「第1次基本計画」及び「重要インフラの指針」の決定

2006年2月

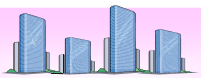
内閣官房情報セキュリティセンター（NISC）

第1次情報セキュリティ基本計画

ー「セキュア・ジャパン」の実現に向けてー（2006年2月2日　情報セキュリティ政策会議決定）

○行政機関からの情報漏洩、国民生活・社会経済活動の基盤となる重要インフラの情報システムの停止等、情報セキュリティ問題は多発し複雑化する一途。
○情報セキュリティ問題全般に関する中長期計画として、「第1次情報セキュリティ基本計画」（2006年度から2008年度までの3ヵ年計画）を策定。

現状



政府機関・地方公共団体
◆行政機関からの情報漏洩（複数　　等

重要インフラ
◆航空関連システムの停止、証券取引システムの停止 等

企業
◆企業からの個人情報の漏洩（複数）　等

個人
◆インターネットバンキング情報の窃取（複数）　　等

第1次情報セキュリティ基本計画
ー 「セキュア・ジャパン」の実現に向けて ー

基本理念

1. 経済国家日本の基盤としての情報セキュリティ
2. 安全・安心を求める、より良い国民生活実現のための情報セキュリティ
3. 新たな安全保障確保の観点からの情報セキュリティ

＜捉えるべき視点＞

◆我が国の経済基盤（商取引）の1／4はITに依存

◆世界最大のブロードバンド大国
◆災害対策等安全・安心に対する国民ニーズの高まり

◆ITに起因する新しい安全保障への脅威と、我が国の「強み」の再認識

今後3年間の取組み

官民の各主体が適切な役割分担を果たす「新しい官民連携モデル」の構築
～ 内閣官房情報セキュリティセンター（NISC）を中心に、全主体が参加して実行 ～

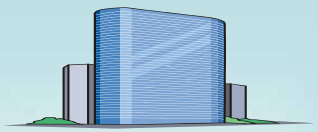
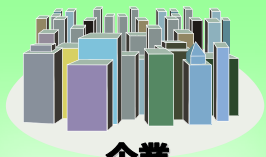
目指すべき姿

「情報セキュリティ先進国」への進展

［政府機関］：**すべての政府機関**が「政府機関統一基準」が求める水準の対策を実施。［重要インフラ］：IT障害の発生を**限りなくゼロ**に。
［企業］：企業における情報セキュリティ対策の実施状況を**世界トップクラスの水準**に。［個人］：「IT利用に不安を感じる」とする個人を**限りなくゼロ**に。

第1次情報セキュリティ基本計画－今後3年間の重点政策－

○全主体が適切な役割分担を果たす「新しい官民連携モデル」の構築に向けて、今後３年間、政府は「第１次情報セキュリティ基本計画」に基づき、各種対策を強化。

	政府機関・地方公共団体	重要インフラ	企業	個人
				
役割	情報セキュリティ対策の「ベストプラクティス」へ	国民生活・社会経済活動の基盤としての安定供給の確保	市場に評価される情報セキュリティ対策の実施	IT社会の担い手としての意識の向上
今後３年間の主な重点政策①（４領域）	◆政府機関統一基準に基づいた 各省庁の評価 ◆ サイバー攻撃等への緊急対応能力の強化	◆ 情報共有・分析機能の整備 ◆ 重要インフラ連絡協議会の設置 ◆ 分野横断的な演習、相互依存性解析の実施	◆政府調達における入札条件の整備 ◆ 情報セキュリティ監査等第三者評価制度の活用推進 ◆ コンピュータウィルス等への対応体制の強化	◆ 情報セキュリティ教育の推進 ◆「情報セキュリティの日」の創設等広報啓発の強化 ◆ ユーザーフレンドリーなサービスの提供等の環境整備
	政府機関統一基準	重要インフラ行動計画	各省庁による施策	各省庁による施策

今後３年間の主な重点政策②（横断的事項）

情報セキュリティ技術戦略の推進
◆政府が活用することを前提とした技術開発実施
◆「グランドチャレンジ型」技術開発の推進

情報セキュリティ人材の育成確保
◆ 多面的・総合的能力を有する実務家の育成
◆ 情報セキュリティの資格制度を体系化

国際連携・協調の推進
◆ 国際的な安全・安心の基盤づくりへの貢献
◆ 我が国発の国際貢献

犯罪の取締り、権利利益の保護救済
◆ サイバー犯罪の取締り強化及び関連基盤整備
◆ サイバー空間の安全性向上のための技術開発

重要インフラの「安全基準等」の指針

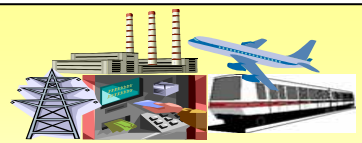
○証券取引や航空関連の情報システムの停止、重要情報の漏洩など、国民生活・社会経済活動の基盤となる重要インフラ(※1)のIT障害(※2)が昨今多発。

○IT障害から重要インフラを防護するための全体計画として「重要インフラの情報セキュリティ対策に係る行動計画」を策定（2005年12月13日情報セキュリティ政策会議決定）。

○このうち、まず喫緊に対応すべきものとして、重要インフラ分野ごとの規範となる「安全基準等」を策定するにあたり、規定が望まれる事項（対策を行うべき事項）について、横断的に示した「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」を今般策定。

（※1）重要インフラ10分野：情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流

（※2）重要インフラの各事業において発生する障害(サービスの停止や機能の低下等)のうちITの機能不全が引き起こすものを「IT障害」という。



重要インフラの情報セキュリティ対策に係る行動計画

（2005年12月13日情報セキュリティ政策会議決定）

【4つの柱】

1. 「安全基準等」の整備
2. 情報共有体制の構築（CEPTOAR）
3. 相互依存性解析の実施
4. 分野横断的演習の実施

重要インフラの「安全基準等」の指針

- 分野横断的視点から、情報セキュリティ対策の実施にあたり、対処がなされていることが望ましい項目を列記

＜4つの柱＞

1. 組織・体制及び資源の確保
2. 情報についての対策
3. 情報セキュリティ要件の明確化に基づく対策
4. 情報システムについての対策

＜3つの重点項目＞

1. IT障害の観点から見た事業継続性確保のための対策
2. 情報漏えい防止のための対策
3. 外部委託における情報セキュリティ確保のための対策

これを受け、各重要インフラ分野において、「安全基準等」の策定・見直し（2006年9月まで）