「情報セキュリティ研究開発戦略（改定版）（案）」に係る意見募集の結果一覧

資料4－2

番号	提出者	該当箇所	ページ数	ご意見	意見の種類	修正の有無	御意見に対する考え方及び修正（案）
1	個人	2（1） 情報セキュリティ研究開発状況	3	・意見内容：追記 「システムのセキュリティ設定を上位から下位まで自動保証する技術」及び「障害に対して自動回復可能なネットワーク構築技術」といったテーマについては、――――十分な進捗が見られていない状況である。（次の文章の追記） 「システムのセキュリティ設定を上位から下位まで自動保証する技術」及び「障害に対して自動回復可能なネットワーク構築技術」の研究テーマは、蓋然性の高いサイバー脅威であるAPT攻撃及びEMP/HPM攻撃（EMP:電磁パルス攻撃,高出力マイクロ波（HPM）兵器）に対する実効性のある対策として不可欠なテーマであるため、研究テーマの具体内容及び研究体制の見直しを行い、継続すべきである。	修正意見	有	（27ページ） ご意見を踏まえて、EMPに対する防御技術について本文に追記させて頂きました。
2	個人	3（1） 研究開発の進め方に関する課題	8	図4が分かりにくく読者が混乱する. 実践−想像の軸とニーズ−シーズの軸で分類されているが「攻撃者」が何故ここに位置づけられるのかが不明である。 その直後の「すなわち」のつながりもおかしい。	修正意見	有	・攻撃者が、（負の方向での）創造性により、新たな攻撃を生み出し、新しい対策の必要性（ニーズとも関連）を発生させていることから、このような図とさせて頂いております。 ・「すなわち、」を削除させて頂きます。
3	個人	3（1）1） サイバー攻撃の検知・防御能力の向上における課題	8−9	・意見内容 IT利用者、ITサービス提供者及び研究者はサイバー脅威に関する共通認識として、APT攻撃は完全には防御できないという認識を持つべきであり、短期的にはサイバー攻撃の検知・防御能力の向上よりも実効性の高い情報資産の脆弱性の状況認識及び任務・業務レベルのリスク可視化に研究目標を重点化すべきである。 ・理由 現状技術では、APT攻撃は完全には防御できないので、革新的に防御能力を向上するためには、情報資産の環境パラメータを動的変更する移動目標(Moving Target)技術のようなサイバー防御能力を長期目標として研究開発する必要がある。	政策展開に係る意見	無	APT攻撃の検知・防御も、重要な事項の1つとして認識しております。 「情報資産の脆弱性の状況認識及び任務・業務レベルのリスク可視化」については、運用レベルの対策や、33ページの「情報セキュリティ理論の体系化／調査研究」の「ITリスクに関する理論から実務までの体系化」の1つの要素に含まれるという考えです。
4	個人	3（1） 研究開発の進め方に関する課題	9−10	項目 4) 5) についてはタイトルが課題になっていない.「の必要性」など の文言をつけ加える必要がある.	修正意見	有	4) 5) タイトルに「～の課題」と追記させて頂きます。

番号	提出者	該当箇所	ページ数	ご意見	意見の種類	修正の有無	御意見に対する考え方及び修正（案）
5	団体	3（2） 研究開発の効果・成果を高めるにあたっての課題	11	意見内容：民間による応用や実用化を意図した研究においては、そのテーマの検討、ニーズの分析などを含め、さらなる民間の関与が必要であると考えます。 理　由：広く社会的な応用や実用化を前提としたテーマについては、広く民間からテーマを募り、その研究主体を民間が担い、そこで明らかになる技術的な障害や課題について、独立行政法人や大学などが基礎的な研究テーマとして取り組み、実用化を支援するといった枠組みが有効だと考えます。 情報セキュリティ対策の現場では、差し迫った課題が多く、そうした課題を解決する方法が強く求められています。実用化という視点で考えるならば、現実の課題を広く募り、知恵を結集して解決していくという流れも重要なのではないかと考えます。	政策展開に係る意見	有	ご意見を踏まえて、本文に追記させて頂きました。 （20ページ） ---- また、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。例えば広く社会的な応用や実用化を前提としたテーマについては、広く民間からテーマを募り、研究主体を民間が担い、そこで明らかになる技術的な障害や課題について、独立行政法人や大学などが基礎的な研究テーマとして取り組み、実用化を支援するといった枠組みなどが考えられる。 ----
