	個人	1	ー	次のような内容の「電子演算情報多目的保安法」を制定すべき。 1. インターネットの使用年齢を18歳以上とする。 2. アフィリエイト系ブログに、「アフィリエイト経営税」を導入し、純利益の25%をサイバーセキュリティ基金として省に納める。 3. 防犯管理番号を全てのユーザーがIDとして拾得。 4. サイバーセキュリティ基金の為に、「インターネット利用税」を導入。 毎月のインターネット料金の25%を基金のために利用者は納める。 5. 自衛隊の国防情報保護のために、ブログ税、動画共有税を導入。自衛隊ネット監視室の創造。 6. 国防情報の漏洩、民族国籍での差別や対立幇助、特定の組織人物への誹謗中傷、反政府的なデマ、などを書き込むだけで3万円以上の罰金とする。	その他	本年次計画に対する御意見ではないため、回答は控えさせていただきます。 御意見については、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	匿名	1	1-①-1)-(サ) 1-①-1)-(シ)	情報技術において、利便性の上昇は安全性の低下に繋がる場合が有る。 マイナンバーカードをクレジットカード等に紐つける場合、その選択は任意とすべきだ。 ビッグデータにしろ、その利用について個人の同意が得られない場合、必要の無い情報については偽情報入力で対処する。これは安全性の為に利便性を犠牲にする行動で、経済的には非効率である。 ビッグデータによる統計も意味をなさなくなっていくだろう。	政策展開に係る意見	政府においては、ビッグデータ時代において、個人情報及びプライバシーを保護しつつ、パーソナルデータの利活用を促進するための検討を進めております。 IT総合戦略本部新戦略推進専門調査会マイナンバー等分科会の中間取りまとめにおいて、「キャッシュカード、クレジットカード等、民間が発行するカードについても、国民や民間事業者のニーズを踏まえ、後述する公的個人認証サービスの民間開放と併せ、個人番号カードとの一体化や連携等につき、官民相互にメリットが得られるよう、柔軟に検討を進める」とされており、これを踏まえ、今後検討を進めるべきものと考えております。 御意見につきましては、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	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
7	個人	1	ー	政府機関におけるセキュリティ面の実装や基準を可能な限り公開するとともに、一般企業においても政府基準を満たすセキュリティ実装が可能とするよう業界団体を通じて通達を出す等の後押しをして頂きたいと思料しております。 また、基準準拠にインセンティブ付与または義務化を行い、政府において抜き打ち調査を行い、問題のある企業は警告を与える等の対応を行っていただけば、セキュリティ向上につながるものと思料しております。	政策展開に係る意見	NISCのHPにおいて、政府機関統一基準群、重要インフラ行動計画のほか、各種規定／ガイドライン等を開示しております。また、情報セキュリティ月間のイベントや業界団体との会合等を通して、広く普及啓発に努めております。 ただし、一般の企業等におけるそれらの利用は、各企業等の主体的判断に委ねられるべきものと考えております。
8	(株)エイチ・エム・アイ	1	ー	弊社は、セキュリティ製品を開発製造販売している弱小企業です。現在、不正侵入者への撃退システムをユニークな技術で開発に進みたいと考えていますが、大企業が弱小企業をつぶしにかかる恐れがあるため、世に出すための資金を調達できません。 官庁はこのような応募をしているが、実際には大企業からの提案に資金補助される可能性が高いと思っております。	その他	「情報セキュリティ研究開発戦略（改定版）」においては、サイバーセキュリティ関連産業の活性化に向けた取組も記載されております。 御意見につきましては、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	法人（匿名）	1	1-①-1)-(ケ)	以下を追記する。 c) 内閣官房において、政府情報システムのクラウド化を進めるに当たり、民間企業が提供するパブリッククラウドに関するセキュリティの認証評価プログラムの導入に向けた検討を2014年夏から開始し、その成果を政府機関の情報セキュリティ対策のための統一基準群の次回改定に反映する。 ＜理由＞ 諸外国（米、英、豪、星）では、政府で統一されたパブリッククラウドの認定・認証プログラムの構築・運用が進んでおり、各省庁が各々にパブリッククラウドの評価をすることなく、一定のセキュリティレベルを維持しながら、コストを削減し、スピーディにパブリッククラウドを導入することが可能となっている。我が国では2021年度を目途に原則全ての政府情報システムをクラウド化することになっており、コストを最小限に抑えつつ、かかる目標を期限までに実現するためには、民間企業が提供するパブリッククラウドに関するセキュリティの認証評価プログラムの導入に向けた検討を早急に開始する必要がある。	修正意見（修正なし）	サイバーセキュリティ2014は、セキュリティ水準の向上やサイバー攻撃への対処能力の強化等に関する取組のうち、2014年度に実施するものについて、サイバーセキュリティ戦略の記載体系に沿って詳細を示すものであり、政府情報システムの在り方を示すものではございません。 政府情報システムのクラウド化につきましては、2014年3月に経済産業省が「クラウドセキュリティガイドライン改定版」及び「活用ガイドブック」を、総務省が同年4月に「クラウドサービスの提供における情報セキュリティ対策ガイドライン」をそれぞれ公表し、さらに同年5月に改定された政府機関統一基準群においては、クラウドサービスを含む情報システムにおける外部委託及び約款における外部サービスの利用についての記載を新しくするなどの取組を実施しているところです。 また、本年次計画の1-①-1)-(ツ)に記載しているとおり、クラウドコンピューティングを含む運用・管理を外部に委託している政府機関の情報システムについて、情報セキュリティを確保するための取組を推進することとしておりますので、記述につきましては、原案のとおりとさせていただきます。
10	個人	1	2-③-(キ) 2-③-(ク) 2-③-(ケ) 2-③-(コ) 2-③-(サ)	サイバーセキュリティの国家資格の新設、見直しにあたっては、経済産業省に閉じることなく、総務省や文部科学省、内閣官房をも巻き込んだ包括的なスキルの整理が必要である。 情報セキュリティは学際分野であり、必要とされるスキルもコンピュータサイエンス、コンピュータエンジニアリング、ネットワーキング（インターネット／テレコム）、ソフトウェアエンジニアリング公共政策学、経済学、経営学、技術者倫理、プライバシー、法学、科学捜査（フォレンジック）等、分野が省庁間にわたる。それらを考慮しないサイバーセキュリティスキルは表面的なものに終わってしまう。 CISSP等のグローバル資格の活用（継続的学習施策を含めて）との整理も必要。上記の整理が為されることのないままにサイバーセキュリティの国家資格（情報処理技術者資格）が新設されたり、既設資格を変更したりするような、非効率的な方向に議論を進めるべきではない。	政策展開に係る意見	情報セキュリティに係る試験制度、資格制度にあたっては、最新の技術動向等を踏まえ、実践的能力を常に評価・担保し、人材の能力の「見える化」を図っていくことが重要と考えております。そのために最適な仕組みとなるよう、関係省庁等と今後検討を進めていくとともに、適切なフォローアップをしていきます。
11	個人	1	1-①-1)-(ウ)	以下を追記する。 c）APT攻撃に対して実効性のある対策である「情報資産及びセキュリティ設定の脆弱性のリアルタイム状況認識」の必要性の認識形成のために「政府情報システム管理データベース更改のためのセキュリティ常時監視に関する調査研究」を行う。 ＜理由＞動的なサイバー脅威であるAPT攻撃に対して実効性のある対策として情報セキュリティリスクマネジメントの考え方に基づきリアルタイムのセキュリティ常時監視を早急に導入する必要がある。米国においては、連邦政府機関及び国防総省並びに民間企業においてセキュリティ常時監視の導入が推進されている。APT攻撃対策の実効性にあるベストプラックティスであるセキュリティ常時監視の必要性に関する政治トップ層の認識を円滑に形成するために調査研究を最優先で行う必要がある。	修正意見（修正なし）	1-①-1)-(ウ)は、「国が保有する情報システムについて、情報システムのライフイベントごとに作成される資料や情報資産等を統一かつ網羅的に管理し、データを蓄積するデータベース」の利活用に関する取組を記述しているものです。御指摘のAPT攻撃対策に関する取組としては1-①-1)-(ア)に記載している取組の実施を予定しており、記述は原案のままとさせていただきます。

番号	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		2	1-⑥-(ス)	以下を追加する。 また、政府機関及び関係機関の役割の整理・明確化とともに、サイバー攻撃への対応体制の法整備を行い、その対応体制を支える基盤として国家の情報資産の脆弱性をリアルタイムに状況認識するセキュリティ常時監視を整備する。 ＜理由＞法律に基づくサイバーセキュリティに関するNISCへの権限付与とともにAPT攻撃に対して実効性のあるインシデント対応ができるように国家情報資産の脆弱性をリアルタイムに状況認識するセキュリティ常時監視の整備が必要である。APT攻撃対策は、静的な紙ベースのPDCAサイクルレベルの情報セキュリティ監査ではほとんど実効性がないためセキュリティ自動化技術に基づくベストプラックティスのツール活用及び意思決定支援のための独自能力開発によるセキュリティ常時監視の仕組みを最優先で整備すべきである。我が国においては、セキュリティ常時監視は米国に比べてほとんど実用レベルの開発が行われていないので、今ある危機に現実に迅速に対応するために米国企業資源の活用も決断する必要がある。	修正意見 （修正なし）	政府機関の情報システムに対するサイバー攻撃は、現在、GSOCにおいてリアルタイムに監視しており、インシデント情報や脆弱性情報等とその対処については、CYMAT、各府省庁CSIRT等で情報共有しております。 なお、GSOCについては、1-①-2)-(ア)に記載のとおり、今後、更なる機能強化を予定しております。 御意見につきましては、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	個人	1	1-①-1)-(ナ)	海外ドメインを中心に普及が進んでいるDMARCについても送信ドメイン認証技術に含めたほうがよいです。	修正意見 （修正なし）	1-①-1)-(ナ)は、送信ドメイン認証技術等の導入により、電子メールに係るなりすましの防止を推進するものです。SPFやDKIMは送信ドメイン認証技術の例示として記載しており、御意見のDMARCを推進の対象から除外しているものではございませんので、記述は原案のままとさせていただきます。
		2	1-①-1)-(ナ)	JEAGは現在は活動休止状態ですので、「JEAG」等と連携しては削除したほうがよいです。	修正意見 （修正有り）	御意見を踏まえ、修正いたします。
13	(株)セールスフォース・ドットコム	1	はじめに	「急速に普及したクラウドサービスやスマートデバイス等」の文章のうち「クラウドサービス」を削除して頂きたい。「クラウドサービスを介した大規模な個人情報の窃取」は少なくとも国内では実例が無いものと考えます。事実に基づかない、いたずらに不安をあおるような表記は適切でなく、従って、「クラウドサービス」という文言を削除することが適当と思われます。	修正意見 （修正有り）	御意見を踏まえ、修正いたします。
		2	1-①-1)-(ク)	情報セキュリティ対策の実施手順（マニュアル等）の中では、情報の区分についても明記すべき。情報のセキュリティレベルの区分けを行った上で、扱う情報のセキュリティレベルによって私物のスマートフォンの利用を許可する業務と、逆に許可しない業務とを切り分ける必要があると考えます。	政策展開に係る意見	各府省庁における私物のスマートフォン等の利用に関しては、御意見の点も含めて検討を行い、実施手順を作成する必要があると考えており、内閣官房においては、そのような点も踏まえて各府省庁を支援してまいります。
