

### 1. 最近の環境変化

#### ○本格的なサイバー攻撃等の発生と深刻化

- ・ 標的型攻撃の拡大と深刻化
- ・ インターネット以外の環境における脅威の顕在化 等

#### ○社会経済活動の情報通信技術への依存度の更なる高まりとリスクの表面化

- ・ スマートフォン等の本格的な普及と脆弱性を利用した攻撃の表面化 等

#### ○新たな技術革新に伴う新たなリスクの出現

- ・ M2M(Machine To Machine)環境の出現 等

#### ○重大なIT障害のリスク回避に向けた取組の必要性の高まり

- ・ 東日本大震災に伴う事業継続計画（BCP）上の問題の顕在化 等

#### ○諸外国における取組の強化

- ・ 諸外国による安全保障面を含む情報セキュリティへの取組の強化 等

### 2. 基本方針

「国民を守る情報セキュリティ戦略」（2010年度～2013年度の4カ年計画）で示された基本的考え方、及び、最近の環境変化と関連施策の実施状況を踏まえた以下の視点の下、施策を重点化して取りまとめる。

- 国や国の安全に関する重要な情報を扱う企業等に対する高度な脅威への対応強化
- スマートフォン等の本格的な普及に伴うリスクの表面化に対応する安全・安心な利用環境の整備
- 国際連携の強化

### 3. 主な施策

- (1) 大規模サイバー攻撃事態への対処態勢の整備等
- (2) 政府機関等の基盤強化
- (3) 重要インフラの基盤強化
- (4) 標的型攻撃に対する官民連携の強化
- (5) 脅威の高度化・多様化への対応
- (6) 研究開発、人材育成の推進
- (7) 情報セキュリティ産業の振興
- (8) 国民・利用者保護の強化
- (9) 制度整備
- (10) 国際連携の強化

## 施策例

- ① 各府省庁は、CSIRT等の機能を有する体制を整備し、遺漏なく継続的な対策を実施する。
- ② 陸自電算機防護システム等、情報システムを監視・防護するための器材を整備する。
- ③ サイバー攻撃に関する官民の情報共有の更なる推進を図る。
- ④ 攻撃手法が複合化・複雑化するサイバー攻撃について高度解析する枠組みを検討する。
- ⑤ スマートフォンにおける情報セキュリティ対策を強化する。
- ⑥ M2M環境における情報セキュリティ対策の在り方を検討する。
- ⑦ 災害時における業務継続性確保のため、クラウドへの移行等を促進する。
- ⑧ 制御システムのセキュリティに係る検証施設の構築、国際標準化及び評価・認証制度の整備等を促進する。
- ⑨ 改正不正アクセス禁止法に基づき、取締りの強化や普及啓発等を図り、官民連携した不正アクセス防止対策を推進する。
- ⑩ サイバー空間に関する国際規範作りに積極的に関与する。