資料 1-1(参考)

「サイバーセキュリティ戦略（案)」に対する意見募集後の本文修正　新旧対照表

変更後	変更前
（略） １．環境の変化 （１）サイバー空間の拡大・浸透 ①（略） ②サイバー空間を取り巻く「リスクの深刻化」 （略） サイバー攻撃はその手法の入手が容易であり、国家のみならず多様な主体が隠蔽や偽装等を行うことに加え、世界中から実行することが可能である。サイバー攻撃は、その主体が存在する国等から我が国に直接行われることもあれば、他国に係るサイバー空間を経由して行われたり、更には我が国に係るサイバー空間を踏み台にして行われたりすることもあり得る状況となっている。また、サイバー攻撃と武力攻撃等の関係については国際的に定説がない状況であるが、武力攻撃等に該当するサイバー攻撃がこのような形で行われる可能性も否定できない状況となっている。 ２．基本的な方針 （１）略 （２）基本的な考え方 ①（略）	（略） １．環境の変化 （１）サイバー空間の拡大・浸透 ①（略） ②サイバー空間を取り巻く「リスクの深刻化」 （略） サイバー攻撃はその手法の入手が容易であり、国家のみならず多様な主体が隠蔽や偽装等を行うことに加え、世界中から実行することが可能である。サイバー攻撃は、我が国に直接行われることもあれば、他国に係るサイバー空間を経由して行われたり、我が国に係るサイバー空間を踏み台にして行われたりすることもあり得る状況となっている。また、サイバー攻撃と武力攻撃等の関係については国際的に定説がない状況であるが、武力攻撃等に該当するサイバー攻撃がこのような形で行われる可能性も否定できない状況となっている。 ２．基本的な方針 （１）略 （２）基本的な考え方 ①（略）

②（略） ③リスクベースによる対応の強化 （略） 脆弱性への対処やサイバー攻撃に関するインシデントの認知・解析機能の向上、これらの機能の連携、情報共有の促進による脅威分析能力の高度化、各主体のＣＳＩＲＴ間の連携や国際的なＣＳＩＲＴ間連携の強化等が重要であり、これらによる動的対応力を通じ、リスクの性質を踏まえたリスクベースによる対応を強化することが必要である。 ④社会的責務を踏まえた行動と共助 （略） その上で、リスクが拡散している状況にあっては、サイバー空間を介し広く被害が波及することから、個々の主体による対策に加え、不正な侵入やマルウェア感染、これらの原因ともなる脆弱性等に対して、社会全体が参加することで予防的に情報セキュリティ対策に取り組む「サイバー空間の衛生」が重要になっている。	②（略） ③リスクベースによる対応の強化 （略） サイバー攻撃に関するインシデントの認知・解析機能の向上、これらの機能の連携、情報共有の促進による脅威分析能力の高度化、各主体のＣＳＩＲＴ間の連携や国際的なＣＳＩＲＴ間連携の強化等が重要であり、これらによる動的対応力を通じ、リスクの性質を踏まえたリスクベースによる対応を強化することが必要である。 ④社会的責務を踏まえた行動と共助 （略） その上で、リスクが拡散している状況にあっては、サイバー空間を介し広く被害が波及することから、個々の主体による対策に加え、不正な侵入やマルウェア感染等に対して、社会全体が参加することで予防的に情報セキュリティ対策に取り組む「サイバー空間の衛生」が重要になっている。
（３）各主体の役割 （略） ①（略） ②（略） ③企業や教育・研究機関の役割 （略） 我が国産業の国際的な競争力の源としても重要な情報が、サイバー攻撃等により窃取や破壊等された場合、我が国の社会経済発展を阻害する可能性がある。従って、企業や教育・研究機関にお	（３）各主体の役割 （略） ①（略） ②（略） ③企業や教育・研究機関の役割 （略） 我が国産業の国際的な競争力の源としても重要な情報が、サイバー攻撃等により窃取や破壊等された場合、我が国の社会経済発展を阻害する可能性がある。従って、企業や教育・研究機関にお