		3	1-①-1)-(ケ)	下記文言を追加願いたい。 c)民間事業者が提供するパブリッククラウドの政府利用促進のため、認証プログラムの導入に向けた検討をはじめ、「政府機関の情報セキュリティ対策のための統一基準群」の次期改訂版に反映させる。 （理由）アメリカ、イギリス、シンガポール、オーストラリア等諸外国ではパブリッククラウド認定・認証制度の導入、検討が進んでおり、これにより導入プロセスが整備され、政府のクラウド利用が促進されております。同様の制度を日本でも取り入れることによりクラウド利用が促進されると考えます。	修正意見 （修正なし）	サイバーセキュリティ2014は、セキュリティ水準の向上やサイバー攻撃への対処能力の強化等に関する取組のうち、2014年度に実施するものについて、サイバーセキュリティ戦略の記載体系に沿って詳細を示すものであり、政府情報システムの在り方を示すものではございません。 政府情報システムのクラウド化につきましては、2014年３月に経済産業省が「クラウドセキュリティガイドライン改定版」及び「活用ガイドブック」を、総務省が同年４月に「クラウドサービスの提供における情報セキュリティ対策ガイドライン」をそれぞれ公表し、さらに同年５月に改定された政府機関統一基準群においては、クラウドサービスを含む情報システムにおける外部委託及び約款における外部サービスの利用についての記載を新しくするなどの取組を実施しているところです。 また、本年次計画の1-①-1)-(ツ)に記載しているとおり、クラウドコンピューティングを含む運用・管理を外部に委託している政府機関の情報システムについて、情報セキュリティを確保するための取組を推進することとしておりますので、記述につきましては、原案のとおりとさせていただきます。
		4	1-①-2)-(サ)	内部人材の育成については、通常の政府職員の人事ローテーションとは違う育成方法の考案が必要と考えます。民間では、金融機関でも一般企業でも、IT要員の長期在籍によりその専門性や自社システムへの知識・経験を蓄積しています。従って、政府要員に関しても、単に「人事ローテーションの工夫」に止まらない、より抜本的な対策（IT要員に対する人事異動の長期化）が肝要と思われます。	政策展開に係る意見	情報セキュリティ担当者が長い間情報セキュリティに係る業務に携わることも含め人事ローテーションの工夫や情報セキュリティ担当者に対する評価の在り方については「新・情報セキュリティ人材育成プログラム」においても課題として記載しており、その解決に引き続き取り組んでいきたいと考えております。

番号	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		5	1-①-2)-(ス)	クラウドサービスが浸透する中で、安易な採用や間違った使い方はセキュリティリスクを増大させるが、正しい認識で適材適所で利用することにより、コストを抑えながらセキュリティを向上させることができます。しかしながらクラウドサービスに対する知識が十分とはいえず、結果としてクラウドファースト政策の下、コストを下げながらサイバーセキュリティの強化している諸外国に後れをとっているのではないかと思われます。したがって一般的な教育施策とは別に重点分野としてクラウドサービスに対する教育・意識啓蒙の推進が必要だと思われます。	政策展開に係る意見	クラウドコンピューティングを含めた情報システムに対するサイバーセキュリティに関連した新たな対策技術等に係る教育・意識啓蒙の推進は重要であると認識しており、本年次計画の1-①-2)-(ス)においては、各府省庁の情報セキュリティ担当者等を対象とした勉強会を開催することにより、政府職員の技術・知見等の向上を目的とした施策を掲げておりますので、御指摘の点については、具体的研修内容を今後検討する上で参考にさせていただきま
		6	1-③-(ケ)-b)	b)において情報セキュリティ監査制度の更なる普及に向けた各種対応を必要に応じて行うとあるが「必要に応じて」は削除して頂きたい。情報セキュリティ監査制度の普及に向けた各種対応は、極めて重要な施策であるため。	修正意見（修正有り）	御指摘のとおり修正いたします。
14	慶應義塾大学国際インターネット政策研究会	1	ー	「サイバーセキュリティ2014」を高く評価し、今後も持続されることを期待しています。サイバー脅威は、非常に困難な問題で、サイバー犯罪や諜報活動に限らず、重要インフラへの攻撃にも及ぶ多様なチャレンジです。したがってこの脅威に対抗する強靭なサイバー空間の構築ために、官民による緊密な連携は必要不可欠です。更に今後は、安全確保と、イノベーションの振興、オープンデータの両立も、効果的なサイバーセキュリティ対策を行うための重要事項として取り組まねばなりません。 「サイバーセキュリティ2014」は、サイバー脅威に対する日本政府の制度設計に、包括的な道筋と計画設定を提供しています。特に、日本版NCFTAの創設、重要インフラの保護に対する詳細な提案は、日本のサイバー攻撃への対処能力の強化に繋がります。今後は、日本政府が、国内外のマルチステイクホルダーとの対話を通じて、サイバーセキュリティ2014で掲げた施策の早期実施を期待しています。	賛同意見	本年次計画に賛同する御意見として承ります。 関係府省庁、重要インフラ事業者等との連携を強化し、引き続き、サイバーセキュリティ政策を推進してまいります。
		2	（関連箇所） 4-(ア)	新しいサイバーセキュリティセンターの管轄権を明確化すべきです。 内閣官房のもとで「サイバーセキュリティセンター」の設立が、推進されることを全面的に支持します。同時に、この新たなセンターが、サイバーセキュリティ対策の司令塔としての役割を果たすために、十分な予算と資源を与えることは必要不可欠です。新たなセンターが機能するために、関係省庁のサイバーセキュリティ分野での責任とプログラムを率先する、明確な法的権限も必須です。そして今の日本は、重要インフラの保護、サイバーセキュリティ研究の強化、サイバーセキュリティ人材の育成、適切な標準の設定を行える、アジアと世界をリードするサイバーセキュリティ立国となることが期待されております。したがって日本がサイバーセキュリティ立国となるためにも、政策の立案と実行を管轄するセンターの設立が待たれます。	政策展開に係る意見	NISCの機能強化については、「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」において検討されており、御意見については、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	（関連箇所） 1-①-1)-(ケ) 2-①-(オ) 2-①-(カ)	サイバーセキュリティセンターの主な責務として、政府機関と民間企業のクラウドコンピューティングに対する認証評価を確立するべきです。この認証評価の枠組みに基づいて、政府によるサイバーセキュリティの標準的アプローチの提供と、各府省庁によるガイドライン遵守のモニタリングを委任することが定められます。この枠組みの確立により、クラウドコンピューティングにおける、情報セキュリティと、クラウドサービスの最大限活用によるイノベーションの振興を両立することが可能となります。以上のように、サイバーセキュリティセンターと政府CIOの協力は、各府省庁と民間企業の円滑で安全なクラウドコンピューティングの導入に不可欠となります。	政策展開に係る意見	本年次計画の1-①-1)-(ツ)に記載しているとおり、クラウドコンピューティングを含む運用・管理を外部に委託している政府機関の情報システムについて、情報セキュリティを確保するための取組を推進することとしておりますので、記述につきましては、原案のとおりとさせていただきます。
		4	ー	日本版国立標準技術研究所（NIST）を設置すべきです。 経済産業省所管の情報処理推進機構（IPA）が、サイバーセキュリティにおける情報技術の研究開発と、ITスキル標準化で先導的役割を担うことについて強い支持を表明します。それに伴い現在のIPAには、サイバー脅威によって生じた技術的問題への対処と、その先導的役割を担える程の法的権限と資源を制度上備えていません。そのため政府は、アメリカのサイバーセキュリティ対策で中心的役割を担う米国の国立標準技術研究所（NIST）をモデルとした、日本版のNISTを内閣官房のもとで作り上げる必要があります。	政策展開に係る意見	現在もNISCを中心に府省横断的にサイバーセキュリティ政策を推進しているところですが、今後ともより一層その体制を強化し推進していく予定としています。なお、御指摘の点につきましては、そのような点も踏まえて今後検討してまいります。
		5	（関連箇所） 1-①-1)-(オ) 1-①-1)-(シ)	昨年、成立した特定秘密保護法に関連する情報セキュリティ施策の迅速な立案と推進を支持します。ただし、これらのガイドラインの作成過程に、民間への透明性と意見参加の機会が、最大限含まれる事も望みます。同時に国民や企業への、政府内データの利活用推進政策を、並行して実行する必要もあります。政府内データの利活用を推進することで、オープンデータと効果的なサイバーセキュリティという、安全と自由（国民、ビジネス）のバランスを保つことが可能となります。	賛同意見	政府においては、並行して、政府データの利活用を促進するオープンデータの取組を推進しているところであり、セキュリティと利活用のバランスを取りながら施策を推進する必要があると考えております。 頂いた御意見につきましては、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	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
15	トレンドマイクロ(株)	1	1-①-1)-(サ)	以下の文言を追加。 内閣官房及び関係府省庁～(省略)～などの対策を講じる。また地方公共団体向けには情報セキュリティ対策を講じやすくするため、情報セキュリティ対策の指針や標準を定め、地方公共団体へ普及する。 ＜理由＞ 社会保障・税番号制度導入に当たって重要なのは中央(内閣官房や関係府省庁)側だけではなく、情報を有する地方(公共団体)側も一律で情報セキュリティ対策を行う必要があります。セキュリティ対策の格差が組織ごとで生まれることにより、組織の脆弱性を生み出し、当該脆弱性がマイナンバー制度のシステム全体に影響を及ぼすリスクが生じる可能性があります。そのため、地方公共団体側への指針、標準、プロシージャまで一律で整理すべきと考えます。	修正意見 (修正なし)	内閣官房では、地方公共団体の既存情報システムの改修及び情報提供ネットワークシステムへの円滑な接続に資するよう「社会保障・税に関わる番号制度が情報システムへ与える影響に関する調査研究」を行い、既存システムから中間サーバーへ情報を引き渡すために実装すべき機能等に係る技術標準の検討結果を取りまとめた「既存システム技術標準の検討に係る報告書」を含む各種報告書を策定したうえで、既に地方公共団体に対し情報提供しています。 なお、情報提供ネットワークシステム等の構築にあたっては、地方公共団体に係る中間サーバーのソフトウェアを国が一括で調達することとしたうえで、侵入検知機能を設置し、侵入を検知した際はシステムを一時的にでも停止させる運用とするほか、各機関の情報システムにおいてもアクセス制御及びデータの暗号化を行う等のセキュリティ対策を行うこととした調達仕様書を作成・公表し、これに則ってシステムの構築を進めています。 また、情報提供ネットワークシステムへ接続する全ての機関に対するガイドライン等の整備も計画しており、この中で情報セキュリティ要件を示すこととしています。
		2	1-①-1)-(ハ)-e)	以下の通り追加。 総務省において、地方公共団体から発信する電子メールについて、悪意の第三者が地方公共団体又は地方公共団体の職員になりすまし、一般国民や民間企業等に害を及ぼすことがないよう、SPF、DKIM等の送信ドメイン認証技術の採用等を推進する。 ＜理由＞ 【電子メールに係るなりすまし防止等の対応強化】(6頁)においては、DKIMも含めて記載されており、表記ゆれの修正が必要と考えます。	修正意見 (修正有り)	御意見を踏まえまして、修正いたします。