6	個人	4（1） サイバー攻撃の検知・防御能力の向上	12	・意見内容：修文 「情報セキュリティの研究開発分野には、コンピュータ・ネットワーク防御（CND：Computer Network Defense）や情報保証（IA：Information Assurance）、情報セキュリティマネジメント、暗号等の基礎分野など様々な専門領域がある」に対して、「情報セキュリティリスクマネジメント」も専門領域の1つとして追加すべきである。	修正意見	無	今後の施策の検討とさせていただきます。なお、本文脈においては、情報セキュリティマネジメントの中に、情報セキュリティに係るリスクマネジメントも含めて考えております。
7	団体	4（1） サイバー攻撃の検知・防御能力の向上 4（2） 社会システム等を防護するためのセキュリティ技術の強化	12	NISTのSCAPフレームワークのように、広範囲からの攻撃に素早く対応するため、国際的に最大限自動化する技術の確立を目標にするべき。	修正意見	無	今後の施策の検討の参考とさせていただきます。
8	団体	4（1） サイバー攻撃の検知・防御能力の向上	12	コンピュータウイルスやマルウェアの解析を行う際のリバースエンジニアリングの必要性について述べられていますが、ITシステムやネットワーク機器の製造段階で仕掛けられた悪意のプログラムに関して解析を行う際の必要性についても記載いただきたい。	修正意見	有	ご意見の内容を踏まえて、本文に追記させて頂きます。 （12ページ） さらに、コンピュータウイルスやマルウェアの解析や、ITシステムやネットワーク機器の製造段階で仕掛けられた悪意のあるプログラムの解析には、リバースエンジニアリングによる解析が一つの有効な手段と考えられる
9	団体	4（1） サイバー攻撃の検知・防御能力の向上	12	フェアユースな情報セキュリティ目的のリバースエンジニアリング部分は、対応する文化庁WEBサイトも拝見しましたが永続的な相互運用性やソースコードのメンテナンスに関しては、著作権者と使用許諾者間で保守契約とエスクロー契約があれば通常は十分で著作権法上も問題無いと考えます。 参考：文化庁WEB　リバース・エンジニアリングに係る法的課題についての論点 仮に資料記載の手法で他者が発見した修正必要箇所等がある場合には、すぐに原著作権者に通知され原著作権者同意によって修正され修正版として市場に供給することが大原則。 原著作権者が対処不能といった場合のみ問題点の発見者が原著作権の継承者等に許諾を得て修正版等を市場に供給すべき。	政策展開に係る意見	無	今後の施策の検討の参考とさせていただきます。 なお、情報セキュリティ目的でのリバースエンジニアリングの適法性の明確化については、サイバーセキュリティ2014(案)に記載があります。

番号	提出者	該当箇所	ページ数	ご意見	意見の種類	修正の有無	御意見に対する考え方及び修正（案）
10	個人	4（1） 今後の情報セキュリティ研究開発取組方針	13	最後の項目（フェアユースを前提としたリバースエンジニアリングの適法性）がp.12で述べられている内容と重複している.	修正意見	無	取り組み方針を記載する部分と、実施すべき施策を記載する部分に、それぞれリバースエンジニアリングについての記載を行っております。
