「情報セキュリティ研究開発戦略（改定版）（案）」に対する意見募集の結果の概要

資料4－1

■ 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26日（月）～6月6日（金）

■ 意見総数： 33件 【内訳：5団体から延べ18件、5個人から延べ15件】

（1）賛同意見 全2件

（2）修正意見 全22件

- プログラムの全体構成、基本的考え方等に修正を求める意見はなし。
- 考え方の追加、表現の適正化等を求めるものについては、必要に応じて趣旨を踏まえて修正（全11件）。
- 他の箇所で言及している等修正不要の意見については、考え方を説明（全11件）。

（3）政策展開に係る意見 全9件

- 今後の政策展開に係る意見については、考え方の説明や今後の施策の検討において参考にする旨回答。（全6件）
- 意見を踏まえ、文章に反映が好ましいと考えたものについて反映を行った。（全3件）

注）提出された意見等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

● 情報セキュリティの研究にあたり、研究開発に役立つ情報やデータの共有に強く賛同する。【P13】

● 技術と他分野の融合の箇所で、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、その際の人選に関し学習履歴等にとらわれないことは、専門家による思い込み等から脱却した有効な現実解を見出す為に非常に有意義。【P21】

（2）修正意見

● 「4　今後の情報セキュリティ研究開発取組方針」に,生活機器等を防護するためのセキュリティ技術を追加頂きたい。

（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。

【P15　下記のように追加】

（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

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。

（2）修正意見

● 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。

【P19　下記のように追記】

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現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。

● 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。【P21 他　下記のように修正】

「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、公共政策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。」

（3）主な政策展開に係る意見

●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。【P8】

●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は、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著作権法上も問題無いと考える。【P12】

●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ではないか。【P13】

●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。【P13】

●セキュリティデバイス、半導体チップ等の研究開発における事前リスク評価を十分に実施できるプロセスを導入すべき。【P14】

●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。【P14】

●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。【P15】

●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。【P16】