		3	1-①-2)-(イ)	以下の通り追加。 内閣官房～(省略)～各政府機関に対して当該分析結果を定期的に提供する。尚、共有手法として機械処理可能な形式での情報発信の検討を行う。 ＜理由＞ 共有をより効率的且効果的に実施するために、例えば、米国非営利団体MITREが中心となって策定しているCybOX(http://www.ipa.go.jp/security/vuln/CybOX.html)などを活用する。 指標値について「Atomic indicators」/「Computed Indicators」/「Behavioral Indicators」の3分野について整理を行い、機械処理可能な形式での情報発信が行えるような体制にする必要があると考えます。	修正意見 (修正なし)	内閣官房と各政府機関との間の情報共有はGSOC(Government Security Operation Coordination team)を通じて実施しています。また、現在、「サイバーセキュリティ戦略」等に基づき、GSOCの抜本的強化について検討を実施しているところです。御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	1-①-2)-(ケ)	以下のとおり修正。 内閣官房～(省略)～民間のCSIRTやユーザや情報セキュリティの事業者団体、セキュリティ対策事業者等との日常的な意見交換等により～ ＜理由＞ SOC事業者の団体に限らず、セキュリティ関連の事業者団体との連携が必要です。例えばJUASや日本シーサート協議会、フィッシング対策協議会、ISOG-J、日本ネットワークセキュリティ協会など、事業者団体は複数あり、より公平性と包括性をもたらすための文言への変更が最適と考えます。 また最終的にはセキュリティの製品やサービスを提供している企業と体制構築を行わなければ、異常時の連携も円滑に図られないため、上述同様に広くセキュリティ企業をくくれるような文言に修正すべきと考えます。	修正意見 (修正有り)	御意見の趣旨を踏まえ、修正いたします。

番号	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		5	1-②-(ソ)	以下のとおり修正。 総務省において～(省略)～ISP事業者団体の「テレコム・アイザック推進会議」をはじめとした情報セキュリティ事業者団体、セキュリティ対策事業者等との情報共有を推進する。 ＜理由＞ ISP事業者の団体に限らず、セキュリティ関連の事業者団体との連携が必要です。例えば日本シーサート協議会やフィッシング対策協議会、ISOG-J、日本ネットワークセキュリティ協会など、事業者団体は複数あり、より公平性と包括性をもたらすための文言への変更が最適と考えます。 また最終的にはセキュリティの製品やサービスを提供している企業と体制構築を行わなければ、異常時の連携も円滑に図られないため、上述同様に広くセキュリティ企業をくくれるような文言に修正すべきと考えます。	修正意見 (修正有り)	御意見を踏まえ、修正いたします。
		6	1-②-(テ)	以下のとおり修正。 経済産業省において～(省略)～より有効な活動に発展させるよう、産業分野とセキュリティ対策事業者等の参加メンバーを拡大させるとともに～ ＜理由＞ 組織を狙った標的型攻撃へのより一層の早期対処として、セキュリティ製品やサービスへの反映は必須と考えます。枠組みにセキュリティ対策事業者を加えることにより、製品やサービスへの迅速なフィードバックが行え、連携がより円滑に行えます。	修正意見 (修正なし)	「サイバー情報共有イニシアチブ」(J-CSIP)は、IPAをハブとした、IPAと重要インフラ事業者間で秘密保持契約を結んだうえで、攻撃情報を各分野内または分野横断的に重要インフラ事業者間で共有するものです。 セキュリティ対策事業者は、重要インフラ事業者ではないため、J-CSIPへの参加は想定されていません。なお、J-CSIPの枠組みで情報共有している標的型攻撃例については、レポートとしてIPAより適時、公表しており、今後も情報発信に努めてまいります。
		7	1-②-(ツ)-c)	以下のとおり修正する。 総務省において、電波監視施設の高度化・高機能化や電波における最新の脅威等を踏まえ、電波監視技術や電波特定の脅威分析・調査研究を実施する。 ＜理由＞ 例えばソフトウェア無線を使ったブロードキャスト型の運行システムにおいては様々な脆弱性が確認されております。監視技術の向上も必要ですが、まずは電波におけるリスクや脅威を適切に洗い出し、その上で脅威の早期発見可能な監視技術の検討も必要と考えます。	修正意見 (修正なし)	総務省では、航空・海上無線等の重要無線通信への妨害原因となっている不法無線局等から発射される電波を監視・特定できる技術について、無線通信分野の動向を踏まえ、調査研究を実施しています。御意見については、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	1-④-(テ)-d)	以下のとおり追加する。 e) 経済産業省において、「偽サイト」に対する早期警戒体制と正規事業者や消費者等が被る被害を防ぐための体制検討を行う。 ＜理由＞ 昨今、偽サイトによる被害が増えています。正規事業者が悪質な事業者によって名を騙られたことによって正規事業者が被る被害、悪質事業者によって模造品が販売されることによって正規ブランド保有者が被る被害、悪質事業者とは知らずに消費者が購入手続きをしたことによって消費者が被る被害(粗悪品の購入/金品の搾取/個人情報の搾取など)、様々な被害が発生しており早期に解決を図っていくことが重要です。	修正意見 (修正なし)	当該偽サイトへの対応等については、消費者庁を中心として、対策の検討を行っているところです。
		9	1-④-(ヘ)	以下のとおり修正する。 経済産業省において、IPAを通じ、我が国の競争力の源泉となる組込み機器の脆弱性に関する調査研究と対策の提示等を行う。 ＜理由＞ 通信機能を有する組込機器においてはそこで利用するプロトコルに引きづられた結果、脆弱な状態となっていることもみられます。対策の提示の前にスマート家電やHEMSといった領域での活用が注目されているプロトコル(ECHONET Lite規格 / ZigBee: IEEE 802.15.4など)が潜在的に抱えている脆弱性に関する調査研究が必要です。	修正意見 (修正有り)	御指摘の内容を踏まえ修正いたします。
		10	1-④-(マ)	以下のとおり追加する。 スパムメール送信事業者が官民の組織を詐称して送信を行った際の体制検討のための対策検討を行う。 ＜理由＞ 悪質な事業者によって信頼できる組織を騙って、迷惑メール配信が行われております。これにより、被害相談対応などを受け付けざるを得ない正規事業者が存在しています。企業は商標権や著作権が侵害され出なく、対応によるコスト増や売上の低下などといった、た副次的な被害が発生しており、早急に検討が必要です。	修正意見 (修正なし)	御指摘のような送信者情報を詐称して送信が行われた場合については、特定電子メール法第5条(送信者情報を偽った送信の禁止)や同法第4条(表示義務)等において既に規制対象になっていると考えております。御意見については、参考として承ります。

番号	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		11	1-⑤-(キ)	以下のとおり追加する。 また不正プログラムを使用したプライバシー性の高い個人情報取得に関する事案対応など活動の検討を行う。 ＜理由＞ フィッシング詐欺ではないですが、PIIを狙っているという点でBanking Trojanとフィッシング詐欺について共通性があり、同協議会と連携実績のある業界（金融系）での被害報告が多く、2014年5月には、「インターネットバンキングの不正送金にあわないためのガイドライン」をリリースするなど、すでに対応実績があります。また偽サイト被害の潮流として、これまでは金銭の巻き上げ（含む、粗悪品の販売）が確認されてきております。これに対し、金銭を巻き上げることなく、偽サイトと連携する怪しげなペイメント会社経由で、クレジットカード情報などのPIIを狙った攻撃が確認されています。被害者が金銭的な被害が直ちに発生しないため、自身が被害に遭遇していることに気づきにくいという懸念があります。しかし、個人情報の転売、取得クレジットカード情報の悪用、パスワードリスト攻撃など、その影響は深刻であり、この問題についても活動の幅を広げることも必要と考えます。	修正意見 （修正なし）	フィッシング対策協議会では、御指摘のとおり、「インターネットバンキングの不正送金にあわないためのガイドライン」をリリースし、金融関係の分野とも連携しております。今後とも引き続き連携して取組を進めてまいります。
		12	2-④-(ア)	以下のとおり修正する。 文部科学省において、現行の学習指導要領の改訂を検討し、発達段階に応じ～(省略)～推進する。 ＜理由＞ IT立国、セキュリティ立国を目指すのであれば現行の学習指導要領の範囲内での学習では、将来のセキュリティ技術者、或いはセキュリティ業務従事者に適する素養を幼少時から培うことは非常に困難と考えます。 よって、学習指導要領の改訂を前提により多くのIT学習、リスク教育の時間を割くことが重要と考えます。	修正意見 （修正なし）	御意見については、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	(一財) 日本情報経済社会推進協会	1	1-①-1)-(ハ)-e)	e)の項目について、「地方公共団体から発信する電子メールについて、SPF、DKIM等の送信ドメイン認証技術の採用を推進する。」と明記するべきである。 電子メールに係るなりすましの防止については、(ナ) 政府機関から発信する電子メールに係るなりすましの防止（内閣官房、総務省及び全府省庁）には送信ドメイン認証技術（SPF、DKIM等）の導入を推進すると記載されている。地方公共団体のメールについても同様に、なりすましを防止する手段として、SPF、DKIM等の送信ドメイン認証技術を明記すべきであるため。	修正意見 （修正有り）	御意見を踏まえまして、修正いたします。
		2	1-①-1)-(ナ) 1-①-1)-(ハ)-e) 1-④-(マ)-b)	なりすましメールの防止については、送信ドメイン認証技術に加えて、金融機関に利用されている電子証明書を用いたS/MIMEについても明記すべきである。 さらに、SPF、DKIM等を利用したDMARCの導入や政府機関や地方公共団体が発信するメールがどこから送ったかを明確にするために、発信元の見える化を行う仕組みの導入を促進するべきである。 メール環境は複雑であり、一つのなりすまし防止だけでは不十分である。メール環境に合わせたなりすまし防止技術を導入すべきであるため。 SPFやDKIM等を採用しても、メール送信者が類似するドメインを使いSPFやDKIMを使って、なりすましメールを送ってくる事案もあるため。	修正意見 （修正なし）	1-①-1)-(ナ)は、送信ドメイン認証技術「等」の導入により、電子メールに係るなりすましの防止を推進するものであり、導入する技術を限定しようとするものではございませんので、記述は原案のままとさせていただきます。
		3	資料2「JIPDEC」	「Japan Institute for Promotion of Digital Economy and Communityの略。一般財団法人日本情報経済社会推進協会。電子計算機を用いた各種情報処理方式及び情報処理産業の開発、振興を通じて、情報処理、情報処理産業の発展を図り、もって日本の経済社会の発展に寄与することを目的とする。」を「一般財団法人日本情報経済社会推進協会の英字名称。電子情報を高度かつ安全安心に利活用するための基盤整備や諸課題の解決を通じて情報経済社会の推進を図り、もって我が国の国民生活の向上及び経済社会の発展に寄与することを目的とする。」に変更をお願いしたい。 （理由） 一般財団法人日本情報経済社会推進協会の説明が財団法人日本情報処理開発協会になっているため。	修正意見 （修正有り）	御指摘を踏まえて、修正します。