11	個人	4（1） サイバー攻撃の検知・防御能力の向上 ［推進すべき施策例］	13	「情報セキュリティの確保という公益性に鑑み、フェアユースを前提としたリバースエンジニアリングの適法性を明確化するための措置を国として速やかに講じる。」とあるが、この実現は困難ではないか。 ・脆弱性の発見等の広く情報セキュリティ目的のリバースエンジニアリングを認めると、ほぼ無制限にリバースエンジニアリングが可能になってしまう。 ・コンピュータウイルスやマルウェアのリバースエンジニアリングに限るとすると、現行法上、マルウェア等も「著作物」に当たると解さざるを得ないこと考える。民事責任は、権利濫用等を根拠にこれを否定できるとしても、刑事責任は、著作権侵害を否定するのが困難だと考える。 ・マルウェア等のリバースエンジニアリングを検察官が起訴するということは、実際上あり得ないと思う。法律を改正してまでマルウェア等のリバースエンジニアリングを適法化する実益がほとんどなく、何か他の改正のついででもない限り、法律の改正は難しいのではないか。 ハードウェアであってもソフトウェアであっても、その経済的な効用は、ほぼ同様だと考える。ハードウェアのリバースエンジニアリングが合法であるのに対し、ソフトウェアについては、これができないのは、不合理である。 　現在のグローバル化した世界において、ソフトウェアのリバースエンジニアリングが他国では可能で、我が国では不可としても、事業が海外に流出するのみであり、我が国にとって不利益なだけである。産業競争力を阻害しているなどの理由から、情報セキュリティに限らずソフトウェアのリバースエンジニアリング全体を合法化するべきだと考える。	政策展開に係る意見	無	頂きましたご意見については、著作権法の所管省庁と情報共有させて頂きます。 なお、情報セキュリティ目的でのリバースエンジニアリングの適法性の明確化については、サイバーセキュリティ2014(案)に以下の記載があり、文部科学省にて実施計画がございます。 ―――――――――― 安全性確保のためのソフトウェア等のリバースエンジニアリングの適法性の明確化（文部科学省） 文部科学省において、文化審議会著作権分科会の報告に基づき、情報セキュリティ目的のリバースエンジニアリングの適法性を明確化するための措置を速やかに講ずる。 ――――――――――
12	個人	4（1） サイバー攻撃の検知・防御能力の向上 ［推進すべき施策例］	13	情報セキュリティの研究に従事する者として，今後の情報セキュリティ研究開発取組方針に記載の，「研究開発の充実に役立つ情報やデータの共有」に関して強く賛同の意を表明致します。 情報セキュリティ技術に関してはこれまでの経験から具体的なデータの解析なくして有効な研究開発はできないと確信しております．是非，このような取り組みを実現して頂くことを切望致します。 また，推進すべき施策例の「政府が保有する攻撃情報やデータの研究者への提供ならびに研究者受け入れ」に関しても同様に強く賛同致します。	賛同意見	無	賛同のご意見ありがとうございます。 「研究開発の充実に役立つ情報やデータの共有」について、関係者と今後検討を進めてまいりたいと存じます。
13	個人	4（1） サイバー攻撃の検知・防御能力の向上 ［推進すべき施策例］	13	学術機関が研究開発を推進する上では成果を論文として発表する営みが必要不可欠である。 そのため、共有情報・データを使った研究および論文投稿が可能となるように，情報・データの公開時点から論文投稿に配慮したルール・ガイドラインを策定頂きたい。 （例：どのデータは論文として投稿できるか，どのような統計データであれば投稿できるかなど） これは必ずしもすべての情報やデータに関して論文投稿を希望するものではなく，研究が進んでしまった後に論文投稿に待ったがかかるような事態を避けることが目的です。	政策展開に係る意見	有	研究開発戦略本文に注釈を追記させて頂きます。 （13ページ） データの可能な範囲・方法・条件（*4）で政府が保有する検体等の攻撃情報やデータを研究者等へ提供～ （*4）データの利用条件について、論文投稿等に配慮したルール・ポリシー策定についての検討も含む

