

「第1次情報セキュリティ基本計画」 の概要について

2006年6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

- 「セキュア・ジャパン」の実現に向けて - (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カ年計画)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

- 「セキュア・ジャパン」の実現に向けて -

< 捉えるべき視点 >

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

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 ~

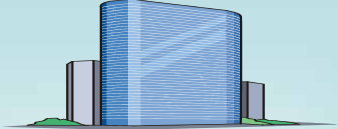
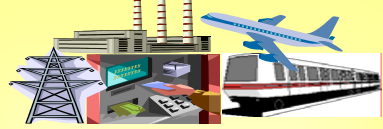


目指すべき姿

「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 (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 |
| 【個別設計図】 | 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
(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

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

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

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

今後3年間のマイルストーン全体像

「全体工程表」(基本計画)と「個別詳細設計図」を組み合わせ、毎年度のマイルストーンを明確にし
ながら、「情報セキュリティ先進国」への進展を目指す。