		4	1-②-(ハ)	以下のように修正。 経済産業省において、日本国内で制御システム等のセキュリティ評価・認証が行えるよう、・・・	修正意見 （修正有り）	御指摘の内容を踏まえ修正いたします。
		5	1-②-(フ)	以下のように修正。 経済産業省において、CSSCによる制御システムのセキュリティに関する評価・認証機関の評価・認証を・・・	修正意見 （修正有り）	御指摘の内容を踏まえ修正いたします。

番号	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
17	（一社）情報処理学会	1	2-①-(サ)	計画としての完成度は高いと思われるのですが、この計画に対するPDCAがきちんとなされているのかについて疑問が残ります。 一例としてリバースエンジニアリングの適法化を挙げます。以下の通り今年も昨年と全く同じ目標が掲げられています。 その他過去に進捗がない施策については，単に繰り返し記載するのではなく、施策をより前進させるための工夫を含めて記述することが望まれます。いずれにしても、問題解決に至らない課題については，安易に断念することなく、繰り返し計画に含め、問題解決に至る具体的取組を促すことを期待します。	政策展開に係る意見	サイバーセキュリティ2013で掲げた施策の中で、十分に進捗が見られないものもあることは御指摘のとおりです。ただし、このように、年度初に施策を公表し、年度終わりにこのように広く評価を受ける仕組み自体には一定の効果もあると考えておりますが、こうした仕組み自体に対する御意見として、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。
18	（一社）知的財産教育協会	1	1-③-(オ)	産業界と政府が一体となって営業秘密保護に関する情報共有・検討を行い、日本における技術・営業秘密保護のための取組を促進することに賛同いたします。 具体的な取組として、次の通り提言申し上げます。 (1) 技術情報・営業秘密等知財マネジメント人材の育成 企業における技術情報や営業秘密の流出は、意図的な漏洩や不正な取得によるものの他、そもそも秘匿化すべき技術情報や秘密情報の区分が十分でないことが原因となっているケースもある。 技術情報・営業秘密の適切な管理については「情報セキュリティ管理基準」にも定められているところではあるが、情報セキュリティマネジメント業務に従事する要員に対して知的財産の知識は要求されていないため、IT上のインシデントの認知及び対応が主となり、知的財産マネジメントの側面からのインシデント評価ができないという課題があると思われる。 よって、情報セキュリティ対策を推進することと併せて、守るべき技術情報や営業秘密等を峻別し、それらを知的財産としてマネジメントする能力を有する人材の育成・確保を推進すべきである。 そうした人材育成・確保のための具体的施策としては、技術保護や営業秘密管理を含む知財マネジメント分野の人材スキルを測る国家試験（例えば、知的財産管理技能検定等）の活用を推奨することも一案である。 (2) 技術・営業秘密等知財マネジメント人材の活用 上述の通り、情報セキュリティ対策と知財マネジメントとは表裏一体の関係にあることから、情報セキュリティ対策の実効性を図るためには、知的財産マネジメント人材（例えば、知的財産管理技能士）を活用し、情報セキュリティ人材との連携を促す取り組みを行うべきである。	政策展開に係る意見	人材育成に関してはあらゆる分野で重要と認識しております。政府においては「新・情報セキュリティ人材育成プログラム」を策定し、それに基づく取組を推進しているところですが、御指摘の知的財産に関する分野とも連携を図りつつ、より良いものとなるようにしていきたいと考えています。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。
19	個人	1	2-③-(ク)	情報処理技術者試験について出願時のアンケートで、合格者へIPAのセキュリティプレゼンター制度への登録、資料送付を行える仕組みを整えてはどうか。情報処理技術者試験の合格者とセキュリティプレゼンター制度を適切に同期させた方が良いのではないか。 内閣官房情報セキュリティセンターにおいても、ITパスポート試験の公式キャラクターを用いた動画コンテンツを作成するなど…（YouTubeへアップする）挙国一致の体制で、情報セキュリティ資格（iパス）の普及を支援してはどうか。	政策展開に係る意見	情報セキュリティに係る普及啓発も重要と考えており、政府においては「新・情報セキュリティ普及啓発プログラム」の策定をする等の取組を行っております。御指摘のITパスポートについても、関係機関で連携し普及に取り組んでいきます。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。
		2	2-③-(ケ)	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。 1. 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。 2. 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。	政策展開に係る意見	情報セキュリティに係る試験制度、資格制度にあたっては、最新の技術動向等を踏まえ、実践的能力を常に評価・担保し、人材の能力の「見える化」を図っていくことが重要と考えております。また、それらの試験、資格が実社会において活用されるよう引き続き取り組んでいきたいと考えています。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。

番号	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		3	2-③-(コ)	情報処理技術者試験については、合格後に継続教育を設ける…とするならば、セキュリティに限らず情報処理技術者の名称、社会的地位など…を国家資格として国（経済産業省）が認定するべき時期が来たのではないか。 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における名称独占（試験区分によっては、必置資格）を認めるなど、国家資格としてはどうか。 【情報セキュリティマネジメント試験について】 ・試験区分の名称を[情報セキュリティプレゼンター試験]としてはどうか。 [情報セキュリティプレゼンター試験] ・ITを利活用しているユーザー企業において、情報セキュリティポリシーの策定や社内の一般利用者の教育、IT技術者と協力してセキュリティ対策を講ずることができる知識を有し、実務において活用できる者。 ・ITを利活用しているユーザー企業の社会人として、情報技術、情報セキュリティに関する一定の知識をもち、部門またはグループ内において、情報セキュリティ環境の維持ならびに、普及啓発を推進する者。 ・ITを利活用するユーザー企業における社会人の受験を奨励していくため、ITパスポートと同様に小問、中問からなる出題形式としてはどうか。 ※日曜日に5時間超え、終日拘束されての受験は、一般のユーザー、社会人の受験者にとって過大な負担となるため。 ・資格の更新制を推奨するため、2020年からのCBT方式を目指した試験としてはどうか。 ・問題作成のコストを抑制するため、情報処理技術者試験の各区分（AD、SU、FE、IP）の過去問題を精	政策展開に係る意見	情報セキュリティに係る試験制度、資格制度にあたっては、最新の技術動向等を踏まえ、実践的能力を常に評価・担保し、人材の能力の「見える化」を図っていくことが重要と考えております。そのため、御指摘の「資格」という点も含め、より最適な仕組みとなるよう、今後省内で検討を進めることとしています。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。
20	（一社）電子情報技術産業協会	1	ー	2015年までの3年間を対象とする「サイバーセキュリティ戦略」の 2年目ということで、NISCを中心に関係省庁・機関及び官民での 情報共有・連携を図り、PDCAによる着実な計画推進を期待する。	賛同意見	本年次計画に賛同する御意見として承ります。 関係府省庁、重要インフラ事業者等との連携を強化し、引き続き、サイバーセキュリティ政策を推進してまいります。
		2	2-④	今後、重要インフラ等へのサイバー攻撃対策に加え、どのようにサイバーセキュリティのリスクを低減するか、いわば、予防という視点での対応強化も必要ではないか。 国民全体へのリテラシー向上への取り組みについて、スマートフォン等の急速な普及に伴い、サイバー攻撃の対象範囲が拡大する中、企業に加え、国民一人一人のサイバーセキュリティに関する早急な意識向上が重要と考える。 地道な活動ではあるが、児童や保護者など幅広い層に合せたリテラシー向上のための教育や広報など、草の根的な取組みの更なる強化も検討頂きたい。	政策展開に係る意見	御指摘いただいたように、産学官民の多様な主体が協力・連携し、社会全体として予防的に対策に取り組む必要性について、「新・情報セキュリティ普及啓発プログラム」において記載しております。同プログラムでは、国民一人一人のリテラシー向上に向け、対象者ごとのきめ細やかな普及啓発活動の推進や、地域における取組の促進等を掲げており、これに沿って、御指摘の点を踏まえつつ施策を推進していきたいと考えております。
21	ソフトバンクBB(株)、ソフトバンクテレコム(株)、ソフトバンクモバイル(株)	1	1-①-2)-(カ) 1-①-2)-(キ) 1-②-(ク)-d) 1-②-(タ)-a)	サイバー演習等を実施する際には、事業者に過度な負荷・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	政策展開に係る意見	民間事業者に過度な負担をお願いすることが無いよう、PDCAを実施しつつ施策を推進してまいります。 御意見については、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。
		2	1-②-(ア)-d) 1-②-(ウ)-a) 1-②-(ウ)-b) 1-②-(ウ)-c)	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。 ただし、仮に事業者間で情報共有することが発生する場合においては、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・徹底すべきです。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。 【理由】 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。	賛同意見	本年次計画に賛同する御意見として承ります。 なお、重要インフラ事業者等との情報共有については、「重要インフラの情報セキュリティ対策に係る第3次行動計画」に記載の情報共有体制に基づき、重要インフラ所管省庁を経由した情報連絡が行われ、「情報連絡を行った重要インフラ事業者等が不利益を被らないよう、情報連絡をした重要インフラ事業者等が特定されないよう情報を加工する等適切な措置を講じた上で情報提供を行う」こととされています。

