新たな情報セキュリティ戦略の方向性について

資料1

環境の変化

サイバー空間と実空間の融合・一体化

- *情報通信技術の普及・高度化・利活用の進展*
  - *→ワイヤレス、クラウド、医療・就労・行政・防衛　等*
- *今後の成長による更なる進展*
  - *→ビッグデータ、M2M、IoT、ITS、スマートグリッド　等*
- *グローバルな拡大・浸透*
  - *→先進・新興・途上国等で成長のエンジンとして期待　等*

サイバー空間を取り巻くリスクの深刻化

- *甚大化するリスク*
  - *→国家・企業機密、基幹インフラ制御、医療機器　等*
- *拡散するリスク*
  - *→スマートフォン、家電、複合機、車、社会インフラ　等*
- *グローバルリスク・ボーダレスリスク*
  - *→外国からの攻撃、国内を踏み台とする外国への攻撃　等*

基本的な方針

国家の安全保障及び経済発展、国民の安全・安心を確保するため、
世界を率先する強靭で活力あるサイバー空間を実現
（「サイバーセキュリティ立国」）

① 情報の自由な流通の確保

- 管理や規制を過度に行うことなく、開放性や相互運用性を確保することにこれまで努力。
- 実空間のあらゆる活動が相互依存する神経系として、経済成長等を実現することが必要。

② リスクの深刻化への新たな対応

- リスクが甚大化、拡散し、さらに、リスクがグローバル化・ボーダレス化する状況が発生。
- 今後は、今までの取り組みとは異なる新たな対応が必要。

③ リスクベースによる対応

- サイバー攻撃の脅威が増大している状況では、全ての脅威に対応するのは不可能。
- リスクの性質を踏まえたリスクベースの対応強化が必要。

④ 社会的責務を踏まえた行動と共助

- サイバー空間に相互依存する官・公・学・産・民による社会的責務を踏まえた行動が必要。
- 社会的立場に応じた役割を発揮し、相互に、国際的にも連携しながら共助することが必要。

各主体の役割の明確化

●サイバー空間に相互依存する官・公・学・産・民による社会的責務を踏まえた行動が必要。
●社会的立場に応じた役割を発揮し、相互に、国際的にも連携しながら共助することが必要。

① 国による積極的・先導的な役割

・国際規範形成への積極的参画等のサイバー空間に関する外交。　サイバー空間の防衛や犯罪対策。
・各種制度整備等による取組促進。　先端技術開発。　対策実施主体としての政府機関等における対策強化。

② 重要インフラ事業者等による安定的な役割

・電子行政やスマートグリッド等が今後展開。サイバー攻撃等により、甚大な被害をもたらす恐れ。
・政府機関等における対策に準じた取組。

③ 企業や教育・研究機関による協調的な役割

・営業秘密、知的財産情報や個人情報等、競争力の源泉となる情報を保有。国際競争力の礎としても重要。
・サイバー攻撃による情報窃取等により、産業競争力を阻害する恐れ。産業全体としての取組。

④ 一般利用者や中小企業による自律的な役割

・全てにおいて隅々までの対応が困難。セキュリティホールとして攻撃対象となり、他者に波及する恐れ。
・リテラシー向上等の取組。

⑤ 情報通信関連事業者等による自浄的・自立的な役割

・サイバー空間を構成する技術等は民間企業が中心に提供。海外技術等への依存が高い状況。
・情報通信関連事業者によるサイバー空間衛生確保や国内セキュリティ事業者による製品開発等の取組。

取組分野

1. 強靱なサイバー空間（サイバー空間の持続性）

▸インシデント情報の共有やサイバー空間の自浄機能等を通じ、攻撃等に対する防御/回復力が強化された社会

①政府・重要インフラ等対策	【例】政府システムのセキュリティ抜本的強化、重要インフラ範囲見直し、GSOC強化　等
②企業等対策	【例】企業秘密等に係るインシデント情報の共有強化、サプライチェーンセキュリティ　等
③サイバー空間の「防衛」	【例】関係主体の役割の明確化　等
④サイバー空間の犯罪対策	【例】証拠保全・フォレンジックの強化、司法・警察分野における人材育成の強化　等
⑤サイバー空間の衛生	【例】セキュリティ認証の制度整備、インシデント認知等における関連制度の弾力化　等

※GSOC（Government Security Operation Coordination team）

2. 活力あるサイバー空間（サイバー空間の発展性）

▸高度な技術や人材の育成/蓄積等を通じ、新たなリスクに自立的に対応できる創造/知識力が強化された社会

①産業活性化	【例】サイバー空間の高度利用、政府による調達等の促進、研究開発の強化　等
②人材育成	【例】高度な資格制度の創設と政府による採用、産学連携による実践教育の強化　等
③リテラシー向上	【例】初等中等教育におけるリテラシー教育の強化、効果的な普及・啓発の推進　等

3. 世界を率先するサイバー空間（サイバー空間のグローバル性）

▸国際的なルール形成や信頼の醸成等を通じ、グローバルな戦略空間における貢献/展開力が強化された社会

①外交	【例】共通の価値を有する国等との関係強化、国際規範形成への積極的参画　等
②国際展開	【例】ASEAN諸国等への日本企業の進出支援、国際標準化の推進　等
③国際連携	【例】海外捜査機関等との情報共有の促進、CSIRT間連携の強化　等