いては、個々における情報セキュリティ対策に加え、業務の委託先や提携先とも連携しつつ、サイバー攻撃に関する情報共有など業界団体等による集団的な対策に取り組むことが期待される。なお、各々の主体において情報セキュリティ対策に取り組む際には、第三者専門機関から、評価、監査を受けて、マネジメント標準を取得する等により、対策を向上していくことが期待される。	いては、個々における情報セキュリティ対策に加え、サイバー攻撃に関する情報共有など業界団体等による集団的な対策に取り組むことが期待される。なお、各々の主体において情報セキュリティ対策に取り組む際には、必要に応じて、第三者専門機関から、評価、監査を受けて、マネジメント標準を取得する等により、対策を向上していくことが期待される。
（略）	（略）
④一般利用者や中小企業の役割	④一般利用者や中小企業の役割
（略）	（略）
全人口の約８割がインターネット利用者となり 62、企業のインターネット利用率がほぼ１００%となる 63 など情報セキュリティ対策が必要となる対象が非常に広範囲に及んでいる中、一般利用者等が使用するパソコンやスマートフォン等がセキュリティホールとなり、サイバー攻撃の対象となる場合には、サイバー空間を介し、他の主体にも被害が波及する可能性がある。	全人口の約８割がインターネット利用者となり 62、企業のインターネット利用率がほぼ１００%となる 63 など情報セキュリティ対策が必要となる対象が非常に広範囲に及んでいる中、一般利用者等が使用するスマートフォン等がセキュリティホールとなり、サイバー攻撃の対象となる場合には、サイバー空間を介し、他の主体にも被害が波及する可能性がある。
（略）	（略）
⑤サイバー空間関連事業者の役割	⑤サイバー空間関連事業者の役割
（略）	（略）
また、現在、情報セキュリティ対策に関する製品等を海外事業者に大きく依存し、国内におけるセキュリティ従事者も不足する中、サイバー空間関連事業者においては、世界最先端の技術をも導入しつつ、高度な技術や製品の開発、高い能力を有する情報セキュリティ人材の育成やそれらの情報セキュリティ対策での利活用による市場創出等により、我が国の「サイバーセキュリティ産業」の国際競争力を強化することが重要である。	また、現在、情報セキュリティ対策に関する製品等を海外事業者に大きく依存し、国内におけるセキュリティ従事者も不足する中、サイバー空間関連事業者においては、高度な技術や製品の開発やそれらの情報セキュリティ対策での利活用による市場創出等により、我が国の「サイバーセキュリティ産業」の国際競争力を強化することが重要である。

３．取組分野 （１）「強靱な」サイバー空間の構築 ①（略） ②重要インフラ事業者等における対策 （略） 具体的には、重要インフラについて、重要インフラ事業者等におけるリスク評価手法に基づく情報セキュリティ対策の重点化を図るため、各分野における直近の安全基準等の策定・変更状況の把握・評価及びリスク分析を通じて、分野横断的に講じることが望ましいリスクを洗い出し、安全基準等を策定するための指針の中に反映するプロセスを確立する。 （略） ③企業・研究機関等における対策 我が国の国際的な競争力の源として重要な営業秘密等の企業秘密、知的財産情報や個人情報等の重要な情報を取り扱う企業や教育・研究機関において、サイバー攻撃に関するインシデント等の認知・解析機能を強化し、インシデント情報の共有促進を図る。また、企業等の海外進出先における情報セキュリティ対策を促進する。 情報セキュリティ対策に関する専門的な人材の確保や十分な投資等が困難となっている中小企業等について、サイバー攻撃に関するインシデントの認知機能等を強化するための環境整備を行うことが必要である。具体的には、中小企業に寄り添った情報提供・相談体制の整備、情報セキュリティ投資を促進する税制等のインセンティブの検討、情報セキュリティ向上のための利用し	３．取組分野 （１）「強靱な」サイバー空間の構築 ①（略） ②重要インフラ事業者等における対策 （略） 具体的には、重要インフラについて、重要インフラ事業者等におけるリスク評価手法に基づく情報セキュリティ対策の重点化を図るため、各分野における直近の安全基準等の策定・変更状況及びリスク分析を通じて、分野横断的に講じることが望ましいリスクを洗い出し、安全基準等を策定するための指針の中に反映するプロセスを確立する。 （略） ③企業・研究機関等における対策 我が国の国際的な競争力の源として重要な営業秘密等の企業秘密、知的財産情報や個人情報等の重要な情報を取り扱う企業や教育・研究機関において、サイバー攻撃に関するインシデント等の認知・解析機能を強化し、インシデント情報の共有促進を図る。 情報セキュリティ対策に関する専門的な人材の確保や十分な投資等が困難となっている中小企業等について、サイバー攻撃に関するインシデントの認知機能等を強化するための環境整備を行うことが必要である。具体的には、中小企業に寄り添った情報提供・相談体制の整備、情報セキュリティ投資を促進する税制等のインセンティブの検討、情報セキュリティ向上のための利用しやすいガイドライン・ツールの整備やクラウド技術を活用し、情報セキュリティが確保された共同利用システムへの移行促進等