番号	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		3	1-⑤-(コ)	本来、通信履歴は、通信事業者の取扱中に係る通信の秘密の対象となり、その知得、窃用及び漏えいは、通信の秘密を侵害するものです。しかし、課金目的や苦情対応などの各通信事業者が業務を遂行する範囲内では保存が認められております。 このような背景から、「通信履歴の保存」については、そ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。仮に上述の目的や理由以外の必要性において通信履歴を保存する場合は、事前に十分な法的議論を経た上で、法令等の改正やガイドラインの整備といったステップを踏むべきです。 また、トラヒックが急増する昨今において、新たな目的のために通信履歴を保存することになれば、通信事業者に対し新たに多大なコスト負担・運用負荷がかかることは明白です。よって、本件に関しては、その必要性及び有効性が認められることを明確にし、国民の理解を得たうえで、議論をすべきと考えます。 現状、通信事業者が保持している通信履歴の範囲内であれば発信者情報開示請求の対象となり、また犯罪捜査において、裁判所の発付する令状によって開示されることがあります。本項において想定されている通信履歴の保存の目的は、サイバー攻撃等への対処であり、これは通信事業者の正当業務行為として違法性が阻却される範囲外の行為であると認識しております。 よって、検討を実施するに当たり、まずは「通信履歴の保存」の必要性及び有効性について慎重に議論する必要があると考えます。また、仮に「通信履歴の保存」が必要と判断された場合においても、関係法令の改正及び基準・ガイドライン等の整備など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	政策展開に係る意見	ログの保存の在り方の検討に当たっては、御意見も踏まえつつ、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て検討いたします。
		4	1-④-(ケ)-c) 1-④-(ケ)-d)	普及・啓発活動の実施は非常に重要である認識しており、弊社でもスマートフォン向けにウィルスチェックサービスの提供及び、アプリ利用に関する注意喚起をすでに実施しているところであり、通信関係団体等と連携した取組みに関しては、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。 全国規模や総合的な普及・啓発活動を継続的に実施するためには、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。	政策展開に係る意見	情報セキュリティ普及啓発にあっては、事業者等にそれぞれの社会的立場に応じた役割を主体的に発揮していただくことが第一であると考えております。 そうした主体的な活動に対し支障が生じないよう、頂いた御指摘を踏まえつつ、効率的な方策を検討していきたいと考えております。
22	日本ユニシス(株)	1	1-④-(ネ)	脆弱性検出や取組だけでなく、脅威が深刻な場合には国民への直接的な情報発信を行うことを検討したいただきたい。 先日のIE(Internet Explorer)脆弱性が発覚した件では、米・英・豪政府は直接国民に対して、IEを使用しないよう呼びかけていました。日本政府も同様の対応をしたほうが良いと考えます。 <http://www.huffingtonpost.jp/2014/04/29/internet-explorer_n_5237063.html>	政策展開に係る意見	経済産業省では、IPA及びJPCERT/CCを通じて、JVNへの掲載に加え、注意喚起を発行し脆弱性の影響および対策について直接国民に対し呼びかけを行っています。
		2	1-④-(ハ)-b)	脅威が深刻な場合には、緊急地震速報と同様に政府または関係機関が直接注意を促したほうが効果的と考えます。	政策展開に係る意見	経済産業省では、IPA及びJPCERT/CCを通じて、JVNへの掲載に加え、注意喚起を発行し脆弱性の影響および対策について直接国民に対し呼びかけを行っております。 また、IPAでは、ソフトウェア等の脆弱性に関する情報をリアルタイムで周知する「icat」というサービスを提供しており、今後とも、即時性を持った情報発信に努めてまいります。
		3	1-④-(ナ)-b)	情報収集／分析、米国とのデータ共有について書かれています。しかし、自国としての積極的対応をもっと盛り込むべきと思いました。例えば、先日の米国のように、サーバー攻撃を首謀した者を訴追するなど、積極的な対応も盛り込んだ方が良いと考えます。 アメリカに倣い、海外からのハッカー攻撃等でインシデントが発生した時は、訴追も含めた積極的な対応を取りうることを、明記すべきと思いました。数日前、以下のニュースが流れました。 <http://jp.reuters.com/article/topNews/idJPKBN0DZ1A020140519> 「米連邦大陪審は、米企業にハッカー攻撃を行い企業秘密を盗んだとして、中国軍関係者5人を訴追した。」	政策展開に係る意見	本項目は、国境を越えたサイバー攻撃が増加しており、まずはサイバー攻撃の実態を把握する必要があることから、そのための米国との情報共有の取組を記述したものであり、原案のとおりとさせていただきます。 サイバー攻撃者の訴追などについては、サイバー犯罪の取締りに関する国際連携を推進することにより対応していきたいと考えております。
		4	ー	ネットワーク経由が前提ではないためUSBメモリ等の媒体の管理を考慮する必要があると考えます。媒体による情報漏洩や、媒体に仕込まれたウィルス・プログラムによる不正侵入のリスクがあるからです。	政策展開に係る意見	御指摘の内容に当たるものとして、政府機関統一基準群(平成26年度版)において、USBメモリ等の利用に関する対策について定めております。 なお、「サイバーセキュリティ2014」(案)は、年次計画であるため、政府機関統一基準群等において既に定めている事項について、網羅的に記載はしておりません。

番号	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		5	ー	ファイル共有ソフト、身元詐称ソフト等、情報漏洩の原因や支援するソフトウェアの管理を考慮する必要があると考えます。 最近はあまり聞かれなくなりましたが、ウィニーなどのファイル共有ソフトを使用すると情報漏洩のリスクが高まります。情報漏洩の原因となるS/Wを社員（職員・・・）が勝手に導入できないよう、組織としての管理を徹底するよう記載すべきと考えます。	政策展開に係る意見	御指摘の内容に当たるものとして、政府機関統一基準群（平成26年度版）において、端末で利用するソフトウェアに関する対策について定めております。 なお、「サイバーセキュリティ2014」(案)は、年次計画であるため、政府機関統一基準群等において既に定めている事項について、網羅的に記載はしておりません。
		6	ー	社員（職員・・・）のブログ・SNSへの投稿に対する管理を考慮する必要があると考えます。複数の情報を組み合わせることで機密・個人情報となりうるためです。 業務内容、個人情報などの機密情報を社員（職員・・・）がブログ／SNS（mixi, twitter, Facebookなど）へ書き込むことのないよう、教育をする、周知を図る」などの記載をしたほうが良いと考えます。	政策展開に係る意見	政府機関統一基準群においては、情報の取扱い(ルール)について定めております。 なお、「サイバーセキュリティ2014」(案)は、年次計画であるため、政府機関統一基準群等において既に定めている事項について、網羅的に記載はしておりません。
		7	1-⑤	物理証拠の収集と解析について。 サイバー領域から外れるかもしれませんが、実際の証拠という範囲においては、写真、映像などの証拠についても「収集元（監視カメラ、スマートフォン等）検討」、「収集方法（自動化？）」、「解析技術」なども追求していただきたい。	政策展開に係る意見	警察では、引き続き、捜査に当たっては、必要な証拠の収集、解析等をより効果的に行うよう努めてまいります。
		8	1-⑤	情報漏えい後対策、かく乱技術について。 情報漏えい後の対応策の整備、情報のかく乱技術なども考慮していただきたい。 情報漏えい後の対応も視野に入れることも望ましいと考えます。	政策展開に係る意見	情報のかく乱技術への対応や、情報が漏えいした後に被害実態の解明や被疑者の追跡を図るための方策を含め、あらゆる視点で事後追跡可能性を確保するための検討を行うよう努めてまいり
23	NPO日本ネットワークセキュリティ協	1	1-①-1)-(ケ)-b)	政府共通プラットフォームのセキュリティ確保については、内閣官房のみならず、民間（からも）広く専門的知見を求める（ための方策を強化すべきと考えます） クラウドコンピューティングの利活用については民間において一日の長があります。同プラットフォームの重要性に鑑みて可能な限り広く知見をもとめ、高いレベルの情報セキュリティ対策を講じるべきと考えます。	政策展開に係る意見	御意見については、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。
		2	1-①-1)-(タ)-b) 1-①-1)-(タ)-c)	政府調達におけるPPの確立は、単に海外事例（主に米国）を収集、参考にするだけではなく、その制定過程をも調査し、それを通じて日本に適した基準作りを目指していただきたいと考えます。 また、その認証手続きについても、より民間企業が利用しやすいよう継続的に改善していただくと同時に、認証機関やそれに関わる人材の育成など、様々な方向から推進策を強める必要があると考えます。 現在、調達基準を評価する最有力候補はCC（ISO/IEC 15408）ですが、ST（セキュリティ設計書）の作成が煩雑であるなど、障害が多いのが現状です。政府調達におけるPP の確立はこうした状況を打開する方策のひとつではありますが、国際的な標準化もさることながら、我が国自身の安全保障にも関わる事項であり、固有の事情を加味した物にしていく必要があると考えます。また、現在、国内におけるCC認定が、EAL1や2といった低レベルのものに集中している現実から、認証手続きの簡素化、認証機関	政策展開に係る意見	御意見については、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	1-①-1)-(テ)	暗号の利用について、アルゴリズムの問題に言及されていますが、同時に、鍵管理についても重要事項として言及されるべきと考えます。 いかに強固なアルゴリズムを使用しても、鍵管理が杜撰では無意味です。アルゴリズムもさることながら、暗号鍵の正しい管理方法についての認識を広げていく必要があると考えます。	政策展開に係る意見	鍵管理を適切に行うことの重要性は御意見のとおりと考えます。 CRYPTRECにおいては、御指摘の視点を念頭に置き活動しているところです。
		4	1-①-1)-(ナ) 1-①-1)-(ハ)-e)	メールに対する電子署名の付加、署名検証が可能なメールサービス、ソフトウエアの推進、GPKIルート証明書の一般への配布方法の検討などについても検討いただければと考えます。 ドメイン認証はメール伝送におけるなりすまし経路の排除には有効ですが、一方で、一旦受信され、保存されているメールの真正性を担保するためには電子署名が必須です。暗号化も含め、保存時の問題や、正規の発信者のサーバが侵害を受ける事態までを考えるならば、メール自体の暗号化や電子署名を行うS/MIME等の標準方式のさらなる普及、署名の自動検証が可能なメールソフトやサービスの普及が不可欠です。また、これらにGPKIの枠組みを利用する場合、民間の受信者による署名検証が容易になるように、GPKIのルート証明書が、一般のメールソフトなどに広く配布されるような仕組み、もしくは民間事業者との相互認証のような仕組みを考えていく必要があると考えます。	政策展開に係る意見	御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	1-①-1)-(ナ) 1-④-(マ)	関連組織としてJAEGがあげられていますが、有効性が疑問視されます。 近年情報発信が皆無で有り、ウェブサイトもアクセスできなくなっているなど、活動実態が不明であるため。	修正意見（修正有り）	御意見を踏まえまして、修正いたします。

