

# 「国民を守る情報セキュリティ戦略」の概要

平成22年5月11日情報セキュリティ政策会議決定

## 現状の課題

### 大規模なサイバー攻撃事案等の脅威の増大

- ✓重要インフラ等、国民生活に直結するサービスの情報通信技術への依存による脅威の増大
- ✓国境を越えたサイバー攻撃が現実化(米韓大規模サイバー攻撃(昨年7月))
- ✓ガンブラーウイルス等、年々新たなウイルスが出現。攻撃手法も高度化・多様化

### 急速な技術革新の進展

- ✓クラウド・コンピューティング技術、IPv6への移行
- ✓暗号の危殆化につながるコンピュータの能力向上

### 社会経済活動の情報通信技術への依存度の増大

- ✓情報家電、電子タグなどあらゆる機器がネットワークに接続
- ✓約8割の国民が情報セキュリティに不安感

### グローバル化の進展

- ✓国境を越えた瞬時の情報流通
- ✓各国の個人情報保護・情報セキュリティ制度の調和

- 重要インフラ等の国民生活に直結するサービスの情報通信技術への依存の高まりにより、脅威(ITリスク)は着実に増大
- 情報セキュリティ上の攻撃手法が多様化・高度化・複雑化しており、従来の取り組みでは対応が困難
- 各国でも戦略的な取り組み(\*)を実施

課題に対応する  
新戦略の必要性

(\*)米国

- ・サイバースペース政策レビュー(60日レビュー)
- ・「サイバーセキュリティ調整官」を設置し、国家的取組みを強化
- ・「2010 Cybersecurity Enhancement Act」(2010年2月)

## 「国民を守る情報セキュリティ戦略」

## 国民を守る情報セキュリティ戦略(2010~2013)

第2次基本計画(2009~2011)

(\*)第2次情報セキュリティ基本計画を  
包含し、今後4年間の重点的な取組み

## 基本的な考え方(取組みの重点化)

- ①サイバー攻撃の発生を念頭に置いた政策強化・対処体制整備
- ②新たな環境変化に対応した政策の確立
- ③受動的な対策から能動的な対策へ

➤ITリスクを克服し、安全・安心な国民生活を実現

- サイバー空間の安全保障・危機管理政策の強化と情報通信技術政策の連携
- 安全保障・危機管理及び経済の観点に国民・利用者保護の観点を加えた3軸構造の総合的な政策(特に、国民・利用者の視点を重視した政策の推進)
- 国際連携の強化

安全・安心な国民生活を実現

サイバー空間上の我が国の安全保障・危機管理の確保

情報通信技術の利活用を促進し、我が国の経済成長に寄与

## 実現すべき成果目標

2020年までに、インターネットや情報システム等の情報通信技術を利用者が活用するにあたっての脆弱性を克服し、全ての国民が情報通信技術を安心して利用できる環境(高品質、高信頼性、安全・安心を兼ね備えた環境)を整備し、世界最先端の「情報セキュリティ先進国」を実現

# 具体的な取組

## ● 強力なリーダーシップの下、総合的な政策推進体制を確立し、官民の役割の明確化、官民連携を強化

### 1 大規模サイバー攻撃事態への対処態勢の整備等

#### サイバー攻撃事態への 対処態勢の整備

・平時からの対策と事案対処の連携強化

#### ➤ 対処態勢の整備

- ・初動対処態勢の整備
- ・初動対処訓練の実施
- ・官民連携の推進
- ・サイバー攻撃に対する防衛分野での体制強化
- ・サイバー犯罪の取締り 等

#### ➤ 平素からの情報収集・共有体制の構築・強化

- ・対処に資する情報収集・分析・共有体制の強化
- ・諸外国等との情報共有体制の構築・強化

### 2 新たな環境変化に対応した情報セキュリティ政策の強化

#### 国民生活を守る情報セキュリティ基盤の強化

##### ➤ 政府機関等の基盤強化

- ・各府省の最高情報セキュリティ責任者(CISO)の強化
- ・政府横断的な情報収集・分析システム(GSOC)の強化
- ・政府統一基準の見直し、政府機関情報システムの対策強化
- ・共通番号制に対応した情報セキュリティ対策の検討 等

##### ➤ 重要インフラの基盤強化

- ・分野横断的な官民連携体制の強化
- ・情報共有体制の強化、サービス提供が確保できるシステム等の検討
- ・事業継続計画(BCP)の充実 等

##### ➤ その他の基盤強化

- ・マルウェア対策の充実・強化
- ・クラウド化、IPv6に対応した情報セキュリティ確保方策
- ・中小企業に対する情報セキュリティ対策支援
- ・医療、教育分野等における情報セキュリティ確保方策 等

#### 国民・利用者保護の強化

##### ➤ 普及啓発活動の充実・強化

- ・情報セキュリティ月間による普及啓発の強化
- ・包括的な普及啓発プログラムの策定

##### ➤ 情報セキュリティ安心窓口(仮称)の検討

- ・地域NPO法人等の支援
- ・国民・利用者からの相談受付窓口の検討

##### ➤ 個人情報保護の推進

- ・プライバシー保護技術の適切な利用促進
- ・個人情報保護に関するガイドラインの見直し
- ・国際的なフレームワークへの対応 等

##### ➤ サイバー犯罪に対する態勢の強化

- ・犯罪取締りのための基盤整備の推進 等

#### 国際連携の強化

##### ➤ 米国、ASEAN、欧州等との連携強化

- ・日米サイバーセキュリティ会合、日ASEAN情報セキュリティ政策会議等を通じた戦略的連携強化
- ・海外CSIRTの構築支援
- ・新たな二国間関係の構築

##### ➤ APEC、ARF、ITU、MERIDIAN、IWWN等の 国際会合を活用した情報共有体制等の強化

- ・国際会議への積極的な参加を通じた情報共有体制の強化

##### ➤ NISCの窓口機能の強化

- ・情報セキュリティに関するベストプラクティスの共有等
- ・情報セキュリティ政策について諸外国等と連携強化 等

#### 技術戦略の推進等

##### ➤ 情報セキュリティ関連の研究開発の戦略的推進等

- ・新たな情報セキュリティ研究開発戦略の策定
- ・高度化・多様化する攻撃等に対応できる技術の実現・普及  
(「グランドチャレンジ型」研究開発の推進)

##### ➤ 情報セキュリティ人材の育成

- ・政府、大学、企業等における高度な情報セキュリティ人材の育成

##### ➤ 情報セキュリティガバナンスの確立

- ・情報セキュリティガバナンスの経営としての位置付け
- ・事業継続計画(BCP)の策定、情報セキュリティ監査 等

#### 制度整備

##### ➤ サイバー空間の安全性・信頼性を向上させる制度の検討等

- ・コンピュータウイルス関連の法改正等サイバー犯罪条約の早期締結に向けた検討
- ・機微な情報へのアクセス権限の明確化の検討 等

##### ➤ 各国の情報セキュリティ制度の比較検討

- ・各国間の法制度等の相違について分析し、情報セキュリティ関連の国際連携のための課題抽出・連携方策の検討を実施