「サイバーセキュリティ研究開発戦略（案）」に対する意見募集の結果の概要

- 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： 2017年６月９日（金）～ ６月19日（月）
- 意 見 総 数： 46者から69件

意見内容の内訳：

１．本戦略の趣旨・位置づけ等に関わるご意見	6件
２．本戦略の状況の認識に関わるご意見	8件
３．今後の具体的な取組に関わるご意見	12件
４．その他のご意見	43件

ご意見を踏まえた修正： 全６件

注）提出されたご意見等は必ずしもこれらに分類されるわけではないが、事務局で理解した区分にて計上している。

意見募集に対して寄せられたご意見の概要及びご意見に対する考え方

※意見の全体像がわかるように、代表的な御意見を例として抽出し、その趣旨を踏まえて編集・整理を行っております。

いただいた御意見の例	御意見に対する考え方
○本戦略の趣旨・位置づけ等に関わるご意見 ・工学的な研究開発だけではなく、社会科学的なアプローチ、AIと倫理などの人文科学的なアプローチについても着目していることは評価できる。 ・全体として理念が記載されているが、抽象的な内容が多いように感じられる。「戦略」である以上、概念だけでなく、中長期的に政府、民間、国民が何をやっていくのか、具体的なアクションプランが必要でないか。 ・本戦略には具体的な評価基準がないように思われるが、どのように評価していくのか。 ・本戦略は、開発技術の幅を広げることに重点が置かれているようだが、その結果、サイバーセキュリティ技術の全体像が曖昧になっていると思われる。	本研究開発戦略は、情報通信技術（IT）の進化の方向性を予測することは難しいため、本戦略では、個々のサイバーセキュリティ技術に関する技術的課題を深掘りすることはしないものとし、情報通信技術（IT）の進化や、人間と情報の関わり方が変化していることを意識しつつ、将来的なサイバーセキュリティ研究開発の方向性についてビジョンを示すものとしています。 また、本戦略が想定する対象者については、我が国のサイバーセキュリティ技術の研究開発に関わる政府機関や公的研究機関だけではなく、サイバー空間は経済社会の活動基盤であることから、直接的であれ、間接的であれ、情報通信技術（IT）に関わる研究開発を行っている大学や企業等を含め、経営者から研究開発の戦略企画を行う担当者、研究者まで、幅広い層を想定しています。 本戦略はこうした方々にお読みいただき、自組織の戦略を議論する際に活用いただくことを期待しています。また、今後、具体的なサイバーセキュリティの研究分野やテーマについて検討を行うなど本戦略を具体化させるための取組を進めてまいります。このため、「４．まとめ」において、本戦略を具体化させるための取組を行い、適時、本戦略の見直しを検討する旨、記載しました。
○本戦略の状況の認識に関わるご意見 ・昨今の世界情勢から鑑みて、国防の側面を加えることは必須と考える。 ・インターネット・イントラネット及び各種端末を根本的に動かすエネルギー関連に対してのセキュリティがおろそかになってはいないか。 ・サイバーセキュリティ対策の関係者を取り巻く課題でつかわれたフレームワークにおいて、創造とシーズの総合関係のなかに悪意や無智があるとどうなるのか。 ・二義的目的は削除し、「攻撃者の非対称優位のサイバー空間から、安全・安心な国際公共財としてのサイバー空間に変革すること」の旨、記載すべきである。 ・全体を通してサイバー攻撃への言及が多く、意図しない障害や不適切な設計などへの対応もサイバーセキュリティの範疇にあるという意識が希薄である。 ・国家的なサイバー攻撃においては、攻撃側は、犯罪者ではなく攻撃国の公的研究機関や企業の研究者が攻撃者となることもありうる。 ・攻撃手法の研究が悪用されないよう、研究者と研究成果の情報管理の徹底、研究実施に際しての倫理審査体制の整備、デュアルユース研究についての安全保障上の配慮なども重要であるが、3章においてその旨の記載がない。	今後、総合科学技術・イノベーション会議やIT総合戦略本部等における取り組みとの連携を図りつつ、内閣サイバーセキュリティセンター（NISC）を中心に、我が国のサイバーセキュリティに関連する研究開発の状況について把握に努め、本戦略の内容について、フォローアップを行うこととしています。併せて、NISC及び関係府省庁の連携の下、具体的なサイバーセキュリティの研究分野やテーマについて検討を行うなど本戦略を具体化させるための取組を行い、適時、本戦略の見直しを検討することとしています。いただいた御意見の内容については、サイバー攻撃への対処に係る政策などを含め、今後の取組の参考とさせていただきます。
○今後の具体的な取組に関わるご意見 ・APT攻撃のようなサイバー攻撃は、多層防御では完全に防御できないため、当面の実効性のある対策としてはリアルタイムのリスク管理を実現していく旨を記載すべきである。 ・サイバー攻撃に対する従来の防御・検知だけでは、十分に対応できないため、サイバー攻撃に対する新たなフレームワークを策定する必要がある。 ・サイバーセキュリティ研究の広がりとして、様々な学術分野が列記されているが、サイバーセキュリティへの関連を踏まえた濃淡を示すべきである。 ・現在、大規模なサイバー犯罪/インシデントが発生した場合に、首謀者が摘発/逮捕された事例は、非常に少ない。犯罪摘発のためのトレーサビリティを担保する仕掛けを構築していく必要があると考える。 ・単なる情報共有を超え、技術開発を促進するデータセットの整備/蓄積やテストベッドの構築/公開が必要と考える。 ・オープンソースソフトウェア(OSS)をどう安全に使うか、安全を担保していくのかについての研究が必要と考える。 ・米国では脅威情報の自動的共有が既に始まっており、日本でもこうした取り組みが今後導入されるものと思われることから、脅威情報の自動的共有、その知見に基づく攻撃の自動的防止など自動化技術に関する研究が必要と考える。 ・セキュリティ・バイ・デザインに加え、コスト減と効率化を進めていくには自動化も必須と考える。 ・今後の研究開発においては、サイバーセキュリティ強化に対するハードル（技術的な難易度やコスト等）を下げ、日本に広く適用できる方策を生み出せる案を考えていただきたい。 ・サイバー脅威および脆弱性によるリスク認識に基づき、サイバーセキュリティ研究開発の戦略目標を産官学の研究開発のテーマ選定基準となるように、具体目標を設定すべきである。 ・なぜインターネット空間でサイバー攻撃が行われるのかを、「小学生でも理解できるよう」周知徹底するべきである。	
○その他のご意見 ・技術的修正に関する意見（内容のわかりやすさ、西暦・和暦表記の統合等） ・脅威やセキュリティの問題を直接可視化しても経営者は理解が困難であるため、経営者の理解できる任務／機能（業務）レベルのリスクに変換して可視化する必要がある旨、記載すべきである。 ・防御の必要性が失われるものではないことについて、経営層をはじめとするビジネスパーソンからの誤解を防ぐ記述が必要である。 ・そもそものサイバーセキュリティについての国民理解が不十分であり、国民の意識啓発等に努めることが重要と考える。	技術的修正に関する御意見の一部については、それを踏まえて本文の修正をさせていただいております。また、その他の意見につきましては、今後の取組の参考とさせていただきます。