番号	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		6	1-①-1)-(ネ)-a)	セキュリティ要件遵守の検証方法についても言及が必要と考えます。また、こうしたセキュリティ対応コストを企業等が見積金額に上積みすべきことを明示していただければと思います。 とりわけ安全保障に係る国の情報を取り扱う企業などについて、定期的に監査を実施するなどの保証措置が必要ではないかと考えます。また、民間企業は経済原理で動きます。こうしたセキュリティ対策の実施、運用には人的な資源も含め多くのコストが必要です。とりわけ政府調達において、こうしたコストを算定、計上できる枠組みがあれば、企業がそのコストを上積みできるだけでなく、審査に当たって、その内容から考慮されている対策を評価しやすくなり、最終的にはセキュリティ向上に資するものと考えます。	政策展開に係る意見	本年次計画の1-①-1)-(ス)で、各府省庁において、システム予算全体の中で必要な情報セキュリティ対策を確保できるよう、「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」を活用することを推進しており、内閣官房において、同マニュアルが情報システムに係る政府調達で広く活用されるよう、本マニュアルの利便性・簡便性の向上、内容の充実や、各府省庁における普及・利用の促進を図るなどの取組を行っていくことを記載しています。
		7	1-①-2)-(オ)	対象が「希望府省庁」となっていますが、原則全省庁が参加すべきと考えます。 Web改ざんが多発する昨今の情勢を考えると、政府機関のWebサイトは格好の水飲み場攻撃対象であり、内容の如何に関わらず、十分な対策が必要です。政府機関のサイトがマルウエア配布等に利用されれば、その影響は計り知れません。	政策展開に係る意見	1-①-2)-(オ)は、内閣官房が実施する脆弱性検査の実施について記載しており、別途、府省庁が自主的に実施している脆弱性検査もあることから、「希望府省庁」としております。内閣官房が実施する脆弱性検査の対象範囲の拡大は、御意見を参考にしつつ、検討させていただきます。
		8	1-①-2)-(シ)	「情報セキュリティに関する素養」の意味の明確化と確認方法、確認手段について具体的に例を記載することを検討してください。 採用時の確認事項とありますが漠然としていて、その確認方法や基準についての方向がわかりません。人材育成の目標としても一つの指針となるので明確にしていただきたいと思います。 （例：重要情報の取り扱い、ルールの遵守などに関する考え方を公務員試験で記述させるなど）	政策展開に係る意見	既に、採用時において情報セキュリティに関する資格の確認等を行っているところですが、引き続き「情報セキュリティに関する素養」の確認に努めていきたいと考えています。
		9	1-①-2)-(ス)	定期的な教育内容自体の見直し、更新についても言及すべきです。 情報セキュリティの分野は常に新しい脅威が登場するため、教育内容が古くならないようにすることはきわめて重要です。	政策展開に係る意見	1-①-2)-(ス)の施策において、内閣官房が支援等を行うことにより、内閣官房が持つ新しい脅威等に関する知見を踏まえた教育内容としております。「サイバーセキュリティ2014」(案)の記載については、原案のとおりとさせていただきます。
		10	1-①-2)-(セ)	現場の実務面を統括、管理する人材についてのキャリアパスの確立が必要と考えます。その上で、こうした人材は国として保有し、継続的に施策を推進できる体制を構築すべきであると考えます。 従前からの状況を見ると、NISCも含め、情報セキュリティを担う各省庁部局における人材の入れ替わりが激しく、マネジメントを含めたノウハウの蓄積が阻害されているように見受けられます。こうした部分、特に現場のマネジメントは技術的な素養、知識も不可欠であり、人材育成には長い期間を要します。また、本来、こうした部分はその組織として担保されなければ、いくら技術的に優秀な民間人材の手を借りても、有効に機能しません。将来的な処遇も含め、こうした人材が自らの人生設計をできるような仕組み作りが重要だと考えます。	政策展開に係る意見	情報セキュリティ人材のキャリアパス提示については「新・情報セキュリティ人材育成プログラム」においても課題として記載しています。引き続きこれらの課題に取り組んでいきます。
		11	1-①-2)-(ソ)	専門的な人材の有期、無期の途中採用制度の拡充が必要と考えます。 外部人材の活用は、早期にセキュリティ管理・対策・運用の強化を行う上で不可欠ですが、米国など先進的な国の状況を見ると、官・民・学の間で、活発な人材の移動がみられます。こうしたことが、間接的に各界のセキュリティ担当者の意識や能力レベルを平均化し、NCFTAのような取り組みが機能する素地になっていると考えられます。現在、外部人材登用に際し、民間からの出向者受け入れという方法が多く見られますが、一方で、長期出向によりこうした人材が出身企業内で自らのキャリアパスを構成する障害となる場合もあり、こうした方法のみに頼るのではなく、優秀な人材を積極的に国として採用、雇用していくことが必要と思われます。	政策展開に係る意見	情報セキュリティ人材のキャリアパス提示については「新・情報セキュリティ人材育成プログラム」においても課題として記載しています。また、NISC自身も高度な情報セキュリティ人材のキャリアパスの1つになるよう更なる取組を推進することとしています。引き続きこれらの課題に取り組んでいきます。
		12	1-①-2)-(タ)	「カウンターインテリジェンス推進会議」及び「カウンターインテリジェンスセンター」との関係についての解るように記載することを検討してください。 既にある「カウンターインテリジェンス推進会議」及び「カウンターインテリジェンスセンター」の仕組みと別な仕組みを作ることを意味するのか分かりにくいので明確に記載していただきたい。	修正意見（修正有り）	「カウンターインテリジェンス推進会議」及び「カウンターインテリジェンスセンター」との関係について分かるよう修正します。
		13	1-①-3)-(ア)	実際に実務面からCIOやCISOの補佐を行う補佐官の専門性についてのクライテリアや報酬基準を明確化することが必要だと考えます。 現在、多くの省庁でCIO補佐官等が民間から登用されていますが、こうした人材のクライテリアが明確でなく、またその業務に比して報酬が低すぎるケースも見受けられます。非常に重要なポジションであり、より高い資質を持った人材を登用できるよう、継続的な改善が必要と思われます。	政策展開に係る意見	CISOアドバイザーは非常勤の国家公務員として採用するため、その報酬額は給与法等に基づき採用予定者の専門性や経験等に応じて算定されていると承知しています。他方で、より高い資質をもった方に応募いただくことは重要であると考えており、御指摘の点について、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	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		14	1-②-(ト) 1-②-(ニ)	脆弱性対応、インシデント対応コーディネーションのさらなる迅速化とそのためのリソースの確保が必要と考えます。 昨今のサイバー攻撃の特性(標的型攻撃、ゼロデイ攻撃の多発)を考えると、現在のコーディネーションの枠組みでは、対応に時間がかかりすぎる可能性があります。米国DHSがUS-CERTを立ち上げたように、自発的な活動には限界があり、より多くのリソースを割けるような仕組みを国主導で立ち上げることも検討する必要があるかもしれません。また、一般企業で対応できる人材が不足してる状況も顕著で、こうした対応の相手方となる人材の育成を支援するなどの活動も積極的に行っていく必要があり、これらにも多くのリソースが必要になると考えます。	政策展開に係る意見	海外案件等は時間を要するケースも多くリソースの確保は重要な課題であり、対応状況を踏まえ検討を行ってまいります。
		15	1-③-(ア)	複数の中小企業が共同でセキュリティ対策への投資を行い負担を軽減できるような枠組みが必要ではないかと考えます。 昨今、産業分野をまたがるサプライチェインの中で、優秀な技術を持つ中小企業の重要性が高まりつつありますが、一方、こうした中小企業が情報セキュリティに割けるコストは僅かです。情報を供給するだけでなく、こうした中小企業が共同でセキュリティシステムを運用したり、共同対処できるような仕組み(企業コンソーシアムや、中小企業グループを対象とした安価なセキュリティサービス事業)の育成など、具体的な施策を打っていく必要があると考えます。	政策展開に係る意見	御意見については、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	1-③-(カ)	こうした制度がもたらす効果だけではなく副作用についても慎重に検討をお願いします。 企業の経営層の意識を変え、情報セキュリティ投資を引き出すための有効な手段になりうる一方で、情報セキュリティに関する知見の少ない企業経営層の過剰反応を引き出したり、実際のセキュリティ対応ではなく、事務作業の繁雑化による過度のコストが生じるなどの副作用が懸念されます。JSOX対応時にも同様のことが発生しており、こうした副作用についても慎重に検討されるべきだろうと考えます。	政策展開に係る意見	上場企業におけるサイバー攻撃によるインシデントに関し、事業等のリスクとしての開示を行うことの可能性については、現在、米国の証券取引委員会(SEC)における取組等を参考にしつつ、検討を行っているところであり、御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	1-③-(ス)	CISOとなるべき人材像を明確にしていく必要があると考えます。 現在、民間企業でCISOが十分に機能していないケースが散見されます。これはCISOとなるべき人材のクライテリアが明確でない点に起因します。経営層の一員であると同時に、情報セキュリティ(とその対象となるビジネス)について広範な知識が必要なポジションであり、専門性、業務経験なども含めその人材像を明らかにしていくことが重要だと考えます。それにより、一般企業において、こうした人材を雇用する風土が醸成できると考えます。	政策展開に係る意見	経済産業省において、情報セキュリティを推進する観点から、「CISOの設置・導入に関するガイダンス」を作成し、CISOの求められる能力等を整理しております。
		18	1-③-(ソ)	国としてのツール開発、配布は慎重に行っていただきたい。むしろ民間事業者が、低コストのサポートを提供できるように国として支援をお願いしたい。 無償ツールの提供は中小企業に対しては、ある程度は有益ですが、それらを使いこなす力がない企業も多いのが現状です。また、民間のセキュリティ事業者のビジネスと重なる部分もあり、民業を圧迫しない配慮が必要です。こうしたツールを開発、提供することもひとつの方法ですが、経済産業省としては民間事業者を経済的、制度的に支援することで、コストの低減による対策を促進していくことをまず考えるべきです。	政策展開に係る意見	脅威等への気付きを与えるツール提供によって、民間事業者が提供する本格的なツール等への投資に誘導することを目的としています。
		19	1-④-(ク)-c)	高齢者向けにとどまらず、青少年向けにも促すような記述をお願いします。 スマートフォン等の情報端末の普及やSNS等のインターネットの利用は目覚ましく低年齢化が進んでいます。高齢者と同様に青少年に向けても、より、わかりやすい言葉で、また必要以上に新技術の活用を萎縮させることがないような啓発活動が必要ではないかと考えます。	修正意見 (修正有り)	青少年、特に児童・生徒に対する啓発活動は極めて重要であると考えております。御指摘を踏まえ、以下のとおり新たな項を設けさせていただきます。 e) 内閣官房において、各府省庁や事業者等と連携し、保護者や学校の教職員、児童生徒を対象とした啓発活動や、学習・参加型のシンポジウム等を引き続き推進する。
		20	1-④-(ス)	こうしたツールの作成、配布には民間企業を活用していただきたい。 国からの安易なツール提供は民業圧迫を引き起こしかねないと危惧します。むしろ、民間企業に対して、こうしたツールの作成、配布を支援するような制度を作るべきではないかと考えます。	政策展開に係る意見	脅威等への気付きを与えるツール提供によって、民間事業者が提供する本格的なツール等への投資に誘導することを目的としています。