やすいガイドライン・ツールの整備、クラウド技術の活用等により情報セキュリティが確保された共同利用システムへの移行促進等を図る。 （略） ④（略） ⑤（略） ⑥（略） （２）「活力ある」サイバー空間の構築 （略） ①産業活性化 （略） 今後、情報通信技術を利活用した製品やサービスが、国際的な取引において、サイバーセキュリティ上の信頼性を求められるようになる中、それを証明するものとして、国際標準化や評価・認証、情報セキュリティ監査の重要性が増してくると考えられる。このため、国際貿易において我が国が有利になるよう、国際標準化や評価・認証の国際的な相互承認枠組み作りに関して、積極的に参画・働きかけを進めるとともに、関係する民間部門への支援や国内の評価・認証機能の整備も進めていくことが必要である。具体的には、クラウドコンピューティングサービスにおける国際標準化や、複合機の国際的な共通セキュリティ要件の策定、セキュリティ検証施設を中核とした産業制御システムの評価・認証機関の整備を進めていく。 （略） ②（略）	を図る。 （略） ④（略） ⑤（略） ⑥（略） （２）「活力ある」サイバー空間の構築 （略） ①産業活性化 （略） 今後、情報通信技術を利活用した製品やサービスが、国際的な取引において、サイバーセキュリティ上の信頼性を求められるようになる中、それを証明するものとして、国際標準化や評価・認証、情報セキュリティ監査の重要性が増してくると考えられる。このため、国際貿易において日本企業が有利になるよう、国際標準化や評価・認証の国際的な相互承認枠組み作りに関して、積極的に参画・働きかけを進めるとともに、国内の評価・認証機能の整備も進めていくことが必要である。具体的には、クラウドコンピューティングサービスにおける国際標準化や、複合機の国際的な共通セキュリティ要件の策定、セキュリティ検証施設を中核とした産業制御システムの評価・認証機関の整備を進めていく。 （略） ②（略）

③（略） ④リテラシー向上 （略） 高齢者層における情報セキュリティ対策も今後一層重要となるため、情報セキュリティに関するサポーター等の育成・活用など高齢者に対するきめ細やかなフォローを行うための環境を整備する。また、一般家庭や若年層に対する知識や情報の提供に係る取組を促進する。 （略） （３）（略） ４．推進体制等 （１）（略） （２）評価等 本戦略に基づく各種取組施策の確実な実施及び各施策間の有機的な連携を確保する観点から、サイバーセキュリティ立国の実現に向けた中長期の目標の管理を行うとともに、本戦略に基づき、２０１３年度から毎年度の年次計画及びサイバーセキュリティに関する国際戦略を策定する。	③（略） ④リテラシー向上 （略） 高齢者層における情報セキュリティ対策も今後一層重要となるため、情報セキュリティに関するサポーター等の育成・活用など高齢者に対するきめ細やかなフォローを行うための環境を整備する。 （略） （３）（略） ４．推進体制等 （１）（略） （２）評価等 本戦略に基づく各種取組施策の確実な実施及び各施策間の有機的な連携を確保する観点から、サイバーセキュリティ立国の実現に向けた中長期の目標の管理を行うとともに、本戦略に基づき、２０１３年度から毎年度の年次計画及び国際分野における総合的な対応を推進するための方針を策定する。