番号	提出者	該当箇所	ページ数	ご意見	意見の種類	修正の有無	御意見に対する考え方及び修正（案）
14	団体	4（1） サイバー攻撃の検知・防御能力の向上	13	（該当箇所） （1）サイバー攻撃の検知・防御能力の向上 ［推進すべき施策例］ （意見内容） 研究者への検体等の情報提供に加えて、対策手法の評価・検証の場としてP26の「（1）情報通信システム全体のセキュリティ向上」の「①サイバー攻撃の検知／防御技術」で構築の必要性が述べられている「解析を行うためのプラットフォーム」の利用も範囲に入れていただきたい。	修正意見	無	今後の施策の検討の参考とさせていただきます。
15	個人	4（1） サイバー攻撃の検知・防御能力の向上[推進すべき施策例]	13	・意見内容：追加 ・APT攻撃を完全に防御するために目標捕捉を困難化する移動目標技術の研究開発を推進する。 ・理由 推進すべき施策例のひとつとして、「サイバー攻撃発生時のネットワーク構成自動変更による防御方式に関する研究開発」が挙げられているが、本方式ではサイバー攻撃が検知できなかった場合の防御は不十分である。したがって、常時目標捕捉を困難化する移動目標技術の研究開発が必要である。	修正意見	無	ご指摘の事項については、「サイバー攻撃の検知／防御」に関する研究の一つの要素として考えております。必要に応じ研究開発を行うべきものと考えております。
16	個人	4（1） サイバー攻撃の検知・防御能力の向上[推進すべき施策例]	14	・意見内容：追加 ・制御システムのセキュリティ常時監視のプロトタイプ研究開発を推進する。 ・理由 制御システムセキュリティにおいても、APT攻撃のような動的なサイバー脅威に対応するためには、情報セキュリティマネジメントの考え方に基づく静的なCSMSによる評価・認証だけでは十分ではないため、情報セキュリティリスクマネジメントの考え方に基づくセキュリティ常時監視が必要である。	修正意見	無	ご指摘の事項については、「制御システムセキュリティ」に関する研究の一つの要素として考えております。必要に応じ研究開発を行うべきものと考えております。
17	団体	4（2） 社会システム等を防護するためのセキュリティ技術の強化	14	（該当箇所） （2）社会システム等を防護するためのセキュリティ技術の強化 （意見内容） 社会インフラを構成するシステムの例として制御システムと自動車が挙げられているが、街中に設置されている監視カメラや計測機器などのセンシングを行う機器についてのセキュリティも考慮いただきたい。	修正意見	無	今後の施策の検討の参考とさせていただきます。
18	団体	4（2） 社会システム等を防護するためのセキュリティ技術の強化	14	意見内容：セキュリティデバイス、半導体チップ等の開発における事前リスク評価を十分に実施できるような研究開発プロセスを導入していただきたい 理　由：セキュリティ機能のハードウエア化、チップ化は、その堅牢性強化につながる反面、万一、設計上の不具合、とりわけセキュリティ上の脆弱性などを作り込んでしまった場合に、事後の対応が困難になるという特性があります。 このため、事前のリスク評価をより慎重に行う必要があり、「想定外」を可能な限り減らすため、事前リスク評価を実施できる研究開発プロセスの導入を検討いただきたい。	政策展開に係る意見	無	ご指摘の内容につきましては「大学や公的研究機関等の研究としても、必要な研究開発が期待される。」に含まれているに内容と考えることができるため、追記はしないこととさせて頂きます。
