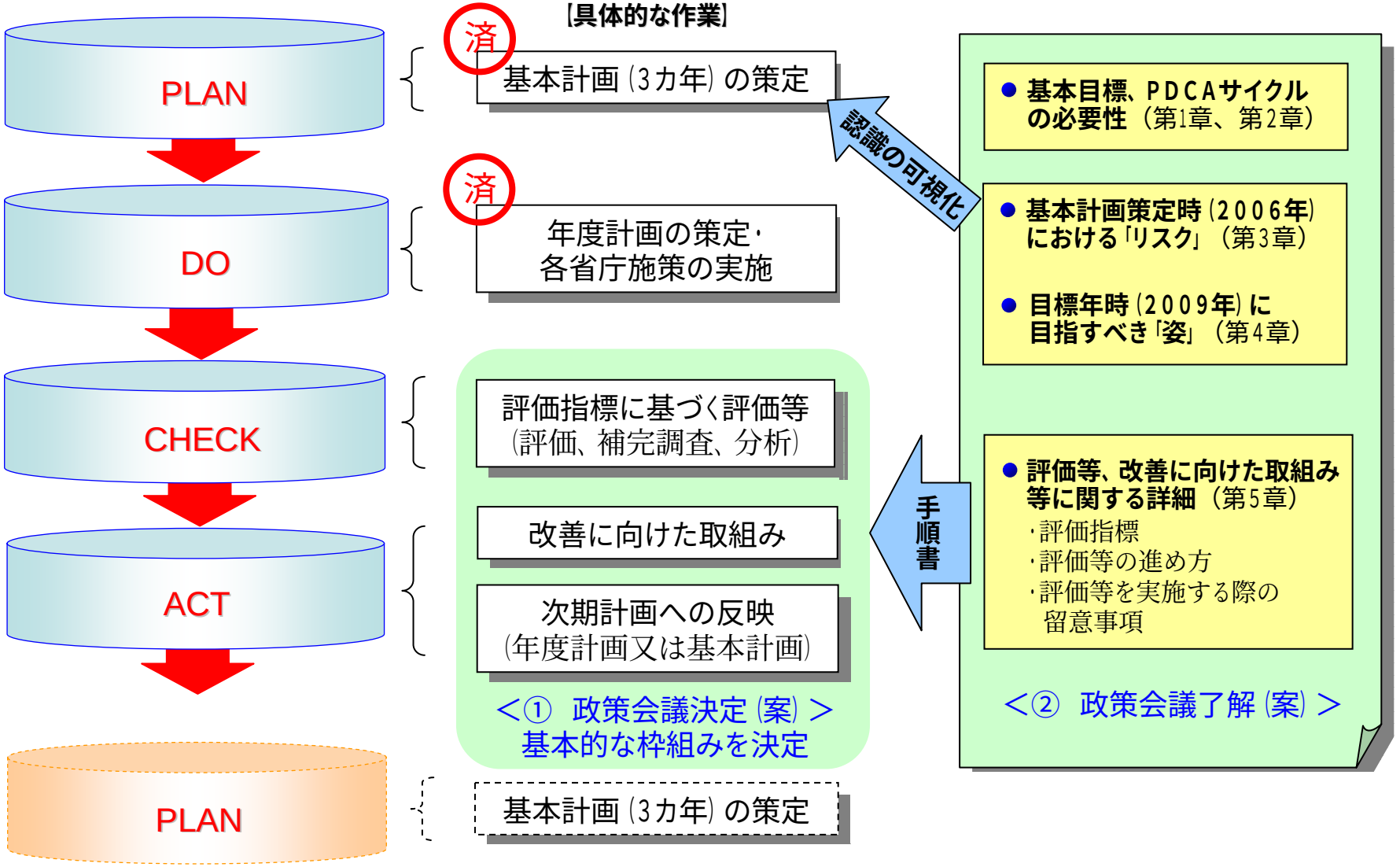
情報セキュリティの観点から見た我が国社会のあるべき姿及び政策の評価のあり方について

