NISC National Information Security Center

「第2次情報セキュリティ基本計画（案）」と技術戦略について

平成21年1月19日

内閣官房情報セキュリティセンター（NISC）
http://www.nisc.go.jp

資料3－2

「次期情報セキュリティ基本計画に向けた第１次提言」(2006年6月19日)の概要

第１次情報セキュリティ基本計画 (2006年度～2008年度)

- 我が国の情報セキュリティ政策の立ち上げ
- 「気付きを与える」ための戦略
- 官民各主体のＩＴの安心・安全な利用へ向けた取組み

『情報セキュリティ立国』の思想

『ジャパン・モデル』の確立・世界への展開 (高品質・高信頼性・安心安全)

『情報セキュリティ先進国』の実現

目指すべき結果

情報セキュリティ上の問題がない水準

継続

- 情報セキュリティ上の問題がない水準は目指す
- 各主体最大限の尽力は更に進める
- 対策の推進、水準の向上

発展

- 具体的取組みの持続的な推進
- 「事故前提社会」への対応力強化
- 合理性に裏付けられたアプローチの実現

第２次情報セキュリティ基本計画(仮称)

基本理念

『成熟した情報セキュリティ立国』

●より現実に即した実効的な情報セキュリティ対策●

- 冷静で迅速な対応
- 最適な水準の対策の効果的・効率的な実施
- 説明責任の明確化

ITルネサンス

世界との協調・イニシアティブの発揮

基本目標

「ＩＴを安心して利用可能な環境」の構築

●基本目標に向けて考慮すべき諸点●

「事故前提社会」への対応力強化

- 理解(気付き)の推進、判断力の向上
- 事後対応への更なる注力
- 主体間の共通理解、信頼関係の構築
- 事実把握と被害拡大防止・再発防止への情報共有

合理性に裏付けられたアプローチの実現

- 脅威の把握、リスクへの柔軟な対応
- コスト・利便性とのバランス
- 最適な「水準」に関する認識の共有
- 人的側面の対策　・説明責任の明確化

「第1次情報セキュリティ基本計画」の成果と「第2次情報セキュリティ計画（案）」の目標（目指す「姿」）

1. 第1次基本計画（'06～'08年）

成果

情報セキュリティ政策の立上げ

◆関係者の「気付き」を高めた

→ P to Pソフトで情報流出の危険性

→ サイバー攻撃で情報を盗まれる危険性

→ システム障害で事業が止まる危険性

◆とりあえず政策推進の枠組みは構築

→ 政府機関の統一基準に基づく対策と評価

→ 重要インフラ事業者間の情報共有体制

→ 日米、日ASEANで情報交換を行う枠組み

◆（問題が生じないための）事前対策の取組みはある程度進展

→ 但し、日々新たなリスクが生まれ、また変化している

2. 第2次基本計画（'09年～'11年）

目標

政策の継続と更なる発展

◆事前対策は当たり前のことに

◆問題が生じても、冷静かつ迅速に事後対応・復旧活動を推進できる

◆情報を管理する側に加えて、情報を預ける側も取組みの対象に

「第2次情報セキュリティ基本計画（案）」の構造

第1章

第1次情報セキュリティ基本計画の下での取組みと2009年の状況

1 第1次情報セキュリティ基本計画の下での取組み （第1次基本計画の考え方などについて記述）

2 2009年の状況 （第1次基本計画の下で様々な取組みを進めた結果、どのような状況となっているか考察）

第2章

第2次情報セキュリティ基本計画における基本的考え方と2012年の姿

1 第2次情報セキュリティ基本計画の基本的考え方 （第2次基本計画の考え方などについて、適宜第1次基本計画と比較しながら記述）

2 2012年の姿 （第2次基本計画の下で様々な取組みを進めた結果、計画期間後にどのような姿となると考えているか記述）

第3章

今後3年間に取り組む重点政策

1 対策実施4領域における取組みの推進と政策目的の着実な実現 （政府・地方公共団体、重要インフラ、企業、個人について記述）

2 横断的な情報セキュリティ基盤の強化と発展 （技術、人材、国際、犯罪対策などについて記述）

第4章

政策の推進体制と持続的改善の構造について

1 政策の推進体制

2 他の関係機関等との関係

3 持続的改善構造の構築

「第2次情報セキュリティ基本計画（案）」の全体像 ［1］

○「第２次情報セキュリティ基本計画（案）」は、情報セキュリティ問題全般に係る中長期計画（全体設計図）として、今後の我が国の取組みに関する、１）基本的考え方と、２）重点政策の方向性を提示。