19	団体	4（2） 社会システム等を防護するためのセキュリティ技術の強化 4（3） 産業活性化につながる新サービス等におけるセキュリティ研究開発	14	意見内容：これらの研究開発に、広い分野のIT,セキュリティに関する知見を集約できるような枠組み作りをお願いしたい 理　由：特定の業種、産業分野に係る研究開発では、研究に関わる人材が、その業種、分野に閉じる傾向が見られます。一方、現実のシステムにおいては、その分野以外の様々な技術を取り入れたり関係したりしていることが多いため、とりわけ脅威やリスクの洗い出し等のセキュリティの検討において、当該分野の知見のみでは網羅できない部分が多くなっていると考えます。単なるアドバイザーではなく、研究当事者として、こうした人材の参画が必要と考えます。	政策展開に係る意見	有	ご意見の内容を踏まえて、本文に追記させて頂きます。 （16ページ） ・特定の分野に係る研究開発では、研究開発に係る人材が分野内に閉じる傾向があり、これらの研究開発(特に脅威やリスクの洗い出し等の検討)に、広い分野のIT、セキュリティに関する知見をもった人材が研究当事者として参画することを推進する。

番号	提出者	該当箇所	ページ数	ご意見	意見の種類	修正の有無	御意見に対する考え方及び修正（案）
20	団体	4（3） 今後の情報セキュリティ研究開発取組方針	14	「4　今後の情報セキュリティ研究開発取組方針」に以下の事項を追加頂きたい。 ―――――――――――――――――――――――――――――――― （3）生活機器等を防護するためのセキュリティ技術の強化 家電、自動車、在宅医療機器、HEMS等の生活機器については、様々なメーカから提供される生活機器をユーザが自由に繋げて利用することが可能となりつつある。この場合、「何が繋がっているか分からない」、「メーカが想定しない形で機器が利用される」、「ユーザにセキュリティ知識がない」、「世代が異なる機器が混在し、通信相手のセキュリティレベルがわからず情報を信頼してよいかわからない」といった状況から、セキュリティ対応が困難である。このため、ユーザを巻き込みながら業界及び業界横断的にセキュリティ技術の検討を実施するとともに、国際標準化や評価認証基盤を実施する体制の整備が求められる。 ［推進すべき施策例］ ・生活機器単体及び連携時のセキュリティ向上のための体制を整備し、研究開発、国際標準化活動、評価認証基盤整備等を実施する。 ・業界及び業界横断的な生活機器のセキュリティに関する検討の場を設置し、共通的・基盤的な技術の検討を行う。 ・相手機器の信頼レベルに応じて段階的に連携内容を変化させる信頼モデルの技術開発、刻々と変化する連携構造を記録し迅速なインシデント対応や事後分析に役立てるトレーサビリティ技術の研究開発を実施する。 ・生活機器のユーザインタフェースを活用して機器のセキュリティレベルや現在のステータスをユーザに伝えたり適切な利用を促す技術の研究開発を実施する。 ――――――――――――――――――――――――――――――――	修正意見	有	ご意見を踏まえ、「4　今後の情報セキュリティ研究開発取組方針」に、生活機器等に関する対応を追記させて頂きます。 （15ページ） また、様々なメーカから提供される、自動車、HEMSや家電等の生活機器についても、ネットワーク接続が進みつつあるが、生活機器は、連携対象が多種多様であることや、操作する者が一般消費者である特性があることから、この分野において、分野横断的な情報セキュリティ技術の研究開発やその国際標準化等の対応についても検討していく。 なお、在宅医療機器については、「医療健康分野での情報流通変革に伴い必要となるセキュリティ技術の開発・検証」の範囲という考え方とさせて頂きます。
21	団体	4（3） 産業活性化につながる新サービス等におけるセキュリティ研究開発	14	日本ブランドのセキュリティを実現するため、大企業が上流工程で組み込んだセキュリティ品質を、中小企業が適切に引き継いで詳細設計・開発を行えるよう、中小企業技術者のセキュリティ技術育成や上流工程を含めたトレーサビリティの確保などの工程改善を支援すべき。	修正意見	無	今後の施策の検討の参考とさせていただきます。