		21	1-④-(ヒ)	開発(IT)技術者全般について、セキュリティ知識、意識の底上げを行うような施策が必要と考えます。 開発技術者に対する情報提供は重要ですが、一方的に発信するだけでは限界があります。たとえばIPAが実施している情報処理技術者試験の「セキュリティ」資格ではない一般の技術資格の要件に、その分野のセキュリティ知識(たとえば、ソフトウエア技術者ならセキュアコーディング、データのアクセスコントロール手法など)を必須とし、これまで以上に重要度をあげていく必要があるでしょう。この場合、既取得者へのフォローアップなども考えるといいと思います。(追加資格の認定など)	政策展開に係る意見	底上げの必要性に応えるため、ガイド等の策定、普及啓発を実施しています。提供を行っているガイド等については、最新規格が発行された際に改訂等を行っています。 情報処理技術者試験では、昨今の情報セキュリティの重要性の一層の高まりを踏まえ、2014年度から同試験の全試験区分において「情報セキュリティ」に関する出題の強化・拡充を図ったところ

番号	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		22	1-⑤-(イ)	こうした取り組みに参加する組織間の人的交流を増やし、参加組織のレベル、意識を高めていく施策が必要です。とりわけ、ITが本業ではない、重要企業のセキュリティ人材確保を支援するような施策も必要と考えます。 米国におけるNCFTAは、官・民・学の人材のダイナミックな移動により情報セキュリティの技術や意識レベルの平均化が行われていることで成り立っている部分が多いと聞きます。互いに、状況がわかっているから情報交換がスムーズに行っている側面が強いようです。日本で、IT企業以外のたとえば重要インフラ企業等も巻き込んだ形を考えていくならば、こうした人材交流(移動)の活性化や、IT企業以外でのセキュリティ人材の雇用促進などの施策も重要ではないかと考えます。	政策展開に係る意見	米国NCFTAが成功した理由として、情報セキュリティを本業としない、サイバー空間の脅威による被害を最も受けやすい立場にある企業が米国NCFTAの意義や効果を認め、積極的に活動に参画していることが指摘されております。日本版NCFTAについても、この種の企業がその意義・効果を認め、積極的に参画することが不可欠であると考えられますので、御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	1-⑥	この項において実施される研究や機能強化、及びそのための基盤、設備等の整備では、可能かつ妥当な範囲において、民間事業者が(広く)参画し実現できることを希望します。 防衛研究は、民間に委託される場合にも、その対象や範囲、委託先が限られているのが実態です。一方、サイバーセキュリティの研究においては、多くの技術や知見が民間に広く存在します。このため、研究開発にあたっては民間や学術界の知見を集めることも不可欠です。防衛研究という特性から、機密保持なと検討すべき問題はありますが、研究開発の体制作りにおいては、こうしたことも念頭に置かれるべきと考えます。	政策展開に係る意見	御指摘のとおり、自衛隊等の態勢の強化には、民間事業者による技術や知見が必要不可欠と考えております。これまでも省内において、調達の競争性や透明性を確保してきたところですが、御指摘を踏まえ、さらなる民生技術の積極的な活用に努めつつ、独法等の研究機関とも連携を深めながら、研究開発事業を推進してまいりたいと考えております。
		24	資料2	巻末に用語解説があるので、目新しい用語について、積極的に盛り込んでいただきたい。 たとえば、以下のような用語について解説を追加いただきたい。 「スマートコミュニティ」「スマートセンサー」「JASPER」「リカレント教育」等 最近の用語については、誤解を避けるため、なるべく多く、用語解説に加え、その定義を明確にした方がいいと考えます。	修正意見 (修正有り)	御意見を踏まえ、「スマートコミュニティ」「スマートデバイス」「スマートメーター」「JASPER」「リカレント教育」の用語を追加いたします。
		25	2-①	この項目に列挙されている(ア)～(サ)の内容が、どのようの「産業活性化」に結びつくのかを示す必要があると考えます。また、それぞれの項目に列挙されている「研究開発」を行う主体をどのように(どのような方針で)選ぶのかについても言及していただければと思います。 こうした研究開発を産業活性化に結びつけるためには、民間が自ら研究、開発を行う活動を行政として支援していくことが重要です。決して、国としての研究開発が直接的に産業活性化に結びつくわけではありません。また、こうした施策を通して、情報セキュリティに関わる業界の活性化も必要です。ITにおいて、様々な技術が密接に結合している現在、それぞれの分野ごとの研究を、その分野ごとに閉じるのではなく、広くIT，情報セキュリティ分野の知恵を結集する体制が必要です。そいう意味で、この項目は、その方向性をより具体的に明示すべきではないかと考えます。	修正意見 (修正なし)	今後の施策の検討の参考とさせていただきます。なお、「情報セキュリティ研究開発戦略(改定版)」においても、民間による応用や実用化を意図した研究においては、研究テーマの検討、ニーズの分析などを含め、更なる民間の関与が必要である旨記載しております。
		26	2-①-(イ)	半導体デバイスの研究開発においては、その設計段階から様々な脅威を想定し、リスクを評価していただきたいと考えます。また、こうした検討に際しては、広くIT分野の知見を結集できるような体制作りが不可欠です。 半導体デバイスは開発に多大なコストが必要な上、一度作ると容易に改修できない特性があります。そうした問題の発生を最小限に抑えるため、設計段階での脅威分析を十分に行い、設計に反映させることや、万一、実用化後に設計上の欠陥が発覚した場合のことも念頭に、ソフトウエアとの組み合わせで改修を容易にすることなどが検討される必要があります。また、こうした研究には、半導体技術分野の知識のみでなく、IT全般のセキュリティ知識が不可欠であり、そうした幅広い人材を含めた形での体制作りが肝要です。	政策展開に係る意見	御意見については、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。
		27	2-①-(コ)	制御システムのみでなく、その周辺のシステムやネットワーク、今後高度化して行くであろう様々な情報系システムを含めて幅広い検討を進めていただきたいと思います。 自動車の情報セキュリティについては、制御系システムがクローズアップされる傾向がありますが、一方で、自動車に搭載される情報系システム、たとえばカーナビゲーションその他の情報端末も、その多くがネットワーク等と結びついて、データ収集、サービス提供が行われています。たとえば、カーナビゲーションに送られる渋滞情報が改ざんされることによる、交通混乱のリスクといった部分も検討に含める必要があります。インターネットやPC,スマートフォンなどとの連携も進むと考えられ、研究に際しては、様々な分野のセキュリティノウハウを結集できる体制作りも必要になります。	政策展開に係る意見	御意見については、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	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		28	2-①-(サ) 2-②-(ケ)	こうした研究で行われる作業のうち、リバースエンジニアリングについては、情報セキュリティ目的で行う場合の適法性の明確化が検討されているが、「攻撃トラフィック収集・解析、マルウエア検体等の収集・保持」についても、同様に適法性について検討し整備いただきたいと思います。 いわゆる、ウイルス作成罪その他によって、コンピュータ・ウイルスの作成保持、供用等が処罰対象とされる可能性があるが、情報セキュリティ上の研究のためには、「攻撃トラフィック、マルウエア検体等」について調査研究が必要であり、それらを収集、保持もしくは研究目的で作成することがあり得ます。また、研究開発基盤を通じてこれらを共有するための法的裏付けについても検討していただきたいと思います。	政策展開に係る意見	御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。
		29	2-③	高度な技術に特化した人材のみでなく、幅広い知識を有し、総合的な判断を下したり、現場を統括、指揮できる人材、さらには、サイバーテロのような広範囲かつ同時多発的なインシデントに際し、総合的な見地から全体を統括したり、リソース配置を最適化したりするような役割を果たす人材の育成についても推進をお願いします。 情報セキュリティ対策やその運用、インシデントへの対応をスムーズに進めるためには、様々な人材を組織的に動かす必要があります。そういう意味で、現在の我が国における人材育成策は専門特化した技術者に偏っていると言わざるを得ず、実際の現場で、こうした技術者に役割を与えて全体を把握できるセキュリティのジェネラリスト(チームリーダー)や、こうした現場チーム全体を統括して、大きな組織や社会で発生する事態に即応し、資源配分も含めて管理する司令部的な役割を担う人材などについての育成が急務であるといえます。とりわけ大規模なインシデントにおいては、現場技術者の自律的連携には限界があり、こうした階層的な管理体制が不可欠です。	政策展開に係る意見	「新・情報セキュリティ人材育成プログラム」においては、情報セキュリティに対する経営層の意識改革とともに、経営層と実務者層との間をつなぐ実務者層のリーダー層の育成が需要と認識しており、そのための施策を推進していくこととしています。
		30	2-③	人材の育成は、魅力ある採用環境の整備が必須条件であり、セキュリティ技術者の社会における地位向上策を検討する必要があります。 大学での情報セキュリティに関する教育、協議会・演習などによる専門家の育成などの施策が充実してきている一方、これらの専門家の社会における採用環境や、社会的地位などが、欧米諸国とくらべ十分に処遇されているとは言えません。たとえば、IT企業以外の企業や公共団体等が、最低限の専門家を雇用するような風土作りも施策として考えていただきたいと思います。 我が国がサイバーセキュリティ立国を目指すにあたり、セキュリティ専門家に対する社会的地位の向上のための施策を是非検討願います。	政策展開に係る意見	「新・情報セキュリティ人材育成プログラム」においては、情報セキュリティに対する経営層の意識改革についても課題としており、経営戦略の一部としての情報セキュリティ対策の推進を図るための取組を行っていくこととしています。
		31	2-③-(ク)	情報セキュリティ専門家の地位向上のため、情報セキュリティ資格の実務的な権威づけの検討をお願いします。 情報処理技術者試験や(民間資格)について一層の周知及び普及を図るとありますが、これらの試験に合格した者の社会における地位を高めるために、国の入札資格として保有者の参画を義務化する、保有人数によって発注単価を高くするなどの実務的な権威づけの手段を検討いただければと思いま	政策展開に係る意見	情報セキュリティに係る試験制度、資格制度にあたっては、最新の技術動向等を踏まえ、実践的能力を常に評価・担保し、人材の能力の「見える化」を図っていくことが重要と考えております。そのために最適な仕組みとなるよう、関係省庁等と今後検討を進めていくとともに、適切なフォローアップをしていきます。
		32	2-④	一般IT利用者のリテラシー向上のみならず、IT技術者全般の情報セキュリティリテラシー向上のための施策を進めていただきたいと考えます。 現状においてIT技術者全般の情報セキュリティに関するリテラシーの低さが大きな問題ではないかと考えます。開発・構築・運用現場の意識が低いことが原因とみられる脆弱性、不注意などに起因するインシデントが後を絶たないことや、セキュリティ専門家の総数に対し、IT技術者の総数が圧倒的に多いことなどを考えれば、脆弱なソフトウエアやシステムを作らない最低限の注意は、IT技術者のリテラシー問題として位置づけられる必要があり、こうした啓発活動は、きわめて重要と考えます。	政策展開に係る意見	企業等の職員向けの普及啓発として、情報セキュリティに関する最新の動向や具体的な事例についての学習等の取組について、「新・情報セキュリティ普及啓発プログラム」において詳しく記載しております。 本プログラムの推進の中で、御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。