2007年2月2日

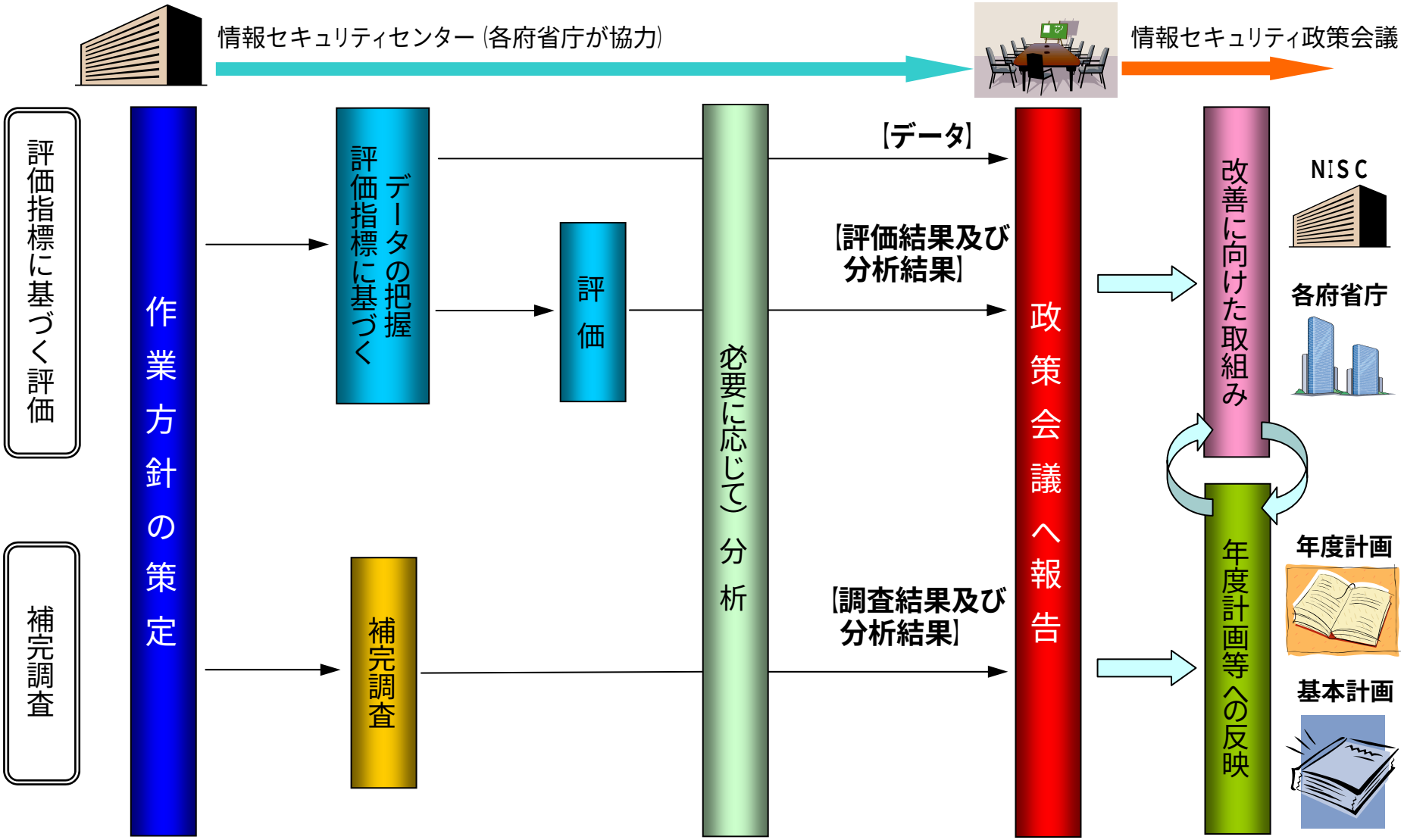
内閣官房情報セキュリティセンター（NISC）

資料２－１

情報セキュリティ政策のＰＤＣＡサイクルと今回決定する事項等の関係



評価指標に基づく評価等の基本的な枠組み



政策会議了解（案）の内容
（2006年時のリスク、2009年時の姿、評価指標等）

○ ２００６年時のリスクの例

・・・適切な対策の実施や事業継続性確保等の取組みが不十分であると、社会に多大な被害や損失が生じる可能性がある。・・・顕在化した問題に対する対症療法にとどまりがちになり、新たな脅威への対応が後手にまわって被害が予想外に拡大する可能性がある。・・・外部脅威による攻撃、改ざん又は破壊等によって、行政サービスのオンライン・サービスが停止する可能性がある。

○ ２００９年時の姿の例

・・・あらゆる主体が各種の取組みを推進したことにより、リスクがＩＴの信頼性を維持できる水準に抑えられ、・・・ＩＴ利用者は、安心して利用しており、・・・リスクに対する対応策を先取り的に考え、根本からリスクを解決する方策を検討する姿勢が定着している。・・・世界最高水準、すなわち他の主体及び諸外国にとって模範となるような政府機関統一基準が確立されている。

○ 評価指標の例

【政府機関】　情報セキュリティマネジメント指標（計画、周知、実施、評価と改善に関して指標を設定）
　　情報セキュリティ対策実施状況評価指標
【重要インフラ】「行動計画」に定める施策の進捗度合い指標
【企業・個人】　企業及び個人の情報セキュリティに関する意識、対策、結果面についての指標
　　（例：情報セキュリティポリシーの策定状況、情報セキュリティ被害経験、セキュリティの言葉の認知度等）