22	団体	4（4） 情報セキュリティのコア技術の保持	15	意見内容：M2M（IoT）については、デバイス認証のみでなく、デバイス自身の攻撃耐性や、デバイスを統括するサービス側のセキュリティに関する研究も重要度が高いと考えます。 理　由：いかに強固な「認証」を行っていても、「正規」デバイスが乗っ取られる可能性もあり、こうした「デバイスなりすまし」防止は「認証」強化だけでは難しいこと。また、個々のデバイスへの侵害よりも、そうしたデバイスを統括、管理するサーバが侵害された場合の方が、はるかに被害が大きくなる可能性があることなど。「デバイス」「組み込みシステム」技術に偏らない幅広い研究が必要であると考えます。	政策展開に係る意見	無	デバイス自身への攻撃耐性については、以下の内容等に含まれるという考え方です。 （P14［推進すべき施策例］） ――― ・また、セキュリティに係る半導体チップの模造や改竄、情報通信ネットワークにおける機密情報の漏洩や個人データの窃取等のセキュリティ事案の解決に向け、セキュリティチップ等の最先端暗号技術の導入と真正性を保証する半導体デバイス製造・流通の確立のための研究開発を実施する。 ――― また、サービス側のセキュリティについては、「ITサービスのセキュリティ（スマートフォン／クラウド等）」という整理とさせて頂いております。

番号	提出者	該当箇所	ページ数	ご意見	意見の種類	修正の有無	御意見に対する考え方及び修正（案）
23	個人	4（4）情報セキュリティコア技術の保持	16	日本がコア技術を有することで国際的な立場を確保する点には同意する．しかしページ10で述べられているように「システムのOSなど重要な製品が海外製品」というのが実情である．NSAによる暗号技術や関連製品へのバックドアを排除するためにも国内産製品の普及への取り組みも検討して頂きたい．政府によるお墨付き制度をCRYPTRECのような暗号アルゴリズムやJCMVPのような暗号モジュール認定の枠組みをIT製品全体に拡大する方向性がよいかどうかは別として，ページ4の表にあるように2011年には重要分野として認識されていた項目11「セキュリティ部品が正しく実装されていることを保証する製品評価認証技術」が今回除外されている点について説明が欲しい．	政策展開に係る意見	無	今後の施策の検討の参考とさせていただきます。 ・バックドアの排除については、34ページ ⑪標準化／評価／制度／基盤整備に「（バックドアなどの）不正な製品に対するチェックしたり排除したりする仕組みや制度の検討」を記載しております。 ・国内産製品の国際競争力を高める施策について、今後とも取り組んでまいりたいと存じます。 ・項目11「セキュリティ部品が正しく実装されていることを保証する製品評価認証技術」については、 －ISO/IEC 15408 ITセキュリティ評価及び認証制度が既に確立されていること。 －2013年に、IPAでソフトウェア品質説明のための制度ガイドラインなどが公開されたこと。 なども踏まえ、表現や整理方法を変更させて頂きました。 現状に不足があれば、「⑪標準化／評価／制度／基盤整備」や「⑤制御システムセキュリティ」の１要素として扱う考え方とさせて頂きました。
24	団体	5（1） 研究開発の効果・成果を高めるための方策等	19	セキュリティ対策やプライバシ対策の効果を数値化（見える化）する研究を行い、技術提供側とユーザ側で価値の共有を図ることで、対策導入を促進すべき。	修正意見	有	ご意見を踏まえ、本文に追加させて頂きます。 （34ページ） 34ページの調査研究の一つに、以下を追記させて頂きます。 ・セキュリティ対策やプライバシー対策の効果の見える化の研究 （技術提供側とユーザ側で価値の共有を図ることで、対策導入の推進を図る）