		33	2-④	昨今、社会問題化しているネットバンキングを悪用した不正送金問題について取り上げてください。 ウイルスによるネットバンキングの不正送金被害は、警察庁によれば、2014年5月9日時点で確認された今年の被害額は14億1700万円を超え、2013年の被害額14億600万円を上回ったと言われています。2014年度のサイバーセキュリティにける利用者のリテラシー向上の最重要課題であることから、是非、施策として明示し取り上げていただきたいと思います。	政策展開に係る意見	御指摘のようなサイバー犯罪防止のための広報啓発の推進に係る施策については、「新・情報セキュリティ普及啓発プログラム」においてより詳細に記載しております。例えば、インターネットバンキングや通販サイト等、個人の財産を狙ったサイバー犯罪に利用されやすいサイトに関する普及啓発に触れさせていただいており、今後も着実に推進していくこととしております。
		34	3-② 3-③	民間における各国のセキュリティ団体、業界団体等との交流促進に関する支援も行っていただきたいと考えます。 情報セキュリティ分野の国内企業は中堅企業も多数あり、個別の海外進出には困難が伴います。こうした企業が多く参加する業界団体の国際交流を国として支援していただければ、優れた技術を持つ国内中堅企業の海外進出を後押しできるだけでなく、業界を通じた民間交流・連携の促進にもつながりま	政策展開に係る意見	御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	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		35	4章 （関連箇所） 1-①-2)-(セ)	1-①-2)-(セ)で述べられているとおり、各施策を担う組織における国としての人材、技術、知見の中長期的な維持、確保を念頭に推進体制を構築していただきたく考えます。 中期的な施策の一貫性の確保や、各組織の効率的運用を考えれば、短期間の人材入れ替わりによる体制再構築が頻繁に発生することが、最大の障害であると考えます。	政策展開に係る意見	情報セキュリティ担当者が長い間情報セキュリティに係る業務に携わることも含め人事ローテーションの工夫や情報セキュリティ担当者に対する評価の在り方については「新・情報セキュリティ人材育成プログラム」においても課題として記載しており、その解決に引き続き取り組んでいきたいと考えております。
24	（一社）新経済連盟	1	1-①-2)-(オ)	検査対象：検査対象を全府省庁のすべての公開ウェブサーバとすべき。もしくは、別途、検査対象外になる公開ウェブサーバにおける脆弱性を確認する手段を確立すべき。 検査内容：サーバ脆弱性とWebアプリケーション脆弱性の両面での対応をすべき。 対処時間：脆弱性への対処時間は短くするべき。OS等の脆弱性に関しては、ホストベースの仮想パッチ技術などを用い、脆弱性への即時対応が必要。 原案では、対象が「希望」府省庁の「主要」な公開ウェブサーバとされており、事実上、各府省庁の判断に検査対象がゆだねられており、希望がなければ検査が実施されないことになってしまう。この結果、検査対象外の公開ウェブサーバが残り脆弱性が解消されないおそれがある。公開ウェブサーバの場合、外部にさらされた状態にあるため、サーバ脆弱性だけでなくWebアプリケーション脆弱性の対応も必要である。脆弱性検査だけでなくその結果を踏まえた対応の早期実施を行わないと意味がない。	政策展開に係る意見	1-①-2)-(オ)は、内閣官房が実施する脆弱性検査の実施について記載しており、別途、府省庁が自主的に実施している脆弱性検査もあることから、「希望府省庁」としております。内閣官房が実施する脆弱性検査の対象範囲の拡大は、御意見を参考にしつつ、検討させていただきます。
		2	1-③-(カ)	制度設計の際は事業運営に与える負担や影響を十分に留意し、導入の際に極力混乱がないよう留意いただきたい。また、リスクの公開に際しては、情報セキュリティ対策が確立している企業に対してメリットがあるような仕組みにすべきである。 (理由)事業運営に与える負担や影響が増える一方で、実質的なセキュリティ対策につながらないことになっては本末転倒であるため、負担・影響、公開のインセンティブ等について十分留意する必要があ	政策展開に係る意見	上場企業におけるサイバー攻撃によるインシデントに関し、事業等のリスクとしての開示を行うことの可能性については、現在、米国の証券取引委員会（SEC）における取組等を参考にしつつ、検討を行っているところであり、御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	1-③-(ソ)	検出ツールは民間の知見と創意工夫を活用することにも留意いただきたい。また、昨今のweb改ざん事案の多発に言及するとともに、啓発活動についても明記いただきたい。 検出ツールについては、既存のセキュリティ企業において多用なソフトが提供されている。web改ざんについては、ここ数年、我が国において、改ざんされた正規のwebサイトを経由したマルウェア感染が広がっているが、必ずしも企業で十分に問題視されていない現状がある。	修正意見（修正なし）	脅威等への気付きを与えるツール提供によって、民間事業者が提供する本格的なツール等への投資に誘導することを目的としています。なお、注意喚起については、本年次計画の1-④-(ト)を参照ください。
		4	1-④-(エ)	ソフトウェア教育の更なる推進（総合的学習の時間等の活用、官民連携、プログラミング等とあわせた情報関係科目としての導入の検討等）に言及いただきたい。 新経済連盟ではかねてよりプログラミング教育の導入を提言しているが、情報セキュリティの推進のみならず、我が国の経済発展に大きく資すると考えるため。また、プログラミングは論理思考を鍛えることにもつながるため、プログラミングは重要と考える。	修正意見（修正なし）	ソフトウェア教育については、「新・情報セキュリティ人材育成プログラム」に記載しており、本プログラムを推進する中で引き続き検討を進めていく所存です。 御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	1-④-(ケ)	スマートフォンにおけるウイルス対策ソフトの利用を促す啓発と、ネットにおけるリテラシーを授業で教えることについて言及すべきである。 スマートフォンは、パソコンと比較して、まだウイルス対策ソフトを導入しなくても良いという意識の人が比較的多い。諸外国では、WEBでの公共マナーを教えており、ネットでの人とのつきあい方のようなものを授業で行うことは重要である。少なくともパソコンもスマホもウィルス対策ソフトを入れる教育を小学校レベルから徹底し、マスコミを通じてそれらを啓発すべき。	修正意見（修正なし）	スマートフォンにおける情報セキュリティ対策の必要性については、情報セキュリティ月間のイベント等を通して、普及啓発に努めているところです。 また、「新・情報セキュリティ普及啓発プログラム」の取組を通して、初等中等教育段階における教育を始め、強化してゆく所存です。御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	1-④-(ス)	a）について、「IPAを通じて当該機能を有するツールの利用を促進する」というコンテキストの文章になるよう改正いただきたい。 まずは対策の必要性の訴求が必須である現状がある。また、対策手法についてはセキュリティベンダーを含む民間の知見や創意工夫を活用することがより高い効果を期待できる。	修正意見（修正なし）	脅威等への気付きを与えるツール提供によって、民間事業者が提供する本格的なツール等への投資に誘導することを目的としています。
		7	1-⑤-(コ)	具体的な導入についてはきわめて慎重な議論が求められるべきである。 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となるおそれがあるので、多角的かつ慎重な議論が必要である。	政策展開に係る意見	ログの保存の在り方の検討に当たっては、御意見も踏まえつつ、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て検討いたしま

番号	提出者	枝番	該当箇所	御意見の概要	意見の種類	御意見に対する考え方
		8	1-⑥-(ス)	サイバー空間関連事業者など関係機関の役割の整理・明確化を行うにあたっては、自由な情報流通の確保との関連で十分なバランスをとることが前提である旨明確に記述するべきである。 サイバー攻撃対策との名目で国民の自由な情報流通やアクセスへの不当な介入や制限、民間事業者や個人に対する萎縮効果を引き起こすような政策が実施されてはいけない。	修正意見（修正なし）	「サイバーセキュリティ戦略」（2013年6月）は、情報の自由な流通の確保、深刻化するリスクへの新たな対応、リスクベースによる対応の強化、社会的責務を踏まえた行動と共助を基本的な考え方としています。 現在、IT利活用とサイバーセキュリティの両立を図るべく、NISCを結節点としてサイバー空間の各主体が連携して取組を進められるよう、NISCの機能強化を検討しております。 御意見につきましては、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	4-(エ)	セキュリティ事業者のみならず、事業者の過度な負担とならない範囲で必要に応じてユーザー企業とも連携を行い、我が国全体として安全なサイバー空間を実現できるようにしていただきたい。 過去の取り組みでは官民連携とは基本的に関連企業との連携であるが、大多数を占めるユーザー企業のセキュリティを底上げすることが我が国のセキュリティレベルを上げるために重要である。	政策展開に係る意見	サイバー空間を構成する各主体との連携の在り方については、NISCの機能強化の議論とあわせて検討を進めております。 御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。
25	個人	1	1-①-1)-(ニ)	政府機関だけでなく、金融機関等の国民が利用する重要なサービスを提供するドメインも属性型のco.jpを利用するよう推進すべきではないか。	政策展開に係る意見	ドメイン名についてはICANNのルールのもと、各主体の判断で取得されており、強制は馴染まないと考えます。 いただいた御意見については、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。
		2	1-④-(マ)	スパムメールや詐欺メールの送信行為で得られる対価と見合わなくなるように、厳罰化等を検討して頂きたい。	政策展開に係る意見	2008年の特定電子メール法改正時に、同法の措置命令に従わない者への罰金額を引き上げておりますが、頂いた御意見については参考として承ります。
		3	2-③-(コ)	資格によっては維持コストばかりがかかり、取得者当人にメリットの薄いものも多い。 バランスの取れた仕組みとなることを期待する。	政策展開に係る意見	御意見については、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	(一社)ITセキュリティセンター	1	1-①-1)-(タ)-c)	下記を追加する。 「また、非認証製品が調達されている場合、その原因を調査し、認証製品が活用されるよう改善策を検討する。」 <理由> 我が国では以前から認証製品の調達はほとんど行われていないと思われる。一方、米国のIT製品調達の規定(CNSS Policy No.11)は非常に簡潔であるにも関わらず、有効に機能している。我が国で評価を依頼するほとんどの申請者(IT製品ベンダ)は、「主に米国に輸出するために認証を取得している」と述べていることが上記の状況を裏付けている。JISECは、我が国政府システムのセキュリティ品質向上に寄与すべくIT製品の調達方法を見直す必要がある。 cryptome.org/2013/07/CNSSP-11.pdf	修正意見（修正なし）	御意見については、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。

※その他、個人等3者から5件の意見