○具体的には、2009年度～2011年度までの3カ年計画として策定。これまで同様、本計画に基づいた年度ごとの推進計画である「セキュア・ジャパン」を策定するとともに、年度ごとの取組み状況や社会変化などに関する評価等を行う予定。

第１次基本計画からの「発展」と「継続」

1. 具体的取組みの持続的な推進、新たな課題への政策的対応　（第1次基本計画で構築した取組みの各種枠組みを持続的に活用）
2. 「事故前提社会」への対応力強化　（十分な事前対策の取組みにも関わらず、万が一問題が生じた場合を考えて準備を怠らない）
3. 合理性に裏付けられたアプローチの実現　（情報資産の価値、リスクの大きさに応じた合理的（最適）な水準の対策を実現）

第２次基本計画の基本的考え方

●基本目標　→　「ITを安心して利用できる環境」の構築　（第1次基本計画と同様。IT基本法第22条の実現）

●取組みにあたっての基本理念　→　「セキュリティ立国」の思想の成熟　（IT時代の力強い「個」と「社会」の確立へ）
（目指す「姿」は、最適な水準の取組みとセキュリティの実現であり、絶対的な無謬性の追求ではない　→　絶対的な無謬性から脱却するには国民や社会全体の意識改革も不可欠）

●基本目標の実現に向けた取組み　→　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」
＋（対策実施側のみならず）情報提供側も視野に入れた取組みの推進
（第1次基本計画の下では、対策実施主体及び対策支援主体による「新しい官民連携モデル」を追求。状況変化を踏まえ、新たに情報提供側も視野に入れた取組みを推進）

「第2次情報セキュリティ基本計画（案）」の全体像 ［2］

第2次基本計画の下で取組みを行う政策領域

●課題の把握から事前対策、事後対応まで視野に入れた取組み
（事前対策のみならず、万が一問題が生じた場合も視野に入れて事後対応の準備を進める）

●技術面での対応から制度面、人的側面の対応まで視野に入れた取組み
（技術開発から人材育成のような側面まで幅広く取組みを進める）

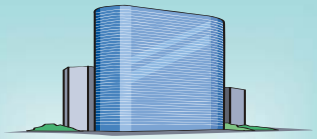
●国内における対策の推進から、情報セキュリティ確保のために国際的になされる活動も視野に入れた取組み
（IT利用・活用においては国境を越えるのは当然となっており、国内の取組みと国際的な取組みを有機的に結びつけた取組みとする）

●国民の日常生活や経済活動といった個別主体に関係の深い領域から、安全保障や文化といった我が国全体に関係の深い領域にまで対応した取組み
（情報セキュリティ問題は相当程度幅が広いことに鑑み、様々な観点から柔軟かつ領域横断的に取組みを進める）

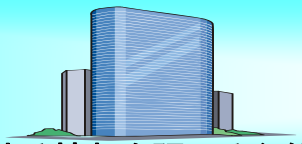
「第2次情報セキュリティ基本計画」に基づく取組み　－今後3年間の重点政策－

NISC

主な重点政策①（4領域）3年間の

政府機関・地方公共団体	重要インフラ	企業	個人
			
◆能動的に情報セキュリティ対策を推進する体制確立 （最高情報セキュリティアドバイザー設置、年次報告書の報告・公表） ◆事業継続性確保の検討、サイバー攻撃等への緊急対応能力強化	◆安全基準等の整備及び浸透 ◆情報共有体制の強化 ◆共通脅威分析の実施 ◆分野横断的な演習、	◆情報セキュリティ監査等第三者評価制度の活用推進 ◆対策容易化のためのツール提供 ◆中小企業の対策促進 ◆コンピュータウィルス等への対応体制の強化	◆学校や地域における情報モラル等の教育の推進 ◆個人の質問対応を行えるようなサポータの育成 ◆サービス提供事業者や対策支援主体によるリスク情報等の個人への適切な提供促進
（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

主体 情報提供



自身の有する情報を預ける主体　（新たな課題として、関係機関等が協力しながら取組みを検討・推進）

主な重点政策②（横断的事項）3年間の

情報セキュリティ技術戦略の推進
- ◆セキュリティ対策を埋め込んだ機器の開発促進
- ◆「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
- ◆政府機関における人材の育成・確保
- ◆保有するスキルの見える化の推進