25	団体	5（1） 研究成果の社会還元の促進	19	当該分野ベンチャー企業等の支援の記載がありますが、「はじめに」部分でも明確に支援等の記載をすべき。 研究機関や前述の経営基盤の弱い組織での当該分野の研究開発活動に関する挑戦や再挑戦の具体的支援策を明示すべき。 特に民間組織で研究開発を主とした場合の決算資料は、研究成果売上げで組織が損益分岐点を越えるまでは無残な決算書になり資金と人材が枯渇します。 これは我が国で情報セキュリティ基礎技術を研究開発し株式上場するような新規上場企業が皆無に等しいことやM＆Aか廃業になる直接的原因の一つ。 そこで通常の民間企業とは異なり、広く社会全体に資する当該分野研究開発を行なう中小零細組織やベンチャー企業には専用の会計基準や組織評価手法を準備し積極的に公的補助や公的出資等を早急に実施すべき。 先進諸外国が行なうように政府予算で中小零細組織からの調達枠を設定し同時に専用の入札資格を準備し、当該研究成果の市場普及と共に新産業と雇用創出に資する施策も必要。 更に中小零細組織の研究開発成果のうち公的実証実験や公的組織との共同研究成果のシステムや技術、関連する知的財産を積極的に公的組織が調達し我が国の情報セキュリティ産業の底辺からの活性化と日本発世界標準化を具現化すべき。	修正意見	無	今後の施策の検討の参考とさせていただきます。 なお、ベンチャー支援については、政府としても様々な施策に取り組んでいるところです。

番号	提出者	該当箇所	ページ数	ご意見	意見の種類	修正の有無	御意見に対する考え方及び修正（案）
26	個人	5（3） 情報セキュリティ技術と他分野の融合	21	情報セキュリティ技術と他分野の融合に関して、「技術的な研究をするのみならず、国際政治、法律、安全保障、危機管理、経済学、心理学等の社会科学的視点も含め様々な領域の研究とも連携して行われることが求められる。」とあるが、社会科学的視点のとして、「公共政策学」を追記すべきである。 公共政策学は、経済原理に基づいて社会最適の為に必要な政策を立案し、実施する方法を研究する学問であり、サイバーセキュリティの問題を横断的に考えるにあたっては連携が必要な分野です。 なぜなら、サイバーセキュリティの脅威が生じる原因の大部分はソフトウェアの脆弱性や弱いユーザのパスワードであり、それらの取扱いに対するソフトウェア製造者やサービス提供者、消費者への経済的モチベーションを制御するのは公共政策の重要な役割だからです。	修正意見	有	（11ページ、22ページ、34ページ） 公共政策学についても連携が必要な分野の一つとの認識です。ご意見を踏まえ、「公共政策学」も明示的に追加させて頂きます。
27	団体	5（3） 情報セキュリティと他分野の融合	21	技術と他分野の融合の箇所で、情報セキュリティに関し広い分野の叡智を集約させることとその活動を支援することと、その活動を行う際の人選に関し学習履歴等にとらわれないようにすることを明記しているところは、専門家集団による思い込みの弊害や既得権益から脱却した有効な現実解を見出す為に非常に有意義と考えます。	賛同意見	無	賛同のご意見ありがとうございます。
28	団体	6（2） 情報セキュリティ研究開発の重要分野	28	（該当箇所） (1)情報通信システム全体のセキュリティ向上　③ITサービスのセキュリティ（スマートフォン／クラウド等） （意見内容） クラウドサービスの具体的なセキュリティ上の課題やリスクが、スマートフォンの記載部分のように述べられておらず、これについても具体的に取り上げていただきたい。例えば、情報を暗号化せずに預けておくことが漏えいにつながる可能性があり安心した利用ができないということが挙げられます。	修正意見	有	ご意見の内容を踏まえて、本文に追記させて頂きます。 （29ページ） さらに、クラウドサービス利用についても、不正アクセス等による情報漏えい等、外部にデータがあることによるセキュリティ上の課題やリスクが残存しており、暗号化等適切な情報セキュリティ対策を講じることが重要である。
29	個人	6（3）⑧ 6（5）⑮ 情報セキュリティ研究開発の重要分野	31 35	項目8 と 項目15 の内容に関して. パーソナルデータやビッグデータにおいて秘密計算は匿名化技術が必要とされているが，現状基礎的研究の段階と認識されている．一方で先駆的に実装された製品も登場しているが，その方式に対しては暗号技術と異なり仕様自体が不透明なものもあり政府システムや民間のシステムにおける導入にあたりCRYPTRECのように方式そのものに対して評価機関がない状況である．項目12 の暗号技術で取り上げられているように監視・評価を行う取り組みについても検討して頂きたい．	修正意見	有	ご意見を踏まえ、本文を変更させて頂きました。 （33ページ） プライバシーを保護したまま有用なデータを計算するための秘密計算や匿名化技術（再識別化を防止する技術等を含む）、プライバシー保護に配慮したデータマイニング等の基礎的研究が考えられ、客観的な検証を経た上で、これらの技術が活用されることが重要である。
