

提出者名	在日米国商工議会所 (The American Chamber of Commerce in Japan)
------	-------------------------------------------------------

意見の内容		
項目 (※セルの右下の▼ボタンから、必ずプルダウンの項目を選択してください。)	意見の対象 (※セルの右下の▼ボタンから、必ずプルダウンの項目を選択してください。)	意見
1～3 (1. 策定の趣旨・背景、2. サイバー空間に係る認識、3. 本戦略の目的)	戦略本文に係る意見	<p>3.1. 基本的な立場の堅持 (3)基本原則 ⑤多様な主体の連携</p> <p>サイバー空間は容易に国境を超え多大な効果をもたらします。しかしその一方で、サイバーセキュリティ対策は予測がつかない対策を強いられます。したがって、以下の下線部分の文を盛り込むことにより、サイバー空間の拡がりを表すべきであると考えます。</p> <p>⑤多様な主体の連携 サイバー空間は、国、地方公共団体、重要インフラ事業者、サイバー関連事業者その他の事業者、教育研究機関、個人などの多様な主体が活動することにより構築される多角的な世界である。更にはサイバー空間上では<u>国外の利害関係者とも容易につながり、サイバー空間の拡がりを特定することは極めて難しい</u>。こうしたサイバー空間が持続的に発展していくためには、これら全ての主体が自覚的にそれぞれの役割や責務を果たすことが必要である。そのためには、個々の努力にとどまらず、連携・協働することが求められる。国は、連携・協働を促す役割を担っており、その役割を果たすことができるように施策を推進していく。</p>
4. 1. 1 新たな価値創出を支えるサイバーセキュリティの推進	政策展開 (サイバーセキュリティ2018) に係る意見	<p>(3)先端技術を活用したイノベーションを支えるサイバーセキュリティビジネスの強化</p> <p>サイバーセキュリティビジネスの強化を歓迎します。とくに、サイバーセキュリティ対策をモノやサービス等を創出する過程において可能な限りあらかじめ組み込んでおくこと (セキュリティ・バイ・デザイン) によって、サイバーセキュリティに関する品質の高いモノやサービス等が期待され、日本のモノやサービスの信頼性向上や海外展開の推進に寄与することとなると考えます。</p> <p>一方で、それらのセキュリティ・バイ・デザインにより、国際競争の高まりや真正性や信頼性の検証が困難になるという理由のもとに、国外製品が排除されたり、または不当に扱われたりすることのないようご配慮を要望します。</p>
4. 1. 2 多様なつながりから価値を生み出すサプライチェーンの実現	政策展開 (サイバーセキュリティ2018) に係る意見	<p>ブロックチェーンはサプライチェーンマネジメントにおいて重要な新技術の一つです。「サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築」とありますが、ブロックチェーン技術をめぐるセキュリティについても考慮に入れた戦略を検討することが経済社会の活力向上に一層資するものと考えます。</p>
4. 1. 3 安全なIoTシステムの構築	政策展開 (サイバーセキュリティ2018) に係る意見	<p>廃棄も含めたIoT機器のサイバーセキュリティ対策について、製造者、通信事業者、エンドユーザー等の相互理解と連携のもとで取り組むことに賛同します。その中で、それぞれのIoT機器について、サイバーセキュリティの要件を整理する際、先述されているように、サイバーセキュリティに関する基本的な要素等の国際標準化との整合性を求めます。</p> <p>日本政府は、独自の基準や規制を設定すべきではなく、世界標準と共通の地盤を維持するために重要な国際基準を採用することを強く推奨します。</p> <p>とくに、サイバー空間における情報システムのインフラストラクチャでは、さまざまな種類とレベルのサイバーセキュリティを解決する「多層防御」に基づいて、IoTデバイスからバックエンドシステムに至るまで、データ分類に基づくエンドツーエンドのデータ転送を想定する必要があります。</p>