○ その他の留意事項

・評価指標に基づく評価が困難な事項に関して、補完調査によって状況を把握。
・評価結果、補完調査結果等について、背景などを明らかにするために分析を実施。
・政策会議は、各府省庁が新しいリスク等に対して効率的・効果的な対応を行えるよう、必要な取組みを推進。

【参考】「第1次情報セキュリティ基本計画」における評価等に関する記述

第4章　第3節　持続的改善構造の構築

情報セキュリティを巡る問題は、新たなリスク要因が次々と発生し、また想定し得なかった事故、災害や攻撃が発生する等、その状況変化が早いことから、政策の効果を常に評価し、改善を行うことが必要である。このため、政府は、以下のような持続的改善のための構造を構築することが必要である。

(1)「年度計画」の策定とその評価等

政府は、本基本計画の実現を図るため、毎年度、より具体的な施策の実施プログラムを「年度計画」として策定するとともに、その実施状況を評価し、その結果を可能な限り公表する。

なお、政府以外の関係機関における対応が不可欠である等、施策を円滑に進捗させる観点から、中長期的な計画を定めることが必要なものについては、単年度にこだわらず、複数年度のマイルストーン設定も検討する。

(2) 年度途中での緊急事態対応に向けた取組みの実施

政府は、「年度計画」の実施途中であっても、新たなリスク要因や想定し得なかった事故、災害や攻撃の発生等の緊急事態に対応するための取組みを実施する。

(3) 評価指標の確立

各対策実施領域等における、情報セキュリティに関する評価の指標は、これまで確固としたものが策定されてこなかったところであるが、このような指標は、各対策実施領域等における、情報セキュリティ対策の浸透の度合いを評価するために不可欠なものであることから、政府は、これを早急に検討し、本基本計画の実施状況を評価するものとして活用することを目指す。

(4) 本基本計画の見直し

政府は、本基本計画について、3年毎に見直しを行うとともに、環境変化が生じた場合には、期間中であっても見直しを行うこととする。

【参考】「セキュア・ジャパン2006」における評価等に関する記述

第4章　第3節　持続的改善構造の構築

情報セキュリティを巡る問題は、新たなリスク要因が次々と発生し、また想定し得なかった事故、災害や攻撃が発生する等、その状況変化が早いことから、政策の効果を常に評価し、改善を行うことが必要である。このため、政府は、以下のような持続的改善のための構造を構築することが必要である。

(1)「年度計画」の策定とその評価等

ア) 評価の実施及び公表 (内閣官房)
2006年度において、セキュア・ジャパン2006を適切に評価するための手法について検討を行いつつ、そこに記載されている具体的施策の取組状況について評価を実施し、その結果を半年ごとに公表する。その際、IT戦略本部評価専門調査会の検討との連携を図る。

イ) 政府機関の情報セキュリティ対策強化に向けたマイルストーンの検討等 (内閣官房)
2006年度において、基本計画の実現に向けて、政府以外の関係機関における対応をあらかじめ促す等の観点から、政府機関自らの情報セキュリティ向上に係る施策について、2008年度までのマイルストーンを検討する。

ウ)「重要インフラの情報セキュリティ対策に係る行動計画」に基づく取組み (内閣官房)
「重要インフラの情報セキュリティ対策に係る行動計画」に基づく2006年度における取組状況を、重要インフラ専門委員会の場を活用して把握する。

(2) 年度途中での緊急事態対応に向けた取組みの実施

ア) 計画の見直しについての検討 (内閣官房)
情報セキュリティに関する大規模な災害や攻撃の発生等の緊急事態や急激な情勢の変化が起こった際に、本セキュア・ジャパン2006の実施途中であっても、迅速に相応の取組みを策定の上実施する。

(3) 評価指標の確立

ア) 情報セキュリティ対策に関する評価指標の確立 (内閣官房、総務省及び経済産業省)
基本計画 (セキュア・ジャパンの実現) の実現に向けた道筋を可視化する視点に立ち、各対策実施領域 (政府機関、地方公共団体、重要インフラ、企業、個人等) における情報セキュリティ対策の浸透の度合いを評価することができる指標を検討するための体制を2006年度のできる限り早期に設置し、2006年度中に的確な評価指標を確立した上で、これらの指標の政府内及び国際機関等における活用を推進する。
なお、当該評価指標の確立に資するため、独立行政法人情報処理推進機構による「国家情報セキュリティ水準評価指標 (仮称)」の策定を促進するほか、「情報通信インフラのセキュリティ水準評価指標 (仮称)」の策定について検討する。