30	個人	6（4）⑪ 情報セキュリティ研究開発の重要分野	33	項目11 において「不正な製品」と書かれているものが不明瞭である．例えばPRNGモジュールが十分なエントロピーを有さないために鍵データなどが本来よりも容易に暴露されてしまうような脆弱性を有する製品を指すのか。	修正意見	無	ここでの「不正な製品」とは、バックドアが仕込まれた製品や、模造品などのことを想定しております。
31	団体	6（2） 情報セキュリティ研究開発の重要分野	34	（該当箇所） (4)研究開発の促進基盤の確立と情報セキュリティ理論の体系化　⑫暗号技術 （意見内容） IoTの拡大に対応するための暗号技術が重要であるという認識には同意しますが、暗号技術が広く様々なものに用いられることから、大量の鍵の管理についても研究範囲に含めるべきではないでしょうか。	修正意見	有	ご意見の内容を踏まえて、本文に追記させて頂きます。 （35ページ） なお、必要に応じて、大量の鍵の管理に関する研究が求められる。

番号	提出者	該当箇所	ページ数	ご意見	意見の種類	修正の有無	御意見に対する考え方及び修正（案）
32	団体	6（5） 情報セキュリティ研究開発の重要分野	35	P35（5）発展が期待される応用分野でのセキュリティ確保について 応用分野においては、機動力やチャレンジ精神のある中小企業を巻き込んだセキュリティ技術開発プロジェクトを支援することで、分野産業全体のセキュリティレベルの底上げを図るべき。	修正意見	無	今後の施策の検討の参考とさせていただきます。 なお、20ページ 5（1）研究成果の社会還元の促進の中で、ベンチャー企業との共同研究などが求められることを記載しております。
33	団体	6（5）⑯ 情報セキュリティ研究開発の重要分野	36	「6　情報セキュリティの研究開発における重要分」の「（5）⑯家電、自動車のセキュリティ技術の開発」を以下の内容として頂きたい。 ―――――――――――――――――――――――――――――― ⑯ 生活機器のセキュリティ技術の研究開発 様々なメーカから提供される家電、自動車、在宅医療機器、HEMS等の生活機器を、ユーザが自由に繋げて利用することが可能となりつつあり、このような状態においてセキュリティを確保する技術開発が求められる。このため、生活機器単体及び連携時のセキュリティの研究開発、国際標準化活動、評価認証基盤整備等を行う体制の整備、業界・業界間連携による技術開発検討の場の設置、柔軟な連携構造に対応するセキュリティ技術開発や機器のユーザインタフェースを利用してユーザのリテラシーを高めたり適切な利用を促すような社会科学的アプローチによる研究開発が求められる。 民間企業等において、様々な技術開発が行われることが想定されるが、我が国の産業競争力確保などの観点から官民連携した標準化や制度づくり、所要の技術開発を行うことが期待される。（原文ママ） ――――――――――――――――――――――――――――――	修正意見	有	（37ページ） ⑯「家電、自動車のセキュリティ技術の開発」 を ⑯「家電、自動車等のセキュリティ技術の開発」 に変更させて頂きました。 また、ご意見を踏まえ、「4　今後の情報セキュリティ研究開発取組方針」に、「業界・業界間連携による技術開発検討の場の設置」に関する検討を追加させて頂きました。 なお、社会科学的アプローチによる研究開発についてのご指摘については、「情報セキュリティ技術と他分野の融合」（22p）の部分で既に記載しております。