国際連携・協調の推進
- ◆世界の脅威動向を把握するための官民連携確立
- ◆アジアにおける知恵の結集と水準の向上

犯罪の取締り、権利利益の保護救済
- ◆犯罪取締りのための基盤整備の推進
- ◆権利利益の保護・救済のための基盤整備の推進

第２次情報セキュリティ基本計画における技術戦略が描く「２０１２年の姿」と重点施策

第2次情報セキュリティ基本計画における「技術戦略の推進」に関する施策

第1次基本計画下での施策：「先進的技術の追求」を基本方針の一つとして、
①効率的な開発実施体制の構築、②技術開発の重点化と環境整備、
③グランドチャレンジ型開発の推進を実施

→①、③について一層の推進が必要。また、社会情勢の変化（ITへの依存度の高まり、社会構成の変化、脅威の変化）に伴い、新たに取り組むべき課題も発生。

第2次計画では

・我が国の研究開発が、世界で最も効果的・効率的に進められる体制となることを目指す。（利用者による対策が不要な端末や情報家電の提供、設計段階からセキュリティを作り込む開発手法の普及定着、リスクの形式的な表記法や リスク評価方式の共通化を実現する）

○ 情報セキュリティ技術開発の重点化と多様性の維持

・・・利用者に対策への過度の負担を強いない、事前に情報セキュリティ対策が埋め込まれた、安全・安心な機器の実現や利用者環境の提供を、重点的に取り組むべき課題として取組みを推進。一方で、研究開発・技術開発の多様性を確保するため、市場として成立していないために企業が取り組まない分野や、将来的なリスクに対抗するための先行的な開発・・・など、我が国として戦略的に推進すべき分野に対しては、政府が積極的に取り組むこととする。

○「グランドチャレンジ型」研究開発・技術開発の推進

○研究開発・技術開発の効率的な実施体制の構築と基盤の整備

・・・開発の計画策定時にプロジェクトの途中で得られた成果を活用する手順を組み込むとともに、プロジェクトの内容および実施状況の公開を促進する。・・・必要性が高い場合には計画変更が可能な、柔軟なプロジェクト管理の仕組みを導入・・・さらに、リスクの表記法や評価方式の共通化、情報セキュリティに関するデータベースの整備と共有、及び隔離ワークベンチの構築などによって、研究開発の支援と加速を図る。

第2次情報セキュリティ基本計画における「技術戦略が描く姿」

技術戦略推進のために描く「2012年の姿」

2012年に情報セキュリティの技術戦略の取組みが以下のような「姿」となっていることを目指す。

① 利用者による情報セキュリティ対策が不要な端末や情報家電の提供

- 利用者に負担を与えずにセキュリティを確保
- 高齢者らの、認識力の衰えなどによるミスや誤認があっても被害の発生を防ぐ

→ 出荷段階からセキュリティ設定が適切になされ、安全で安心な製品を提供

② 設計段階からセキュリティを作り込む開発手法の普及と定着

- 信頼性や性能等の品質と同じく、情報セキュリティを設計段階から考慮すべきと広く認識
- 効率的に安全な製品を開発する手法の確立とノウハウと人材の蓄積

→ ・セキュリティへの考慮が必要な製品やサービスの範囲拡大への対応、
妥当なコストで重大な脆弱性や欠陥を事前回避
・日本製品の国際競争力の強化

③ リスクの形式的な表記法や、リスクの評価方式の共通化

- 表記法や評価方式の共通化

→ ・ソフトウェアや情報システムのセキュリティに関するリスク情報の迅速な共有を寄与
・新たな脅威の危険性の評価、安全なソフトウェアの効率的な開発手法の確立、
対策の合理性の判断などにも大きく寄与

技術戦略関連で今後3年間に取り組むべき重点政策の概要

① 情報セキュリティ技術開発の重点化と多様性の維持

- 基盤としてのIT強化、ITを安心して利用できる環境実現を目標とした開発を重点促進
- 将来にわたる主導的かつ優位な国際的な地位を確保する視点を持って開発を推進
- 市場が成立してない分野や開発コストが巨大な分野における、基礎研究や先行的な開発を推進

②「グランドチャレンジ 型」研究開発・技術開発の推進

- 喫緊の課題の解決：
  (1) 要素技術の統合・実装で迅速に対応
  (2) 組織・人間系の管理手法の高度化や利用者の啓発と、技術とを組み合わせた対策を推進
- 中長期的な研究開発の推進：
  (1) 将来の社会像に基づいて必要なセキュリティ技術を検討し、研究テーマを設定

③研究開発・技術開発の効率的な実施体制の構築と基盤の整備

- 投資効果最大化のため、プロジェクトの途中成果を活用する方策を管理手順に組み込む
- プロジェクトの内容および実施状況の公開を促進
- 情勢変化などを評価し、必要ならば計画変更が可能な、柔軟な管理の仕組を導入
- 官民の連携による研究開発に有用な環境の整備を積極的に推進