※CSIRT（Computer Security Incident Response Team）

体制・制度

【例】政策会議・NISCの強化、中長期目標の管理、セキュリティクリアランスによる情報共有促進　等

【参考①】　サイバー空間を取り巻くリスクの深刻化（例）

●：国内外で実際起こったもの、○：可能性が指摘されているもの。

甚大化するリスク

- ● 標的型攻撃により、国家機密、企業機密の窃取が発生。数年前からの窃取も発覚。
- ● 海外にて、クローズな制御系システムがウィルス感染。核関連施設が稼働不能化。
- ● 海外にて、元契約社員により、制御系システムが不正操作され、川に汚水が流入。
- ○ ITSやスマートグリッドへの攻撃による交通混乱やブラックアウトの恐れが指摘。

拡散するリスク

- ● 常時、電源ON・ネット接続で携帯されるスマートフォンから情報流出が多発。
- ● コンビニにおける防犯カメラが踏み台となり、DDoS攻撃を実施。
- ○ ネット接続の家電や自動車から生活情報や位置情報が流出する恐れが指摘。
- ○ オフィスにおけるコピー機等の複合機が情報窃取の起点となる恐れが指摘。

グローバルリスク

- ● 海外にて、外国政府の関与が疑われる政府機関等に対するDDoS攻撃が発生。
- ● 海外にて、企業秘密の窃取等を狙った外国軍隊の関与が疑われる攻撃が発生。
- ● 国内の個人PC等が踏み台となり、指令サーバとして外国にDDoS攻撃を実施。
- ○ 武力攻撃の一環としてのサイバー攻撃が国内を起点に外国へ行われる恐れが指摘。

【参考②】 新たな情報セキュリティ戦略のイメージ

環境の変化

サイバー空間と実空間の融合・一体化 ［普及・高度化、更なる進展、グローバルな拡大・浸透］ ▶ サイバー空間を取り巻くリスクの深刻化 ［甚大化、拡散、グローバル・ボーダレス］

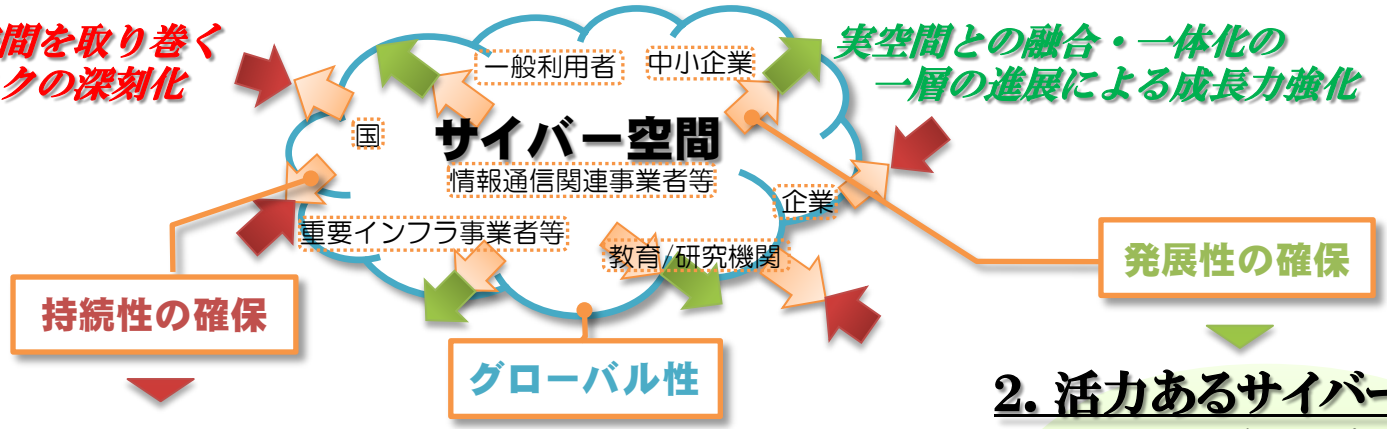
基本的な方針

国家の安全保障及び経済発展、国民の安全・安心を確保するため、世界を率先する強靭で活力あるサイバー空間を実現（「サイバーセキュリティ立国」）

① 情報の自由な流通の確保　② リスクの深刻化への新たな対応
③ リスクベースによる対応　④ 社会的責務を踏まえた行動と共助

各主体の役割の明確化

国による積極的/先導的な役割 ／ 重要インフラ事業者等による安定的な役割 ／ 企業や教育・研究機関による協調的な役割 ／ 一般利用者や中小企業による自律的な役割 ／ 情報通信関連事業者等による自浄的/自立的な役割



取組分野

1. 強靭なサイバー空間

サイバー空間の防御力・回復力の強化

①政府・重要インフラ等対策
②企業等対策
③サイバー空間の「防衛」
④サイバー空間の犯罪対策
⑤サイバー空間の衛生

2. 活力あるサイバー空間

サイバー空間の創造力・知識力の強化

①産業活性化
②人材育成
③リテラシー向上

3. 世界を率先するサイバー空間

サイバー空間の貢献力・展開力の強化

①外交
②国際展開
③国際連携

体制・制度

情報セキュリティ政策会議・ＮＩＳＣの強化、中長期目標管理、セキュリティクリアランスによる情報共有促進　等